Česká pobočka AFCEA
a Centrum kybernetické bezpečnosti, z.ú.

Výkladový slovník kybernetické bezpečnosti

Petr Jirásek, Luděk Novák, Josef Požár

Cyber Security Glossary

Páté doplněné a upravené vydání
vydané pod záštitou

Národního úřadu pro kybernetickou a informační bezpečnost

The fifth supplemented and revised edition
is published under the auspices of

The National Cyber and Information Security Agency

Národní úřad pro kybernetickou a informační bezpečnost NÚKIB

Na přípravě slovníku rovněž spolupracovali:

pracovníci Národního úřadu pro kybernetickou a informační bezpečnost,

členové Pracovní skupiny kybernetické bezpečnosti, AFCEA,

členové AFCEA,

členové ČIMIB,

členové ICT Unie,

zástupci akademické obce,

a další odborníci z oblasti kybernetické bezpečnosti.

Vydáno za odborné podpory Policejní akademie ČR v Praze

Tato publikace není určena k prodeji.

Publikace bude distribuována zdarma v tištěné a elektronické podobě. V tištěné podobě výhradně autory, v elektronické podobě autory a spolupracujícími organizacemi.

Also cooperating in the preparation of the Glossary:

Experts of the National Agency for Cyber And Information Security,

Experts of AFCEA Working Group – Cyber Security,

AFCEA members,

Members of ČIMIB,

Members of ICT Union,

Representatives of the academia,

and other professionals from the area of cyber security.

Published with the professional support of the Police Academy of the Czech Republic in Prague

Obsah / Summary

Úvodní slovo

Pojmosloví je v každém oboru významným prostředkem k racionální verbální komunikaci a k nezkreslenému pochopení sdělovaných informací. Obory lidské činnosti se vzájemně prolínají a doplňují. Také jejich odborný jazyk má specifické významy slovické, které se však mezioborově obohacují. Sestavit slovník z oblastí spojených s informačními a komunikačními technologiemi (ICT) je úkol značně složitý a současně velmi naléhavý, zvláště ve spojitosti s bezpečností.

Obor kybernetické bezpečnosti se velmi rychle rozvíjí, což sebou nese terminologickou explozi, doprovázenou zákonitě mnohonásobně různým pojmenováváním stejných jevů, a to přímo v dominantním jazyku oboru – angličtině. Pokoušíme se kodifikovat a sjednocovat vyjadřovací prostředky v oboru ICT – bezpečnosti také proto, že zde pracuje stále větší množství lidí na různém stupni znalostí, dovedností a postavení, kteří nutně potřebují komunikovat prostřednictvím homologizované české a anglické slovní zásoby.

Cílem této publikace je pokročit ve sjednocení terminologie z oblasti kybernetické bezpečnosti na úrovni konce druhé dekády 21. století, včetně doplňků termínů kryptografických a oborů, které mají k dané problematice vztah, jako je například umělá inteligence a „průmysl 4,0“. Všechny uvedené termíny byly diskutovány odborníky z veřejné i soukromé sféry a velký podíl na tvorbě tohoto výkladového slovníku mají i akademičtí pracovníci.

Proměny současné společnosti, v níž stále významnější úlohu zaujímá věda, moderní technologie a ICT se pochopitelně odrážejí i v rozsahu specifické slovní zásoby v oblasti kybernetické bezpečnosti. Ze strany uživatelů jazyka je často velice kriticky a vnímavě posuzovaný proces přejímání slov z cizích jazyků, jehož nedílnou součástí je i vznik nových slovních spojení a utváření dříve jen okrajově zaznamenávaných slovních významů. Všechny tyto změny podněcují potřebu moderního člověka slovům cizího původu dobře rozumět a přesně a výstižně je používat. Platí to pro všechny sociální a věkové uživatelské kategorie. Komunita ICT – bezpečnostních profesionálů se rozšiřuje účastí na sociálních sítích a na mobilních koncových zařízeních. Jsou mezi nimi i latentní „pachatelé“, které je třeba získat do legální sféry.

Výkladový slovník kybernetické bezpečnosti navazuje na výsledky dlouhodobé badatelské a praxeologické aktivity. Rozšiřuje a aktualizuje materiál předchozího 3. vydání Výkladového slovníku kybernetické bezpečnosti (2015), který byl vydán Policejní akademií České republiky v Praze společně s Českou pobočkou AFCEA. Slovník se stal brzy po svém uvedení na knižní trh i v elektronické kopii vyhledávanou příručkou, kterou veřejnost přijala s opravdovým zájmem. Slovník vznikl překladem české terminologie a pojmosloví z kybernetické bezpečnosti do anglického jazyka a vice versa. Tento proces je v podstatě nekonečný a je tomu tak proto, že terminologie kybernetické bezpečnosti se nadále rozšiřuje a vyvíjí.

Snažili jsme se vytvořit slovník, který by zahrnoval jak základní slovní zásobu oboru, tak perspektivní výrazy. Vybírali jsme z kartotéky obsahující více než 1000 výrazů z nejnovějších domácích i zahraničních pramenů. Největší nesnází bylo, že jsme neustále naráželi na slovní spojení, metafory, odborný slang a termíny přejaté a počeštěné z angličtiny, což si vyžádalo tvorbu odpovídající české podoby. Návrh českých ekvivalentů jsme prováděli po prostudování různých odborných publikací a po konzultacích s odborníky příslušných oborů. Tam, kde se nám nepodařilo vytvořit vyhovující termín, uvádíme sousloví, které charakterizuje obsah daného pojmu. Zahrnutí slangových spojení, jako je kyberprostor zvažujeme podle frekvence používání – živého odborného jazyka a podle důvodu vzniku.

Snažili jsme se dát uživatelům dílo z oblasti kybernetické bezpečnosti co nejobsáhlejší a doufáme, že se nám to podařilo, neboť tento aktualizovaný slovník je jedním z prvních česko – anglických slovníků v oboru. Nedostatky slovníku se mohou nejlépe projevit až v praktickém užívání. Jelikož naší snahou je veškeré nedostatky soustavně odstraňovat, uvítáme i nadále všechny připomínky a odpovědně je zvážíme. Tento dvojjazyčný výkladový slovník obsahuje i mnoho výrazů z českého jazyka do angličtiny nepřekládaných, anglické výrazy, které zatím nemají český ekvivalent, jakož i výrazy se kterými lze polemizovat, neboť jsou využívány v okrajových oblastech anebo na ně mohou mít různé odborné skupiny odlišný názor. Je však třeba zdůraznit, že nejde o oficiálně přijatou terminologickou normu.

V pořadí již páté vydání výkladového slovníku je rozšířenou, doplněnou a upravenou verzí předchozího vydání. Autoři tak reagují na připomínky odborné veřejnosti, jakož i na vznik nové legislativy a standardů v oblasti kybernetické bezpečnosti. Autoři zároveň děkují všem, kteří se aktivně podíleli na přípravě této verze slovníku,

jeho připomínkování, jakož i všem autorům původních termínů, které posloužily jako zdroj informací. Speciální poděkování patří pracovníkům Národního úřadu pro kybernetickou a informační bezpečnost, jmenovitě pánům Martinu Konečnému a Adamu Kučínskému a členům pracovní skupiny kybernetické bezpečnosti ČP AFCEA pánům Petru Hrůzovi, Milanu Kný a Jaroslavu Pejčochovi.

Závěrem je vhodné zdůraznit, že výklad v anglickém jazyce reflektuje pojetí výrazů českých mluvčí i v případě přijatých termínů do užívání z angličtiny ze zemí původu. Také poctivá poznámka k autorství – hlavní přidanou hodnotou je sestavení, utřídění a optimalizace významů. Uznání v neposlední řadě patří i překladatelům.

V Praze dne 1. října 2022 Autoři

Introduction

In any human area of activity, terminology is a powerful means of rational verbal communication and undistorted understanding of the information communicated. Moreover, as the areas of human activities interlink and supplement each other, the specialised technical language has no precise limits and is constantly enriched across all the areas. Therefore, a compilation of a glossary, in particular from the areas related to information and communication technology (ICT), is a task which is both rather complicated and highly necessary, and more so in connection with security.

Cyber security develops very quickly, resulting in a terminological explosion accompanied as a rule by an assortment of names for the same phenomena, even in the area's dominant language, English. The necessity for a codification of communication in ICT security follows directly from the fact that more and more employees and managers are active here who have different levels of knowledge and skills and share a need to communicate, if possible, in officially recognised Czech and English vocabularies.

The objective of this publication is an attempt to advance in unifying the terminology in cyber security as of the end of the second decade of the 21st century, supplemented by terms from cryptology and other related areas such as artificial intelligence and "industry 4.0". All the given terms have been discussed by experts from both the public and private domains, and also experts from academia have contributed a significant share in the creation of this Glossary.

Recent transformations in society, with science, modern technology and ICT growing more and more in importance, naturally find their reflection in the scope and specific terminology in the cyber security area. As a result, users of the language are highly critical and sensitive about the process of taking over words from foreign languages as well as about the creation of jargon and new word meanings or word use of words formerly used only marginally. All these changes stimulate the need for a modern human being to understand foreign words quite well and use these precisely and aptly. It holds good for all social and age categories of users. The community of ICT and security professionals is being expanded into social networks and mobile end stations. It includes even the latent "culprits", which could be, ideally, acquired into the legal sphere.

The Glossary of Cyber Security is based on the results of lengthy research and practical activities. It expands and updates the materials of the previous third edition of The Glossary of Cyber Security (2015), published jointly by the Police Academy of the Czech Republic in Prague and the AFCEA Czech Chapter. Shortly after its introduction into the book market, the Glossary, also in its electronic form, became a requested handbook, which was welcome with natural alacrity by the public. The Glossary came into being by translating Czech cyber security terminology into English and vice versa. This process is practically endless because cyber security is expanding and developing.

We have tried to compile a glossary, which would contain both the basic vocabulary and the vocabulary just at the horizon. We have been selecting from card indexes containing more than 1,000 expressions of cyber security, and we intend to supplement the indexes continuously from recent foreign sources. The biggest issue is the fact that we have been encountering vocabulary and terms new even in English and thus have been forced to find the appropriate Czech counterpart. We have made proposals for Czech equivalents after studies of various professional publications and upon consultations with experts from the relevant area. Where we have been unable to find a suitable term, we give an explanation characterising the idea behind the term. The inclusion of slang, such as cyberspace, is considered based on the frequency of use-living technical language-and the reason why it exists.

We have endeavored to present to our users a piece of work as compendious as possible in the area of cyber security, and we hope it will be a success as this Glossary is one of the first Czech-English glossaries in our line of expertise. The deficiencies are best found during practical use. Because we aim to remove the deficiencies rather consistently, we welcome users' comments and will consider these very seriously. This encyclopedic and bilingual Glossary also contains many expressions with no translations from Czech into English and also some debatable expressions whose use is either marginal or where two or more groups of professionals differ. We stress that this is not any officially adopted terminological standard.

This fifth edition of the Glossary is an expanded, amended and updated version of previous editions. It responds to comments of the professional public as well as to new legislation and standards in cyber security. The authors also wish to thank all who have taken an active role in preparing this edition and the commenting process and all those authors of the original terminology, which served as an information

source. Special thanks are due to the employees of the National Cyber and Information Security Agency, namely Messrs. Martin Konečný and Adam Kučínský, as well as members of the AFCEA Cyber Security Working Group, Messrs. Petr Hrůza, Milan Kný and Jaroslav Pejčoch, and experts of the Czech Cyber Center (Centrum kybernetické bezpečnosti, z.ú.).

Finally, it is appropriate to emphasise that the wording in English reflects the point of view of the Czech speakers even though the native English terminology may differ. Also, an honest remark about authorship-the principal added value is the compilation, ordering and optimisation of keywords. Last but not least, credit is due to the translators.

Prague, 1 October 2022 Authors

Česko – anglický slovník / Czech – English Glossary

3DES **Triple DES**

Blokový symetrický šifrovací algoritmus založený na trojnásobné aplikaci normy DES. Může být používán ve variantě EDE (K1, K2, K3) s využitím délky klíčů 168 bitů nebo (K1, K2, K1) s využitím délky klíčů 112 bitů.

A block symmetric encryption algorithm based on the triple application of the DES standard. It could be used in the form of EDE (K1, K2, K3) using key lengths of 168 bits or (K1,K2,K1) with the key length of 112 bits.

Administrace sítě **Network administration**

Každodenní obsluha a správa infrastruktury zaměřená především na provoz, údržbu a rozvoj sítí.

Day-to-day servicing and management of infrastructure, focused on processes, maintenance and development of networks.

Administrativní / procedurální bezpečnost **Administrative / procedural security**

Administrativní opatření pro zajištění počítačové bezpečnosti. Tato opatření mohou být operační postupy nebo postupy týkající se odpovědnosti, postupy zkoumání porušení bezpečnosti a revize auditních záznamů.

Administrative measures to ensure computer security. These measures can be operational procedures or procedures related to responsibility, procedures for examining security incidents and revision of audit records.

Administrátor **Administrator**

Osoba odpovědná za správu části systému (např. informačního systému), pro kterou má zpravidla nejvyšší privilegia přístupu (práva supervizora).

The person responsible for the management of a part of a system (e.g. information system) for which he/she usually has the highest access privileges (supervisor rights).

Adresářová služba **Directory service**

Služba pro vyhledávání a získávání informací z katalogu přesně definovaných objektů, které mohou obsahovat informace o certifikátech, telefonních číslech, přístupových podmínkách, adresách atd.

A service to search and retrieve information from a catalogue of well-defined objects, which may contain information about certificates, telephone numbers, access conditions, addresses, etc.

Adresový (adresní) prostor **Address space**

Souvislý rozsah IP adres. Adresní prostor je tvořen sadou jedinečných identifikátorů (**IP adres**). V prostředí Internetu je správcem jeho adresového rozsahu organizace **IANA**.

*A continuous range of IP addresses. Address space is made up of a set of unique identifiers (**IP addresses**). In the **Internet** environment, **IANA** organisation is the administrator of the address range.*

Adware **Adware**

Reklamní aplikace, která uživateli zobrazuje nevyžádanou reklamu. Často při tom sbírá informace o jeho chování. Poznámka: aplikace může být instalována bez vědomí uživatele nebo bez jeho souhlasu nebo může být uživateli vnucena v rámci licenčních podmínek jiného software.

Advertising application which shows the user unsolicited advertising. Often it acquires information about behaviour. Note: the application may be installed without user knowledge or consent or may be pushed to the user under licencing conditions of other software.

Agentura Evropské unie pro kybernetickou bezpečnost **European union agency for cybersecurity (ENISA)**

Agentura založená Evropskou unií jako kooperativní centrum v oblasti síťové a informační bezpečnosti v roce 2004. Jejím úkolem je tvořit informační platformu pro výměnu informací, znalostí a „best practices“, a tím pomáhat EU, jejím členským státům, soukromému sektoru a veřejnosti při prevenci a řešení bezpečnostních problémů.
ENISA změnila svůj statut nařízením Evropského parlamentu a Rady EU (EU) 2019/881 ze dne 17. dubna 2019 (zákon o kybernetické bezpečnosti) o ENISA (Agentura Evropské unie pro kybernetickou bezpečnost) a o certifikaci kybernetické bezpečnosti informačních a komunikačních technologií a o zrušení nařízení (EU) č. 526/2013.

Agency founded in 2004 by the European Union as a cooperative centre in the area of network and information security. Its role is to create an information platform for the exchange of information, knowledge and "best practices" and thus help EU,

its member states, the private sector and the public in the prevention and solutions of security problems.
ENISA changed its statute by regulation of the European Parliament (EU) 2019/881 of the European Parliament and of the EU Council of 17 April 2019 (Cybersecurity Act) on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013.

Agregace **Aggregation**

Řízená ztráta či omezení informace nebo prostředků, obvykle slučováním, spojením, či statistickými metodami.

Controlled loss or limitation of information or equipment, usually by aggregation, merge, or statistical methods.

Akceptační kritéria **Acceptance criteria**

Kritéria, která se použijí při provádění přejímacích postupů (např. úspěšná kontrola dokumentů nebo úspěšné testování v případě softwaru, firmwaru nebo hardwaru).

Criteria to be applied when performing the acceptance procedures (e.g. successful document review, or successful testing in the case of software, firmware or hardware).

Akceptační prohlášení **Acceptance statement**

Formální prohlášení vedení o převzetí odpovědnosti za vlastnictví rizik, ošetření rizik a zbytkové riziko.

Formal management declaration to assume responsibility for risk ownership, risk treatment and residual risk.

Akční člen, aktuátor **Actuator**

Zařízení pro pohyb nebo ovládání mechanismu nebo systému. Je poháněn zdrojem energie, typicky elektrickým proudem, tlakem hydraulické kapaliny nebo pneumatickým tlakem a přeměňuje tuto energii na pohyb. Akční člen je mechanismus, kterým řídicí systém působí na prostředí. Řídicí systém může být jednoduchý (pevný mechanický nebo elektronický systém), software (např. ovladač tiskárny, řídicí systém robotů) nebo člověk nebo jiný činitel.

A device for moving or controlling a mechanism or system. It is operated by a source of energy, typically electric current, hydraulic fluid pressure, or pneumatic pressure, and converts that energy into motion. An actuator is a mechanism by

which a control system acts upon an environment. The control system can be simple (a fixed mechanical or electronic system), software-based (e.g. a printer driver, robot control system), or a human or another agent.

Aktivní hrozba **Active threat**

Jakákoliv hrozba úmyslné změny stavu systému zpracování dat nebo počítačové sítě. Hrozba, která by měla za následek modifikaci zpráv, vložení falešných zpráv, vydávání se někoho jiného nebo odmítnutí služby.

Any threat of an intentional change in the state of a data processing system or computer network. Threat, which would result in messages modification, the inclusion of false messages, false representation, or service denial.

Aktivní kybernetická obrana **Active cyber defence**

(1) Soubor opatření k detekci, analýze, identifikaci a zmenšení hrozeb v kybernetickém prostoru či z něho vycházejících, v reálném čase, spolu se schopností a zdroji na proaktivní či útočnou činnost proti původcům hrozeb v domovských sítích těchto původců.
(2) Proaktivní opatření za účelem detekce či získání informace o kybernetickém průniku, kybernetickém útoku nebo hrozící kybernetické operaci, nebo pro určení původu operace, které v sobě zahrnuje spuštění útočně preventivní, preventivní nebo kontra-operace proti zdroji.

(1) A set of measures to detect, analyse, identify and mitigate threats in and from the cyberspace, in real time, combined with the capability and resources to take proactive or attack action against threat agents in those agents˙ home networks.
(2) Proactive measures to detect or obtain information about a cyber intrusion, cyber attack or an imminent cyber operation, or to find the source of an operation, which includes launching a preemptive, preventive or counter-operation against the source.

Aktivum **Asset**

Cokoliv, co má hodnotu pro jednotlivce, organizaci nebo veřejnou správu.

Anything that has value to an individual, company or public administration.

Akreditace **Accreditation**

Oficiální manažerské rozhodnutí kompetentního zástupce organizace autorizovat provoz určitého informačního systému a výslovné přijetí rizik (včetně

strategických, provozních, ekonomických nebo reputačních), která organizaci, jejím aktivům nebo jednotlivcům plynou z implementace dohodnutých bezpečnostních opatření.

The official management decision of a competent representative of an organisation, to authorise the operation of the information system and the explicit acceptance of risks (including the strategic, economic or reputational ones) which ensue to the organisation from the agreed security measures.

Aktualizační balík **Service pack**

Souhrn (balík) více aktualizací, který lze instalovat najednou.

Collection (pack) of several updates, which could all be installed at the same time.

Alarm **Alarm**

Zařízení nebo funkce, které upozorňuje na mimořádný stav pomocí slyšitelných anebo viditelných signálů. (2) V procesním řízení alarm znamená událost/stav, který je pro proces nebezpečný. Tyto stavy jsou ukládány v alarm systému. Alarm musí být po svém vyskytu potvrzen (vyřízen), jinak zustává v Alarm systému stále jako aktivní.

A device or function that signals the existence of an abnormal condition by making audible or visible signals. (2) In process control, an alarm means an event / condition that is dangerous for the process. These states are stored in the alarm system. The alarm must be confirmed (reset) after the occurrence. Otherwise, it still remains active in the Alarm System.

Alarm system **Alarm system**

Systém registrace, ukládání a přehledu alarmů.

System for alarms registering, saving and viewing.

Algoritmus **Algorithm**

Jednoznačně definovaný matematický proces spočívající v provedení řady početních operací, který, pokud je dodržen, vede k očekávanému výsledku.

Unambiguously defined mathematical process for the execution of a set of computational rules that, if followed, will give a prescribed result.

Analýza datového provozu **Traffic analysis**

Jednoduché i pokročilé matematické a vizualizační metody sloužící k analýze datového provozu TCP/IP v počítačové síti.

Simple and advanced mathematical and visual methods for the analysis of data traffic TCP/IP in a computer network.

Analýza dopadů na činnosti organizace **Business impact analysis (BIA)**

Proces analýzy provozních funkcí a dopadu, který by na ně mohlo mít narušení.

Process of analysing operational functions and the effect that a disruption might have upon them.

Analýza hrozeb **Threat analysis**

Zkoumání činností a událostí, které by mohly negativně ovlivnit kvalitu služby IT (systém zpracování a přenosu dat) i / nebo data samotná.

Analysis of activities and events, which could negatively affect IT service quality (system of data processing and transfer) and/or data proper.

Analýza komunikace **Traffic analysis**

Viz **Analýza datového provozu**

*See **Traffic analysis***

Analýza počítačového viru **Virus analysis**

Komplexní činnost zahrnující analýzu chování počítačového viru (způsob šíření, skrývání, škody působené virem), analýzu kódu viru, nalezení způsobu vyhledání viru a jeho odstranění ze souborů, resp. nalezení postupu pro nápravu škod virem způsobených. Více též disassemblování, debugger, trasování, emulace kódu.

Complex activity including the analysis of computer virus behaviour (how it spreads, hides, damage caused by the virus), analysis of virus code, finding of the virus and its removal from files, or rectification of damage caused by the virus. More also in Disassembly, Debugger, Tracing, Code emulation.

Analýza rizik **Risk analysis**

Proces pochopení povahy rizika a určení úrovně rizika.

Process to comprehend the nature of risk and determine the level of risk.

Analýza zranitelnosti **Vulnerability analysis**

Systematické zkoumání systému a provozovaných služeb vzhledem k bezpečnostním slabinám a efektivitě bezpečnostních opatření.

Systematic analysis of a system and operating services in view of security weaknesses and the efficiency of security measures.

Analyzátor protokolů **Protocol Analyser**

Viz **Síťový analyzátor**

*See **Network Sniffer***

Anonymita **Anonymity**

Vlastnost určité informace, která zabraňuje určení subjektu, kterého se daná informace týká.

The specific characteristic of information that prevents to identify the subject concerned.

Anonymizace **Anonymisation**

Proces, kterým jsou osobně identifikovatelné informace (PII) nevratně změněny tak, že subjekt PII již nemůže být přímo nebo nepřímo identifikován, ani samotným správcem PII, ani ve spolupráci s jinými stranami.

The process by which personally identifiable information (PII) is irreversibly altered in a way that a PII principal can no longer be identified directly or indirectly, either by the PII controller alone or in collaboration with any other party.

Anonymizované údaje **Anonymized data**

Údaje, které byly vytvořeny jako výstup procesu anonymizace informací.

Data produced as the output of a personally identifiable information anonymisation process.

Anonymní přihlášení **Anonymous login**

Přihlášení do sítě a zpřístupnění jejích zdrojů bez ověření totožnosti účastníka.

Login into network and access to its resources without authentication of the party.

Antispamový filtr **Antispam**

Sofistikovaný software, který každý email porovnává s množstvím definovaných pravidel a pokud email pravidlu vyhovuje, započítá váhu pravidla. Váhy mohou mít různou hodnotu, kladnou i zápornou. Pokud součet vah emailu překročí určitou hodnotu, je označen jako spam.

Sophisticated software comparing each email with a number of defined rules and if the email satisfies a rule, counts in the weight of the rule. The weights can vary in value, positive and negative. When the total of weights exceeds a certain value, it is labelled as spam.

Anti-stealth technika **Anti-stealth technique**

Schopnost **antivirového programu** detekovat i stealth viry (sub-stealth viry), které jsou aktivní v paměti, například pomocí přímého čtení dat z disku bez použití služeb operačního systému.

*Ability of an **antivirus programme** to detect even stealth-viruses (sub-stealth-viruses) which are active in memory, for example by using direct disc reading bypassing the operating system.*

Antivir **Antivirus**

Viz ***Antivirový program***.

*See **Antivirus programme**.*

Antivirový program **Antivirus programme**

Jednoúčelový nebo vícefunkční program plnící jednu nebo několik následujících funkcí: vyhledávání počítačových virů (jednou nebo několika různými technikami, často s možností jejich výběru nebo nastavení režimu vyhledávání – scanování, heuristická analýza, metoda kontrolních součtů, monitorování podezřelých činností), léčení napadených souborů, zálohování a obnova systémových oblastí na disku, ukládání kontrolních informací o souborech na disku, poskytování informací o virech aj.

Single-purpose or multipurpose programme doing one or more of the following functions: searching for computer viruses (by a single or several different

techniques, often with a possibility of their selection or setting mode for search – scanning, heuristic analysis, methods of checksums, monitoring of suspicious activities), healing of infected files, backup and recovery of system sectors on the disc, storing control information on files on disc, providing information on viruses, etc.

Aplikace **Application**

IT řešení, zahrnující aplikační software, aplikační data a procedury, vytvořené za účelem podpory vybraných organizačních procesů nebo funkcí.

IT solution, including application software, application data and procedures, designed to support selected organisational processes or functions.

Aplikační server **Application Server**

Software specializovaný pro provozování sdílených aplikací.

Software specialised for operating shared applications.

Aplikační služby **Application services**

Software, jehož funke jsou doručovány odběratelům prostřednictvím on-line modelu, který zahrnuje webovou nebo klient-server aplikaci.

Software whose functions are delivered to subscribers using an on-line model, which has a web or client-server application.

Architekt kybernetické bezpečnosti **Cyber Security Designer**

Definovaná bezpečnostní role v souladu se zákonem o kybernetické bezpečnosti, představující osobu zajišťující návrh a implementaci bezpečnostních opatření, která je k této činnosti odborně způsobilá a svoji způsobilost prokáže praxí.

Defined security role by the law on cyber security and representing the individual who provides for the design and implementation of security measures, having the expertise for such an activity and who can prove such a capability in practice.

Asymetrický algoritmus **Asymmetric Algorithm**

Šifrovací algoritmus pro realizaci **Asymetrická kryptografie**.

*Encryption algorithm to implement **Asymmetric cryptography**.*

Asymetrická kryptografie **Asymmetric cryptography**

Skupina kryptografických metod (někdy nazývaná také kryptografie s veřejným klíčem), ve kterých se pro šifrování a dešifrování používají dva různé, matematicky svázané klíče: klíč veřejný a klíč soukromý. Jeden klíč je použit jako šifrovací a druhý jako dešifrovací. Kromě utajení obsahu komunikace se asymetrická kryptografie používá také pro digitální podpis, který umožňuje ověřit identitu autora dat.

A group of cryptographic methods (sometimes known as public-key cryptography) where different keys are used for encrypting and decrypting – more precisely a pair of mathematically bound keys. The pair is made up of a public key and a private key. The first key is used as the encryption key, the second one as the decryption key. In addition to making the content of communication secret, asymmetric communication is also used for the electronic (digital) signature that gives the possibility to verify the author of data.

Attack surface **Attack surface**

Kód v počítačovém systému, který může být spuštěn neautorizovanými uživateli.

Code within a computer system that can be run by unauthorized users.

Audit **Audit**

Systematický, nezávislý a dokumentovaný proces k získání důkazů z auditu a jejich objektivní ohodnocení, aby se určil rozsah, v jakém jsou auditní kritéria splněna.

Systematic, independent and documented process for obtaining audit evidence and evaluating it objectively to determine the extent to which the audit criteria are fulfilled.

Audit počítačové bezpečnosti **Computer security audit**

Nezávislé ověření implementace opatření a jejich účinnosti vzhledem k dosažení počítačové bezpečnosti.

Independent verification of measures of implementation and their efficiency with the view of attaining computer security.

Audit počítačového systému **Computer system audit**

Zkoumání postupů používaných v systému zpracování dat s cílem zhodnotit jejich účinnost a správnost, a doporučit zlepšení.

Analysis of procedures used in data processing in order to evaluate their efficiency and correctness, and to recommend improvements.

Auditní logování **Audit logging**

Zaznamenávání údajů o událostech v oblasti bezpečnosti informací pro účely přezkumu a analýzy a průběžného sledování.

Recording of data on information security events for the purpose of review and analysis, and ongoing monitoring.

Auditní záznam **Audit trail, audit log**

Chronologický zápis aktivit v systému, které jsou dostatečné pro rekonstrukci, zpětné sledování a vyhodnocení sekvence stavu prostředí a aktivit souvisejících s operacemi a procedurami od jejich počátku ke konečnému výsledku.

A chronological record of those system activities, which suffice for restoring, backtracking and evaluation of the sequence of states in the environment as well as activities related to operations and procedures from their inception to the final result.

Auditovaná událost **Audit event**

Systémem detekovaná akce, která vyvolá spuštění a zápis auditu.

Event detected by the system and resulting in triggering and recording the audit.

Autentičnost **Authenticity**

Vlastnost vyjadřující, že určitá entita je totožná s tou, za kterou se vydává.

Property that a certain entity is identical with what it claims to be.

Autentizace **Authentication**

Viz **Ověření totožnosti**

*See **Authentication***

Autentizace dat **Data authentication**

Viz **Ověření totožnosti dat**

*See **Data authentication***

Autentizace entity / identity — **Entity / identity Authentication**

Viz **Ověření totožnosti entity / identity**

*See **Entity / identity authentication***

Autentizace zprávy / původu dat — **Message / data origin authentication**

Viz **Ověření totožnosti zprávy / původu dat**

*See **Message / data origin authentication***

Autentizační faktor — **Authentication factor**

Informace anebo proces využívaný ke zjištění nebo ověření totožnosti určité entity. Autentizační faktory jsou rozdělené do čtyř kategorií: (1) něco, co určitá entita vlastní (např. podpis zařízení, průkaz, hardwarové zařízení obsahující pověření, soukromý klíč); (2) něco, co určitá entita ví (např. heslo, PIN); (3) něco co určitá entita je (např. biometrická charakteristika); nebo (4) něco, co určitá entita zpravidla dělá (např. vzorec chování).

A piece of information and/or process used to authenticate or verify the identity of an entity. Authentication factors are divided into four categories: 1) something an entity has (e.g., device signature, passport, hardware device containing a credential, private key); 2) something an entity knows (e.g., password, PIN); 3) something an entity is (e.g., biometric characteristic); or 4) something an entity typically does (e.g., behaviour pattern).

Autentizační kód zprávy — **Message authentication code (MAC)**

Kód určený pro kontrolu integrity a oveření totožnosti zprávy. Slouží k ochraně proti náhodným nebo úmyslným změnám nebo chybám v datovém souboru. Datový soubor je zašifrován blokovým algoritmem tajným klíčem (v módu CBC), z takto zašifrovaných dat se vyjme část posledního bloku a tento krátký kód je označen jako MAC.

Code to check the integrity and secure the authentication of a message. It serves to protect against contingent or intended alterations or errors in the data file. The data file is encrypted by a block algorithm using a secret key (in CBC mode), a

portion from the last block of this encrypted data is taken out, and this short code is denoted MAC.

Autentizační protokol **Authentication protocol**

Definovaná posloupnost zpráv mezi entitou a ověřovatelem, která ověřovateli umožňuje provést ověření pravosti entity.

Defined sequence of messages between an entity and a verifier that enables the verifier to perform authentication of an entity.

Autentizační výměna **Authentication exchange**

Mechanizmus, jehož cílem je zjistit totožnost entity (subjektu) pomocí výměny informací.

Mechanism whose objective is to find out the identity of an entity (subject) by way of information exchange.

Automatické monitorování výskytu bezpečnostního incidentu **Automated security incident measurement (ASIM)**

Automatické monitorování provozu sítě s detekcí neautorizovaných aktivit a nežádoucích událostí.

Automatic monitoring of network operations with the detection of non-authorised activities and undesirable events.

Automatizace budov **Building automation**

Systém řízení ventilace, teploty, vlhkosti, osvětlení a dalších procesů v budově. Důvodem je efektivní nakládání s energiemi a zjednodušení údržby. System řízení budovy je typickým příkladem DCS (Distribuovaný řídicí systém).

Central ventilation, temperature, humidity, lighting and other building control system. The reason is efficient energy management and simplification of maintenance. The building management system is a typical example of a DCS (Distributed Control System).

Autorita časového razítka **Time-stamping authority (TSA)**

Důvěryhodná třetí strana, které bylo svěřeno poskytování služby časového razítkování.

Trusted third party trusted to provide a time-stamping service.

Autorizace **Authorization**

Udělení práv, které zahrnuje udělení přístupu na základě přístupových práv. Proces udělení práv subjektu pro vykonávání určených aktivit v informačním systému.

Granting rights including granting access on the basis of access rights. Process of rights granting to a subject to perform defined activities in the information system.

Autorizační údaje **Credentials**

Data, která jsou přenášena k ustavení prohlašované identity dané entity, pověření.

Data transferred in order to establish proclaimed identity of a given entity, credentials.

Autorizovaný uživatel **Accredited user**

Uživatel, který má určité právo nebo povolení pracovat v Informačním systému a s aplikacemi podle stanovených zásad přístupu.

User having certain right or permission to work in the information system and with the applications in accordance with defined access guidelines.

Bezdrátová lokální síť **Wireless local area network (WLAN)**

Počítačová síť, která spojuje dvě nebo více zařízení pomocí bezdrátové distribuční metody v omezeném prostoru.

A computer network that links two or more devices using wireless communication within a limited area.

Bezpečnost **Security**

Vlastnost prvku (např. informační systém), který je na určité úrovni chráněn proti ztrátám, nebo také stav ochrany (na určité úrovni) proti ztrátám. Bezpečnost IT zahrnuje ochranu důvěrnosti, integrity a dosažitelnosti při zpracování, úschově, distribuci a prezentaci informací.

Property of an element (e.g. an information system) which is at a certain level protected against losses, or also a state of protection (at a certain level) against losses. IT security covers protection of confidentiality, integrity and availability during processing, storage, distribution and presentation of information.

Bezpečnost dat **Data security**

Počítačová bezpečnost aplikovaná na data. Zahrnuje například řízení přístupů, definování politik a procesů a zajištění integrity dat.

Computer security applied to data. Includes for example control of access, definition of policies and processes and ensuring data integrity.

Bezpečnost informací / informačních systémů **Information security (INFOSEC)**

(1) Zabezpečení (ochrana) důvěrnosti, integrity a dostupnosti informací.
(2) Uplatnění obecných bezpečnostních opatření a postupů sloužících:
(a) k ochraně informací před jejich ztrátou nebo kompromitací (ztráta důvěrnosti, integrity, a dalších vlastností jako např. autentičnost, odpovědnost, nepopíratelnost a spolehlivost), případně k jejich zjištění a přijetí nápravných opatření.
(b) k zachování dostupnosti informací a schopnosti s nimi pracovat v rozsahu přidělených oprávnění. Opatření INFOSEC zahrnují bezpečnost počítačů, přenosu, emisí a šifrovací bezpečnost a odhalování ohrožení skutečností a systémů a jeho předcházení.

(1) Preservation (protection) of confidentiality, integrity and availability of information.
(2) Implementation of general security measures and procedures for:
(a) protection of information against loss or compromise (loss of confidentiality, integrity and reliability), or as the case may be for their detection and adoption of remedial actions.
(b) continuation of information availability and the ability to work with them within the scope of functional rights. Measures INFOSEC cover security of computers, transmission, emissions and encryption security and exposing threats to facts and systems and prevention thereof.

Bezpečnost internetu **Internet security**

Ochrana důvěrnosti, integrity a dostupnosti informací v síti internet.

Protection of confidentiality, integrity and availability of information in the Internet network.

Bezpečnost komunikací **Communication security (COMSEC)**

Použití bezpečnostních opatření v komunikacích, které znemožní neoprávněným osobám získat informace, které lze získat z přístupu ke komunikačnímu provozu a

z jeho vyhodnocení, nebo které zajistí autentičnost komunikačního provozu. Počítačová bezpečnost aplikovaná na datovou komunikaci – přenos dat.

Use of such security measures in communications which prohibit unauthorised persons from obtaining information which could be gained from access to communication traffic and its evaluation, or which ensure the authenticity of the communication process. Computer security as applied to data communications – data transfer.

Bezpečnost transportní vrstvy **Transport layer security (TLS)**

Kryptografický protokol, který poskytuje komunikační bezpečnost pro Internet. Používá se asymetrické šifrování pro výměnu klíčů, symetrické šifrování pro důvěrnost a kody pro ověřování celistvosti zpráv. Široce se používá několik verzí těchto protokolů v aplikacích jako prohlížení na webu, elektronická pošta, faxování přes internet, instantní zprávy and voice-over-IP (***VoIP***).

*A cryptographic protocol that provides communication security over the Internet. It uses asymmetric cryptography for authentication of key exchange, symmetric encryption for confidentiality and message authentication codes for message integrity. Several versions of the protocols are in widespread use in applications such as web browsing, electronic mail, Internet faxing, instant messaging and voice-over-IP (**VoIP**).*

Bezpečnostní audit **Security audit**

Nezávislá revize a zkoumání záznamu systému zpracování dat a činností pro testování adekvátnosti systémových kontrol, k zjištění shody s přijatou bezpečnostní politikou a operačními postupy, k detekování porušení bezpečnosti a doporučení jakýchkoliv indikovaných změn v řízení, bezpečnostní politice a postupech. Nezávislé testování činnosti informačního systému a záznamů o této činnosti. Cílem je určení, zda kontroly jsou odpovídající, zda existuje shoda s bezpečnostní politikou, doporučení případných změn v systému protiopatření. Je zpravidla prováděn externím, nebo interním auditorem.

Independent revision and analysis of records in the data processing system as well as activities for testing of the suitability of system controls, checking compliance with accepted security policy and operational procedures, detection of security infringements and recommendation for any indicated changes in the control, security policy and procedures. Independent testing of the information system activity and records thereof. The objective is to determine if checks are appropriate if there is compliance with security policy, the recommendation of eventual changes

in the system of countermeasures. As a rule, it is done by an external or an internal auditor.

Bezpečnostní autorita **Security authority**

Entita odpovědná za správu bezpečnostní politiky v rámci bezpečnostní domény.

The entity accountable for the administration of security policy within the security domain.

Bezpečnostní brána **Security gateway**

Bod připojení mezi sítěmi nebo mezi podskupinami v rámci sítí nebo mezi softwarovými aplikacemi v různých bezpečnostních doménách, které mají chránit síť podle dané bezpečnostní strategie.

Point of connection between networks, or between subgroups within networks, or between software applications within different security domains intended to protect a network according to a given security policy.

Bezpečnostní cíle **Security aims**

Stav bezpečnosti, který má daný systém nebo produkt dosáhnout.

State of security which the given system or product has to reach.

Bezpečnostní dohled **Security assurance**

Kontrolní role, která prověřuje, zda jsou, nebo budou plněny bezpečnostní cíle.

Control role, which verifies whether the security objectives are or will be met.

Bezpečnostní doména **Security domain**

Skupina uživatelů a systémů podléhající společné bezpečnostní politice.

A group of users and systems subject to a common security policy.

Bezpečnostní filtr **Security filter**

Důvěryhodný počítačový systém, který prosazuje bezpečnostní politiku u dat procházejících systémem.

Trusted computer system enabling security policy for data passing through the system.

Bezpečnostní hrozba **Information security threat**

Potenciální příčina nežádoucí události, která může mít za následek poškození systému a jeho aktiv, např. zničení, nežádoucí zpřístupnění (kompromitaci), modifikaci dat nebo nedostupnost služeb.

A potential cause of an undesired event, which may result in damage to the system and its assets, e.g. destroying, undesired disclosing (compromising), data modification or unavailability of services.

Bezpečnostní incident **Security incident**

Porušení nebo bezprostřední hrozba porušení bezpečnostních politik, bezpečnostních zásad nebo standardních bezpečnostních pravidel provozu Informační a komunikační technologie.

Infringement or an imminent threat of infringement, of security policies, security principles or standard security rules of operation for the information and communication technologies.

Bezpečnostní kategorie **Security category**

Seskupení citlivých informací používaných k řízení přístupu k datům.

Grouping of sensitive information used when controlling data access.

Bezpečnostní klasifikace **Security classification**

Určení, jaký specifický stupeň ochrany před přístupem data nebo informace vyžadují, spolu s vyznačením tohoto stupně ochrany.

The determination which level of protection for data or information is required before access, together with noting this level of protection.

Bezpečnostní manažer **Security manager**

Zaměstnanecká role pro výkon odpovědnosti gestora IS za bezpečnost s definováním odpovědností a pravomocí.

Employee role to act as a guarantee for IT security with the definition of responsibilty and authority.

Bezpečnostní opatření **Security measures**

Organizační, provozní a technická opatření (tj. zabezpečení nebo protiopatření) předepsaná určitému informačnímu systému za účelem ochrany důvěrnosti, integrity a dostupnosti systému a v něm obsažených informací.

The management, operational, and technical measures (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and information in it.

Bezpečnostní opatření – zabezpečení **Security measures-safeguards**

Opatření pro zajištění bezpečnostních požadavků kladených na systém. Mohou mít různý charakter (fyzická ochrana zařízení a informace, personální bezpečnost – kontrola pracovníků, organizační opatření – provozní předpisy apod.).

Protective measures to ensure security requirements put on the system. May vary in character (physical protection of equipment and information, personnel security – checking of employees, organisational measures – operational rules, and similar).

Bezpečnostní opatření – protiopatření **Security measures-countermeasures**

Úkon, zařízení, postup, nebo technika, která snižuje dopad hrozby, zranitelnosti či útoku tím, že:
(1) je zcela eliminuje,
(2) zmírňuje způsobené škody,
(3) je rozpozná a ohlásí a tím umožní zjednání nápravy.

An action, device, procedure, or technique that reduces a threat, vulnerability, or an attack:
(1) by eliminating or preventing it,
(2) by minimising the harm it can cause,
(3) or by discovering and reporting it so that corrective action can be taken.

Bezpečnostní politika **Security policy**

Pravidla, nařízení a postupy, kterými se řídí správa, ochrana a distribuce informačních aktiv včetně citlivých informací v rámci organizace a jejích systémů, a které mají dopad na systémy a jejich prvky.

Rules, directives and procedures that govern the management, protection and distribution of information assets, including sensitive information, within an

organisation and its systems, particularly those which impact the systems and their elements.

Bezpečnostní politika informačního systému **IS security policy**

Celkový záměr vedení a směr řízení bezpečnosti informačního systému se stanovením kritérií pro hodnocení rizik.

General purpose of management and direction in the control of information system security with the definition of criteria to assess risks.

Bezpečnostní politika IT **IT security policy**

Pravidla, směrnice a praktiky, které rozhodují o tom, jak jsou aktiva včetně citlivých informací spravovány, chráněny a distribuovány uvnitř organizace a jejich systémů **ICT.**

*Rules, directives and practices deciding how are assets including sensitive information administered, protected and distributed inside the organisation and its **ICT** systems.*

Bezpečnostní politika organizace **Security policy of an organisation**

Soubor bezpečnostních pravidel, postupů a doporučení v rámci organizace.

Set of security rules, procedures and recommendations for an organisation.

Bezpečnostní politika sítě **Security policy of network**

Soubor prohlášení, pravidel a příkladů, které vysvětlují přístup organizace k využívání svých síťových zdrojů a stanoví, jak by měly být její síťová infrastruktura a síťové služby chráněny.

Set of statements, rules and examples that explain an organisation's approach to the use of its network resources, and specify how its network infrastructure and network services should be protected.

Bezpečnostní požadavky **Security requirements**

Požadavky kladené na informační systém, které jsou odvozeny ze zákonů, instrukcí, právních úprav, závazných norem a standardů, vnitřních předpisů organizace; prostředí, ve kterém systém působí a poslání, které plní; nutné pro zajištění důvěrnosti, dostupnosti a integrity informací, která se v systému zpracovává.

Requirements put on the information system, which follow from laws, instructions, legal amendments, binding standards, internal regulations of an organisation; environment where the system operates and the mission it fulfills; necessary for ensuring confidentiality, availability and integrity of information processed in the system.

Bezpečnostní prověření **Security clearance**

Povolení udělené jednotlivci pro přístup k datům nebo informacím na nebo pod specifickou bezpečnostní úrovní.

Clearance given to an individual for accessing data or information on or below the specified security level.

Bezpečnostní přístrojový systém **Safety Instrumented System (SIS)**

Systém složený ze senzorů, logických automatů a koncových řídících prvků, který uvede process do bezpečného stavu dojde-li porušení předem stanovených provozních podmínek. Často se nazývá rovněž nouzový vypínací systém (ESS), bezpečnostní vypínací systém (SSD) a bezpečnostní blokovací systém (SIS).

A system that is composed of sensors, logic solvers, and final control elements whose purpose is to take the process to a safe state when predetermined operational conditions are violated. Often also called emergency shutdown system (ESS), safety shutdown system (SSD), and safety interlock system (SIS).

Bezpečnostní rada státu **National security council**

Stálý pracovní orgán vlády České republiky (ČR) pro koordinaci bezpečnosti ČR a přípravu návrhů opatření k jejímu zajištění.

Permanent working body of the government of the Czech Republic (CZE) for the coordination of security of CZE and preparation of proposals to implement them.

Bezpečnostní role **Security roles**

Definované role v souladu se zákonem o kybernetické bezpečnosti (například: výbor pro řízení kybernetické bezpečnosti, manažer kybernetické bezpečnosti, architekt kybernetické bezpečnosti, garant aktiva), definující odpovědnosti spojené s řízením kybernetické bezpečnosti.

Defined roles in accordance with the law on cyber security (examples: committee to manage cyber security, cyber security manager, cyber security designer,

guarantor of assets) which define responsibilities linked to cyber security management.

Bezpečnostní rozšíření systému doménových jmen **Domain name system security extensions (DNSSEC)**

Sada specifikací, které umožňují zabezpečit informace poskytované ***DNS*** systémem v IP sítích (např. Internet). DNSSEC používá asymetrické šifrování (jeden klíč pro zašifrování a druhý klíč na dešifrování). Držitel domény, která používá DNSSEC, vygeneruje privátní a veřejný klíč. Svým privátním klíčem pak elektronicky podepíše technické údaje, které o své doméně do ***DNS*** vkládá. Pomocí veřejného klíče, který je uložen u nadřazené autority jeho domény, je pak možné ověřit pravost tohoto podpisu. DNSSEC dnes používá řada velkých serverů.

*Set of specifications which enable the security of information provided to **DNS** by a system in IP networks (Internet, for example). DNSSEC uses asymmetric encryption (one key for encryption and the second one for decryption). The owner of the domain, which uses DNSSEC generates both the private and the public key. Using its private key it then electronically signs technical data about the domain, which are then input into **DNS**. Using the public key, which is stored at an authority superior to the domain, it is possible to verify the authenticity of the signature. Some large servers use DNSSEC at present.*

Bezpečnostní standardy **Security standards**

Soubor doporučení a obecných principů pro vymezení, udržování a zlepšování bezpečnosti informací v organizaci.

Set of recommendations and general principles to define, maintain and improve information security inside an organisation.

Bezpečnostní událost **Security event**

Událost, která může způsobit nebo vést k narušení informačních systémů a technologií a pravidel definovaných k jeho ochraně (bezpečnostní politika).

Event, which may result in or cause the infringement of information systems and technologies and rules defined for the protection (security policy).

Bezpečnostní úroveň **Security level**

Kombinace hierarchické bezpečnostní klasifikace a bezpečnostní kategorie, reprezentující citlivost objektu nebo bezpečnostní prověření jednotlivce.

Combination of a hierarchic security classification and security category, representing sensitivity of an object or security clearance of an individual.

Bezpečnostní zranitelnost **Security vulnerability**

Úmyslná chyba nebo neúmyslný nedostatek či závada v software obecně nebo ve firmware zařízení komunikační infrastruktury, která může být zneužita potenciálním útočníkem pro škodlivou činnost. Tyto zranitelnosti jsou buď známé a publikované, ale výrobcem ještě neošetřené nebo skryté a neobjevené. V případě skrytých zranitelností je důležité, zda je objeví dříve útočník, výrobce, bezpečnostní analytik, či uživatel. Bezpečnostní zranitelnosti jsou proto potenciálními bezpečnostními hrozbami. Bezpečnostní zranitelnosti lze eliminovat důsledným bezpečnostním záplatováním systémů.

Intentional error or unintended defect or software error in general or in the firmware of the communication infrastructure equipment, which may be used by a potential attacker for harmful activity. These vulnerabilities are either known or published but yet untreated by the manufacturer, or hidden and undetected. In case of hidden vulnerabilities, it is important whether these are detected sooner by the attacker, manufacturer, security analyst or user. Security vulnerabilities are therefore potential security threats. Security vulnerabilities can be eliminated by consequential security patches for the system.

Běžný provoz **Normal operation**

Provoz, ve kterém jsou všechny algoritmy, bezpečnostní funkce, služby nebo procesy dostupné anebo konfigurovatelné.

Operation where the entire set of algorithms, security functions, services or processes are available or configurable.

Biometrické údaje **Biometric data**

Osobní údaje vyplývající z technického zpracování fyzických, fyziologických či behaviorálních znaků určité osoby, které umožňují určit nebo potvrdit totožnost dané osoby, například obraz tváře nebo otisky prstů.

Personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or fingerprints.

Biometrický systém **Biometric system**

Systém pro automatické rozpoznávání osob na základě jejich chování a fyziologických charakteristik.

System for the purpose of the automated recognition of individuals based on their behavioural and physiological characteristics.

Biometrie **Biometrics**

Automatické rozpoznání určité osoby založené na jejích behaviorálních anebo biologických znacích.

Automatic recognition of a specific individual based on their behavioural or biological characteristics.

BitTorrent **BitTorrent**

Nástroj pro peer-to-peer (**P2P**) distribuci souborů, který rozkládá zátěž datových přenosů mezi všechny klienty, kteří si data stahují.

*Tool for peer-to-peer (**P2P**) distribution of files, which spreads out the load of data transfers among all clients downloading data.*

Black hat **Black hat**

Více **Cracker**.

*See **Cracker**.*

Blacklist **Blacklist**

Seznam určitých entit, například hostů, nebo aplikací, o kterých je známo, že jsou škodlivé a jsou proto zakázané, odmítané nebo přehlížené.

A list of specific entities, such as hosts or applications that are known to be malign and are thus denied, rejected, or disregarded.

Bloková šifra **Block Cipher**

Symetrický šifrovací systém, ve kterém šifrovací algoritmus transformuje blok otevřeného textu, tedy řetězec bitů definované délky (blok), do bloku zašifrovaného textu.

Symmetric encryption system with the property that the encryption algorithm operates on a block of plaintext, i.e. a string of bits of a defined length, to yield a block of ciphertext.

Bluetooth **Bluetooth**

Standard bezdrátové technologie pro přenos dat na malé vzdálenosti.

Wireless technology standard for data transfer over short distances.

Bod obnovy dat **Recovery point objective (RPO)**

Určitý bod, k nemuž musí být informace používané při činnosti obnoveny, aby při opětovném zahájení provozu mohla být činnost vykonávána. Může být rovněž označen za „maximální ztrátu dat“.

Point to which information used by an activity must be restored to enable the activity to operate on resumption. Can also be referred to as “maximum data loss”.

Bot (Robot) **Bot**

V rámci kybernetické kriminality: program, který ovládne počítač v síti a používá ho k provádění nekalých aktivit – např. distribuované útoky (***DDoS***) a hromadná distribuce nevyžádané komerční pošty. Individuální boty jsou základem velkých skupin robotů známých jako botnety. Počítač zcela nebo částečně ovládaný botem je známý jako "zombie".

Within the framework of cyber criminality: programmes which take over computers in the network and use them for criminal activities – for example, distributed attacks (DDoS) and mass distribution of unsolicited commercial emails. Individual bots are the basis for large groups of robots known as botnets. Computer wholly or partially taken over by a bot is known as "zombie".

Botnet **Botnet**

Software, který slouží ke vzdálenému ovládání botů, které běží na infikovaných počítačích, a zajišťuje, že cracker má přístup k výpočetnímu výkonu mnoha strojů současně. Umožňuje provádět nezákonnou činnost ve velkém měřítku – zejména útoky ***DDoS*** a distribuci spamu.

Software for the remote control of bots, which run on infected computers. The software ensures that the cracker can access the computing power of many machines simultaneously. It allows for illegal activities on a large scale-in particular DDoS attacks and spam distribution.

Brána **Gateway**

Zařízení, které převádí určitý protokol na jiný protokol.

Device that converts a specific protocol to another protocol.

BSD licence **BSD licence**

Třída tolerujících licencí na volný software, která klade minimální omezení na opakované šíření takového softwaru.

A family of permissive free software licenses, imposing minimal restrictions on the redistribution of covered software

Broadcast **Broadcast**

Přenos na všechna zažízení v určité síti bez potvrzení ze strany příjemců.

Transmission to all devices in a network without any acknowledgment by the receivers.

BYOD **Bring Your Own Device (BYOD)**

Vztahuje se na zaměstnance, kteří přinášejí, užívají a připojují na pracovišti vlastní mobilní zařízení, jako například chytré telefony, laptopy nebo PDA.

Refers to workers bringing their own mobile devices, such as smartphones, laptops and PDAs, into the workplace for use and connectivity.

CAPTCHA **Completely automated public Turing test to tell computers from humans apart (CAPTCHA)**

Turingův test, který se na webu používá ve snaze automaticky odlišit skutečné uživatele od robotů, například při vkládání komentářů, při registraci apod. Test spočívá zpravidla v zobrazení obrázku s deformovaným textem, přičemž úkolem uživatele je zobrazený text opsat do příslušného vstupního políčka. Předpokládá se, že lidský mozek dokáže správně rozeznat i deformovaný text, ale internetový robot při použití technologie OCR ne. Nevýhodou obrázkové CAPTCHA je nepřístupnost pro zrakově postižené uživatele, proto je obvykle doplněna o možnost nechat si písmena z obrázku přečíst.

Turing test used on the web to automatically differentiate real users from robots, for example, when entering comments, at registration, etc. The test usually consists of an image with a deformed text and the task for the user is to rewrite the pictured

text into the entry field. It is assumed that the human brain can properly recognise even corrupted text, but an internet robot using OCR technology cannot do. The disadvantage of the image CAPTCHA is its unavailability for users with visual impairment; hence usually there is the option of having the letters from the image read aloud.

Certifikace **Certification**

(1) Atestace vydaná třetí stranou, která se vztahuje k produktům, procesům, systémům nebo osobám.
(2) Proces ověřování způsobilosti komunikačních a informačních systémů k nakládání s utajovanými informacemi, schválení této způsobilosti a vydání certifikátu.

(1) Third-party attestation related to products, processes, systems or persons.
(2) Proces for verification of the competence of communication and information systems for handling classified information, approval of such competence and issuance of a certificate.

Certifikační autorita (CA) **Certification authority (CA)**

V počítačové bezpečnosti třetí strana, která vydává digitální certifikáty, tak, že svojí autoritou potvrzuje pravdivost údajů, které jsou ve volně dostupné části certifikátu.

In computer security, a third party which issues digital certificates and uses its authority to confirm the authenticity of data, which exist in the freely accessible part of the certificate.

Certifikační dokument **Certification document**

Dokument označující, že systém řízení např. systém řízení bezpečnosti informací klientské organizace vyhovuje předepsaným normám a další dokumentaci vyžadované pro certifikovaný systém.

Decument stating that any system of control, for example system for the control of information security, meets the required standard, and other documentation needed for a certified system.

Certifikační orgán **Certification body**

Třetí strana, která hodnotí a certifikuje systém řízení např. systém řízení bezpečnosti informací klientské organizace s ohledem na mezinárodní normy a další dokumentaci požadovanou pro certifikovaný systém.

Third party which assesses and certifies a system, for example system for the control of computer security for a client organization, with regard to international standards and other documentation needed for a certified system.

Certifikát **Certificate**

Data subjektu, která jsou nefalšovatelná pomocí soukromého nebo tajného klíče certifikační autority. Poznámka: Nefalšovatelný znamená, že je nemožné jej nezákonně zkopírovat nebo napodobit.

Entity's data rendered unforgeable with the private or secret key of a certification authority. Note: Unforgeable means impossible to copy or imitate unlawfully.

Certifikát řízení přístupu **Access control certificate**

Bezpečnostní certifikát obsahující informaci o řízení přístupu.

Security certificate containg information on access control.

Certifikát veřejného klíče **Public key certificate**

Informace o veřejném klíči entity, která je proti padělání chráněna podpisem příslušné certifikační autority.

Public key information of an entity signed by an appropriate certification authority and thereby protected against forgery.

Cíl **Objective**

Výsledek, kterého má být dosaženo.

Result to be achieved.

Cíle opatření **Control objective**

Prohlášení popisující, čeho má být dosaženo zavedením opatření.

Statement describing what is to be achieved as a result of implementing controls.

Cíle přezkoumání **Review objective**

Prohlášení popisující, za jakým účelem je prováděno přezkoumání.

Statement giving the reason for review.

Citlivá data **Sensitive data**

Chráněná data mající pro chod organizace zásadní význam. Jejich vyzrazením, zneužitím, neautorizovanou změnou nebo nedostupností by vznikla organizaci škoda, případně by organizace nemohla řádně plnit svoje poslání.

Protected data having fundamental importance for the operation of an organisation. Its leakage, abuse, unauthorised alteration or unavailability would mean damage to the organisation, or, as the case may be, the organisation would be unable to meet its objectives.

Citlivá informace **Sensitive information**

Informace, která na základě rozhodnutí příslušné autority musí být chráněna, protože její zpřístupnění, modifikace, zničení, nebo ztráta by způsobilo někomu nebo něčemu znatelnou újmu, škodu.

Information which, on the basis of a decision by the relevant authority, must be protected, because access to it, modification, destruction, or loss would cause a substantial damage to someone or something.

Citlivost **Sensitivity**

Míra důležitosti přiřazená informacím vlastníkem těchto informací, označující potřebu jejich ochrany.

Measure of importance assigned to information by the owner of the information, describing the need for protection.

Cloud computing **Cloud computing**

Způsob využití výpočetní techniky, kde jsou škálovatelné a pružné IT funkce zpřístupněné uživatelům jako služba. Výhody cloudů: snadný upgrade softwaru, nenáročné klientské stanice a software, levný přístup k mohutnému výpočetnímu výkonu bez nutnosti investic do HW, garantovaná dostupnost. Nevýhody: k důvěrným datům má přístup i provozovatel cloudu.

Mode of utilisation of computing technology whereby scalable and flexible IT functions are accessible to users as a service. The advantage of clouds: easy software upgrade, unsophisticated client stations and software, cheap access to a mighty computing power without hardware investments, guaranteed availability. Disadvantages: confidential data are available also to the cloud provider.

COBIT **Control Objectives for Information and Related Technology (COBIT)**

Správa cílů pro informační a s nimi spojené technologie (COBIT) je rámec, vytvořený ISACA pro řízení a vedení informačních technologií (IT). Jde o podpůrný soubor nástrojů, umožňující řídícím pracovníkům překlenout mezery mezi požadavky řízení, technickými otázkami a riziky podnikání.

Control Objectives for Information and Related Technology (COBIT) is a framework created by ISACA for information technology (IT) management and IT governance. It is a supporting toolset that allows managers to bridge the gap between control requirements, technical issues and business risks.

Cookie / HTTP cookie **Cookie / HTTP cookie**

Data předaná mezi HTTP serverem a prohlížečem za účelem uchování stavové informace na straně klienta, která může být později vyzvednuta a využita http serverem. Cookie se dnes nejčastěji používá pro rozpoznání uživatele, který již aplikaci dříve navštívil, nebo pro ukládání uživatelského nastavení webové aplikace. Dnes jsou často diskutovány v souvislosti se sledováním pohybu a zvyklostí uživatelů některými weby.

Data exchanged between an HTTP server and a browser to store state information on the client side and retrieve it later for HTTP server use. A cookie is at present mostly used for the recognition of a user who visited the application before, or for storing user setting of the web application. Nowadays, discussions are underway about cookies in connection to watching the movements and habits of users by some webs.

Crack **Crack**

Neoprávněné porušení zabezpečení či ochrany programu nebo systému, jeho integrity nebo systému jeho registrace / aktivace.

Unauthorised infringement of programme or system security protection, its integrity or system of its registration/activation.

Cracker **Cracker**

Jednotlivec, který se pokouší získat neoprávněný přístup k počítačovému systému. Tito jednotlivci jsou často škodliví a mají prostředky, které mají k dispozici pro prolamování se do systému.

An individual trying to obtain an unauthorised access to a computer system. These individuals are often harmful and possess means for breaking into a system.

CRAMM **CRAMM**

Metoda analýzy a řízení rizik (CRAMM, CCTA Risk Analysis and Management Method) je nyní v páté verzi, CRAMM Version 5.0. CRAMM má tři etapy a každá z nich má dotazníky na cíle a má návody. První dvě etapy identifikují a analyzují systémová rizika. Třetí etapa doporučuje, jak tato rizika řídit.

CRAMM (CCTA Risk Analysis and Management Method) is a risk management methodology, currently on its fifth version, CRAMM Version 5.0. CRAMM comprises three stages, each supported by objective questionnaires and guidelines. The first two stages identify and analyse the risks to the system. The third stage recommends how these risks should be managed.

Creative commons **Creative commons (CC)**

Nezisková organizace se sídlem v Mountain View, Kalifornie, Spojené Státy, která se věnuje rozšiřování rozsahu kreativních děl tak, aby i jiní na nich mohli legálně stavět a sdílet je. Organizace již uvolnila zdarma veřejnosti několik licencí na autorská práva, známých jako Creative commons.

A non-profit organisation headquartered in Mountain View, California, United States devoted to expanding the range of creative works available for others to build upon legally and to share. The organisation has released several copyrights – licenses known as Creative Commons licenses free of charge to the public

Cross-site scripting **Cross-site scripting (XSS)**

Útok na webové aplikace spočívající v nalezení bezpečnostní chyby v aplikaci a jejího využití k vložení vlastního kódu. Vložený kód se obvykle snaží získat osobní informace uživatelů, obsah databáze či obejít bezpečnostní prvky aplikace.

The attack on web applications consisting in an attempt to find a security error in the application and using this for the insertion of own code. The inserted code usually tries to get personal data of users, the content of the database or to bypass the security elements of an application.

Cvičení, procvičování **Exercise, skill training**

Proces výcviku pro posouzení, prověření a zlepšování výkonnosti.

Process of training to assess, verify and improve performance.

Časovaná bomba **Time bomb**

Logická bomba aktivovaná v předem určený čas.

Logical bomb activated at a predetermined time.

Časové razítko **Time-stamp**

Časový parametr, který označuje časový okamžik vzhledem ke společnému referenčnímu času.

Time variant parameter which denotes a point in time with respect to a common time reference.

Časový hlídač **Watchdog timer**

Elektronický časovač, který se používá pro zjištění a obnovu po počítačových chybách. V průběhu normální činnosti počítač pravidelně spouští časovač, aby zabránil uplynutí času do konce jeho činnosti neboli jeho "vyčasování". Jakmile však z důvodů buďto technické nebo programové chyby počítač znovu nespustí časovač, časovač se vypne a vydá signál o přerušení. Tento signál o přerušení se používá pro zahájení nápravy nebo náprav. Takové typické nápravy jsou uvedení počítače do bezpečného stavu a obnova normální činnosti systému.

An electronic timer that is used to detect and recover from computer malfunctions. During normal operation, the computer regularly restarts the watchdog timer to prevent it from elapsing, or "timing out". If due to a hardware fault or program error, the computer fails to restart the watchdog, the timer will elapse and generate a timeout signal. The timeout signal is used to initiate corrective action or actions. The corrective actions typically include placing the computer system in a safe state and restoring normal system operation.

Červ **Worm**

Autonomní program (podmnožina **Malware**), schopný vytvářet své kopie, které rozesílá do dalších počítačových systémů (sítí), kde vyvíjí další činnost, pro kterou byl naprogramován. Často slouží ke hledání bezpečnostních skulin v systémech nebo v poštovních programech.

*Autonomous programme (a subset of **Malware**) capable of creating its copies which, it then sends out to other computer systems (networks), where these pursue further activities they have been programmed for. Often it may serve to detect security holes in systems or mail programmes.*

Český kyberprostor **Czech cyberspace**

Kyberprostor pod jurisdikcí České republiky.

Cyberspace under the jurisdiction of the Czech Republic.

Černá listina **Blacklist**

Viz **Blacklist.**

*See **Blacklist.***

Čidlo **Sensor**

Více ***Senzor***.

*See **Sensor**.*

Člověk uprostřed **Man in the middle (MITM)**

Útok, v rámci něhož je útočník schopen číst, vkládat a upravovat zprávy přenášené mezi dvěma komunikujícími stranami, aniž by si toho komunikující strany byly vědomy.

Attack in which an attacker is able to read, insert, and modify messages between two communicating parties without their awareness.

DarkWeb **DarkWeb**

Překryvná síť, která využívá síť Internet, ale vyžaduje zvláštní software (např. TOR browser, Freenet, I2P anonymous network, apod.), konfiguraci, nebo autorizaci.

An overlay network that uses the Internet but requires specific software (e.g. TOR browser, Freenet, I2P anonymous network, etc.), configurations, or authorization.

Historian **Data Historian**

Centralizovaná databáze s podporou analýzy dat pomocí statistických postupů pro analýzu procesů.

A centralized database with the support of data analysis using statistical procedures to analyse processes.

Databáze **Database**

Souhrn dat uspořádaný podle pojmové struktury, v níž jsou popsány vlastnosti těchto dat a vztahy mezi odpovídajícími entitami, slouží pro jednu nebo více aplikačních oblastí.

Set of data arranged by a notional structure, which describes properties of these data and relations among corresponding entities, serves one or more application areas.

Datová dioda **Data diode**

Zařízení pro automatickou jednosměrnou komunikaci v kritických systémech. Datová dioda umožňuje přenos dat ze systému s nižším zabezpečením do systému s vyšším zabezpečením.

Data diode is a device to provide for automatic unidirectional communication in critical systems. Data diode allows transfer of data from a system with lower security to a system with higher security.

Datové centrum **Data centre**

Datové centrum je zařízení pro umístění počítačových systémů a souvisejících součástí, jako například telekomunikace a systémy pro ukládání dat. V obecnosti sem patří redundantní nebo zálohovací napájecí zdroje, redundantní datové komunikace, prostředky pro správu prostředí (například klimatizace, protipožární ochrana), a různá bezpečnostní zařízení.

A data center is a facility used to house computer systems and associated components, such as telecommunications and storage systems. It generally includes redundant or backup power supplies, redundant data communications connections, environmental controls (e.g., air conditioning, fire suppression) and various security devices.

Dávkové viry **Batch viruses**

Počítačové viry vytvářené pomocí dávkových souborů. Zajímavá možnost pro některé operační systémy (např. UNIX), ale existují i pro MS-DOS. Nejsou příliš rozšířené a jsou spíše raritou.

Computer viruses created using batch files. An interesting possibility for some operating systems (e.g. UNIX), exist however even for MS-DOS. They are not too widespread and are more of a rarity.

Dávkové zpracování **Batch Processing**

Spouštění jednoho nebo vice programů pomocí skriptů.

Running one or more programmes using scripts.

Definice virů **Virus Definitions**

Předefinované podpisy známých škodlivých programů používané detekčními algoritmy antivirů.

Predefined signatures for known malware used by antivirus detection algorithms.

Demilitarizovaná zóna **Demilitarized zone (DMZ)**

Obvodová síť, která plní funkci „neutrálního území“ mezi dvěma sítěmi, nejčastěji mezi vnitřní sítí organizace a internetem. V demilitarizované zóně jsou zpravidla soustředěny služby poskytované někomu z okolí, případně celému internetu. Tyto vnější (veřejné) služby jsou obvykle nejsnazším cílem internetového útoku; úspěšný útočník se ale dostane pouze do DMZ, nikoliv přímo do vnitřní sítě organizace.

Perimeter network (also known as a screened sub-net) inserted as a "neutral zone" between networks. DMZ concentrates services provided to someone in the neighbourhood or the whole internet. These external (public) services are usually the easiest target of an internet attack; a successful attacker however only gets to DMZ, not straight into the internal network of the organisation.

DES **Data Encryption Standard (DES)**

Data Encryptor Standard je symetrický blokový šifrovací algoritmus. Jedná se o veřejně dostupný standard s délkou klíče 56 bit. Více také ***3DES***.

*Data Encryption Standard is a symmetric block enciphering algorithm. It is a publicly available standard with key length of 56 bits. See also **3DES** for more.*

Dešifrování, rozšifrování **Decryption, deciphering**

Opačný proces k šifrování.

Reverse process to encryption.

Detekce anomálního chování sítě **Network Behavior Anomaly Detection (NBAD)**

Řešení pro pomoc při obraně proti útokům zero-day. NBAD je integrální částí analýzy chování sítě, která poskytuje bezpečnost kromě bezpečnosti již posytované tradičními aplikacemi proti hrozbám, jako jsou ***firewall***, antivirový software a software pro zjišťování spyware.

A solution for helping protection against zero-day attacks. NBAD is an integral part of network behaviour analysis, which offers security in addition to that provided by traditional anti-threat applications such as firewalls, antivirus software and spyware-detection software.

Detekce manipulace **Manipulation detection**

Postup, který je použít ke zjištění, zda data nebyla modifikována, ať už náhodně nebo záměrně.

Procedure to ascertain whether data were modified, either by accident or by design.

Detekce průniku **Intrusion detection**

Formalizovaný process detekce průniků, obecně charakterizovný získáváním poznatků o neobvyklých vzorcích využití HW a SW prostředků, včetně rozpoznání, která zranitelnost byla využita, jakým způsobem a kdy se to stalo.

The formalised process of detecting intrusions, generally characterised by gathering knowledge about abnormal usage patterns using HW and SW means, including the recognition which vulnerability was used, how and when it happened.

Diagnostická informace **Diagnostic information**

Informace o známých chybových stavech a jejich vlastnostech. Tuto informaci lze využít při testování a analýze závad k určení příčiny závady a k nalezení vhodných nápravných opatření.

Information concerning known failure modes and their characteristics. Such information can be used in troubleshooting and failure analysis to help pinpoint the cause of a failure and help define suitable corrective measures.

Dialer **Dialler**

Škodlivý program, který připojuje počítač nebo chytrý telefon uživatele k Internetu komutovanou linkou prostřednictvím velmi drahého poskytovatele připojení (obvykle útočníka).

The harmful programme which connects the computer or smartphone of the user to the Internet by a commuted line using a very expensive service provider (usually of the attacker).

Digitální důkaz **Digital evidence**

Informace nebo data uložená nebo přenášená v binární podobě, u nichž bylo v procesu analýzy zjištěno, že jsou relevantní pro vyšetřování. Poznámka: Toto by nemělo být zaměňováno s legálními digitálními důkazy nebo potenciálními digitálními důkazy.

Information or data, stored or transmitted in binary form which has been determined, through the process of analysis, to be relevant to the investigation. Note: This should not be confused with legal digital evidence or potential digital evidence.

Digitální podpis **Digital signature**

Elektronický podpis neoddělitelně spojený se zprávou kryptografickými prostředky tak, že umožňuje ověřit totožnost autora zprávy i její integritu a chrání tak zprávu proti padělání, například příjemcem. Digitální podpis často využívá asymetrické kryptografie (podpis je vytvořen pomocí soukromého klíče autora a je ověřován veřejným klíčem autora).

An electronic signature is inseparably linked cryptographically to the message so that it makes it possible to verify the identity of the author and the message integrity and thus protect the message against forgery by, say, the recipient. A digital signature is often used by asymmetric cryptography (the signature is created using a private key of the author and is verified by the public key of the author).

Dispečerské řízení a sběr dat / SCADA **Supervisory control and data acquisition (SCADA)**

Počítačový systém pro dispečerské řízení a sběr údajů. Mohou to být průmyslové řídicí systémy, nebo počítačové systémy monitorování a řízení procesů. Procesy mohou být průmyslové (např. výroba elektrické energie, výroba a rafinace PHM), infrastrukturní (např. úprava a rozvod pitné vody, odvádění a čištění odpadních vod, ropovody a plynovody, civilní systémy protivzdušné obrany – sirény, a velké komunikační systémy) a zařízení (např. letiště, železniční stanice a uzly).

A computer system for dispatcher control and data acquisition. It could be industrial control systems or computer systems for monitoring and process control. The processes could be industrial ones (e.g. electrical energy generation, manufacture and purification of fuel), infrastructural (e.g. treatment and distribution of drinking water, taking away and purification of sewage, oil and gas pipes, civilian systems of antiaircraft defence – sirens, and large communication systems), and facilities (e.g. airports, railway stations and hubs).

Digitální zařízení **Digital device**

Elektronické zařízení používané ke zpracování nebo ukládání digitálních dat.

Electronic equipment used to process or store digital data.

Dodavatel **Supplier**

Organizace nebo fyzická osoba, která uzavře s nabyvatelem smlouvu o dodávce výrobku nebo služby. Poznámka: Další běžně používané termíny pro dodavatele jsou kontrahent, výrobce, prodávající nebo prodejce. Nabyvatel a dodavatel mohou být součástí téže organizace. Mezi typy dodavatelů patří organizace, které umožňují sjednání dohody s nabyvatelem, a organizace, které sjednání dohody neumožňují, např. licenční smlouvy s koncovým uživatelem, podmínky použití nebo uvolnění autorských práv nebo duševního vlastnictví k produktům s otevřeným zdrojovým kódem.

Organization or an individual that enters into agreement with the acquirer for the supply of a product or service. Note: Other terms commonly used for supplier are contractor, producer, seller, or vendor. The acquirer and the supplier can be part of the same organization. Types of suppliers include those organizations that permit agreement negotiation with an acquirer and those that do not permit negotiation with agreements, e.g. end-user license agreements, terms of use, or open source products copyright or intellectual property releases.

Dodavatelský řetězec **Supply chain**

Soubor organizací s propojeným souborem zdrojů a procesů, z nichž každá vystupuje jako nabyvatel, dodavatel nebo obojí a vytváří postupné dodavatelské vztahy navázané na základě objednávky, smlouvy nebo jiné formální dohody o dodávkách. Poznámka: Dodavatelský řetězec může zahrnovat prodejce, výrobní zařízení, poskytovatele logistických služeb, distribuční centra, distributory, velkoobchodníky a další organizace podílející se na výrobě, zpracování, návrhu a vývoji a manipulaci s výrobky a jejich dodávkách nebo poskytovatele služeb

podílející se na provozu, řízení a dodávkách služeb. Pohled na dodavatelský řetězec je relativní vzhledem k postavení nabyvatele.

Set of organizations with linked set of resources and processes, each of which acts as an acquirer, supplier, or both to form successive supplier relationships established upon placement of a purchase order, agreement, or other formal sourcing agreement. Note: A supply chain can include vendors, manufacturing facilities, logistics providers, distribution centres, distributors, wholesalers, and other organizations involved in the manufacturing, processing, design and development, and handling and delivery of the products, or service providers involved in the operation, management, and delivery of the services. The supply chain view is relative to the position of the acquirer.

Diskrétní (nespojité) zpracování **Discrete Processing**

Druh zpracování, ve které se konkrétní množství materiálu přesouvá jako samostatná jednotka (součást skupiny jednotek) mezi pracovními místy, a každá tato jednotka je samostatně identifikována.

A type of procesings where a specified quantity of material moves as an independent unit (part of group of parts) among workplaces and each unit maintains its unique identity.

Dispečerské řízení **Supervisory Control**

Řídicí proces, kdy výstup jedné řídící jednotky nebo počítače je použit jako vstup pro jiné řídicí jednotky. Viz Řídicí server

Control process when the output of one control unit or computer is used as input to another control unit. See Control Server.

Distribuované odmítnutí služby **Distributed denial of service (DDoS)**

Distribuované odmítnutí služby je technika útoku na internetové služby nebo stránky, při níž dochází k přehlcení požadavky a k pádu nebo nefunkčnosti a nedostupnosti systému pro ostatní uživatele a to útokem mnoha koordinovaných útočníků.

Distributed denial of service is the technique of attack by many coordinated attackers on the internet services or pages resulting in flooding by requests or breakdown or unfunctionality or unavailability of the system for other users.

Distribuované výpočetní prostředí **Distributed computing environment (DCE)**

Programový systém vyvinutý na počátku devadesátých let konsorciem zahrnujícím Apollo Computer (později část Hewlett-Packard), IBM, Digital Equipment Corporation, a jinými. DCE poskytuje rámec a soubor nástrojů pro vyvíjení aplikací klient/server.

A software system developed in the early 1990s by a consortium that included Apollo Computer (later part of Hewlett-Packard), IBM, Digital Equipment Corporation, and others. The DCE supplies a framework and toolkit for developing client/server applications.

Distribuovaný řídicí systém — **Distributed Control System (DCS)**

Řídicí systém, jehož řídicí jednotky jsou rozmísteny na vice místech a společně působí na určitý proces.

A control system whose control units are placed in several locations and jointly influence a specific process.

Distribuovaná výroba — **Distributed manufacturing**

Geograficky odloučený závod, který je určitému podniku dostupný prostřednictvím internetu.

A geographically separate plant that is accessible through the Internet to a specific enterprise.

DNS server — **Domain name system server (DNS server)**

Distribuovaný hierarchický jmenný systém používaný v síti Internet. Překládá názvy domén na číselné IP adresy a zpět, obsahuje informace o tom, které stroje poskytují příslušnou službu (např. přijímají elektronickou poštu či zobrazují obsah webových prezentací) atd.

Distributed hierarchical name system used in the Internet network. It translates the names of domains to numerical IP addresses and back, contains information about which machines provide the relevant service (e.g. receive emails or show the content of web applications) etc.

Doba cyklu, čas cyklu — **Cycle Time, period time**

Čas, zpravidla vyjádřený v sekundách, za který řídicí jednotka dokončí jednu řídicí smyčku (načtení signálů ze senzorů do paměti, vyhodnocení řídicích algoritmů,

odeslání řídicích signálů do akčních členů, regulace procesu, odeslání nových signálů senzory).

Time, usually in seconds, in which the control unit completes one control loop (reading sensor data to memory, evaluation of control algorithms, the output of control signals to actuators, process regulation, the input of new signals from sensors).

Doba obnovy chodu **Recovery time objective (RTO)**

Časový interval následující po incidentu, během kterého musí být produkt nebo služba obnoveny nebo činnost obnovena nebo zdroje nahrazeny.

A period of time following an incident within which product or service must be resumed or activity must be resumed or resources must be recovered.

Doba platnosti klíče **Key validity period**

Časový interval, po který může být kryptografický klíč použit k šifrování nebo dešifrování dat. Po ukončení platnosti klíče může být stanoven „čas překrytí“ / „extension period“, po který je možno klíč použít pro dešifrování dat.

The time period during which a cryptographic key may be used to encipher or decipher data. After the expiration of key validity, an extension period may be defined to use the key for data deciphering.

Dohoda **Agreement**

Vzájemné odsouhlasení si podmínek a okolností, za kterých je realizován určitý pracovní vztah.

Mutual acknowledgement of terms and conditions under which a working relationship is conducted.

Dokumentovaná informace **Documented information**

Informace, která má organizace řídit a udržovat, včetně médií, na kterých jsou uloženy.

Information required to be controlled and maintained by an organisation and the medium on which it is contained.

Doména **Domain**

(1) Soubor prvků provozovaných pod jednotnou bezpečnostní politikou, např. pod certifikátem veřejného klíče vytvořeným jednou autoritou nebo více autoritami pomocí jedné bezpečnostní politiky.
(2) Určité prostředí, nebo určitý kontext, který zahrnuje sadu systémových zdrojů a sadu systémových prvků, které mají právo využívat zdroje na základě společné bezpečnostní politiky, bezpečnostního modelu nebo bezpečnostní architektury

(1) Set of entities operating under a single security policy, e.g. public key certificates created by a single authority or by a set of authorities using the same security policy.
(2) An environment or context that includes a set of system resources and a set of system entities that have the right to access the resources as defined by a common security policy, security model, or security architecture.

Doména nejvyšší úrovně **Top level domain (TLD)**

Internetová doména na nejvyšší úrovni stromu internetových domén. V doménovém jméně je doména nejvyšší úrovně uvedena na konci (např. u nic.cz je doménou nejvyššího řádu cz). Domény nejvyššího řádu jsou pevně stanoveny internetovou standardizační organizací **IANA:**
a) Národní **TLD** (country-code **TLD**, ccTLD) sdružující domény jednoho státu. Jejich název je dvoupísmenný, až na výjimky odpovídající kódu země podle ISO 3166-1, např. cz pro Českou republiku;
b) Generické **TLD** (generic **TLD**, gTLD) společná pro daný typ subjektů (např. aero, biz, com, info, museum, org,…), nespojené s jedním konkrétním státem (až na výjimku **TLD** mil a gov, které jsou z historických důvodů vyhrazeny pro vojenské, resp. vládní počítačové sítě v USA);
c) Infrastrukturní **TLD** využívané pro vnitřní mechanismy Internetu. V současné době existuje jediná taková **TLD**: arpa, používaná systémem **DNS**.

This is the internet domain at the highest level in the tree of internet domains. In the domain name, top-level domain is given at the end (e.g. in nic.cz, CZ is the top level domain). Top-level domains are fixed by the internet standards organisation IANA:
a) National TLD (country-code TLD, ccTLD) unites domains in one country. Their name has two letters, with exceptions corresponding to country code per ISO 3166-1, e.g. CZ for the Czech Republic;
b) Generic TLD (generic TLD, gTLD) is common for a given type of subjects (e.g. aero, biz, com, info, museum, org,...) not tied to one concrete country (with exceptions TLD mil and gov which out of historical reasons are assigned for military and government computer networks in the U.S.A.);

c) Infrastructure TLD used for the internal mechanisms of the internet. At present, there is just one such TLD: arpa, used by the DNS system

Doménové jméno **Domain name**

Název, který identifikuje počítač, zařízení nebo službu v síti (včetně internetu). Příklad doménového jména: www.afcea.cz.

Name to identify a computer, equipment or service in the network (including the Internet). Example of a domain name: www.afcea.cz.

Doménové pirátství **Cybersquatting**

Registrace doménového jména souvisejícího se jménem nebo obchodní známkou jiné společnosti za účelem následného nabízení domény této společnosti za vysokou finanční částku.

Registration of the domain name related to the name or trademark of another company, with the purpose of subsequent offering the domain to this company at a high financial amount.

Dopad **Impact**

(1) Nepříznivá změna dosaženého stupně cílů.
(2) Následky určitého činu nebo události.

(1) Adverse change in the attained degree of objectives.
(2) Consequenses of a certain act or event.

Dost dobré soukromí **Pretty good privacy (PGP)**

Mechanismus/program umožňující šifrování a podepisování dat. Nejtypičtěji se používá pro šifrování obsahu zpráv (e-mailů) a pro vybavení těchto zpráv elektronickým (digitálním) podpisem.

Mechanism/programme enabling encryption and signature of data. Most typically it is used for encrypting the content of messages (emails) and for providing these messages with an electronic signature.

Dostupnost **Availability**

Vlastnost přístupnosti a použitelnosti na žádost oprávněné entity.

Property of being accessible and usable upon demand by an authorised entity.

Dotaz **Request**

Žádost o informace, obecně jako formální žádost zaslaná databázi nebo do vyhledávače nebo signál z jednoho počítače do druhého, nebo na server s žádostí o konkrétní informaci nebo údaj.

Request for information, in general as a formal request sent to a database or to a browser, or a signal from one computer to another, or to a server with the request for concrete information or data item.

Doxingware **Doxingware**

Druh ransomware, doplněný o metody získání obsahu souborů a hrozbu prozrazení takto získaných souborů, společně s hrozbou medializace kauzy a zveřejnění jména napadené osoby či společnosti.

A type of ransomware, which includes methods for collecting file contents and a threat of disclosing these files together with a threat of mediatisation and disclosing the name of the attacked person or organisation.

Důkaz **Evidence**

Informace, které se používají buď samy o sobě, nebo ve spojení s jinými informacemi k prokázání události nebo činnosti. Poznámka: svědectví nemusí nutně dokazovat pravdivost nebo existenci něčeho, ale může přispět k vytvoření takového důkazu.

Information which is used, either by itself or in conjunction with other information, to establish proof about an event or action. Note: Evidence does not necessarily prove the truth or existence of something, but can contribute to the establishment of such a proof.

Důvěrná informace **Confidential information**

Informace, které by neměly být zpřístupněny nebo sděleny neoprávněným osobám, subjektům nebo procesům.

Information that should not be made available or disclosed to unauthorized individuals, entities or processes.

Důvěrnost **Confidentiality**

Vlastnost, že informace není dostupná nebo není odhalena neoprávněným jednotlivcům, entitám nebo procesům.

Property that information is not made available or disclosed to unauthorised individuals, entities or processes.

Důvěryhodná třetí strana **Trusted third party (TTP)**

Služba poskytující důkaz, že datová položka existovala před určitým časovým okamžikem.

Security authority, or its agent, trusted by other entities with respect to security-related activities.

Důvěryhodný počítačový systém **Trusted computer system**

Systém zpracování dat, který poskytuje dostatečnou počítačovou bezpečnost na to, aby umožnil souběžný přístup k datům uživatelům s odlišnými přístupovými právy a k datům s odlišnou bezpečnostní klasifikací a bezpečnostními kategoriemi.

Data processing system having sufficient computer security to allow for a concurrent access to data to users with different access rights and to data with different security classification and security categories.

Efektivnost, účelnost **Effectiveness, usefulness**

Rozsah, ve kterém jsou realizovány plánované činnosti a dosaženy plánované výsledky.

Extent to which planned activities are realized and planned results achieved.

Elektromagnetická analýza **Electromagnetic analysis (EMA)**

Analýza elektromagnetického pole vyzařovaného kryptografickým modulem v důsledku spínání jeho logických obvodů za účelem získání informací souvisejících s činností bezpečnostní funkce a následně hodnot tajných parametrů, jako jsou kryptografické klíče.

Analysis of the electromagnetic field emanated from a cryptographic module as the result of its logic circuit switching, for the purpose of extracting information correlated to security function operation and subsequently the values of secret parameters such as cryptographic keys.

Elektromagnetické kompromitující vyzařování **Electromagnetic compromising emanations (EME)**

Zpravodajský signál, který v případě zachycení a analýzy potenciálně odhaluje informace, které jsou vysílány, přijímány, manipulovány nebo jinak zpracovávány jakýmkoli zařízením pro zpracování informací.

Intelligence-bearing signal, which, if intercepted and analysed, potentially discloses the information that is transmitted, received, handled, or otherwise processed by any information-processing equipment.

Elektromagnetický ventil **Electromagnetic valve**

Ventil ovádaný elektromagnetickou cívkou, má zpravidla pouze dva stavy: otevřeno a zavřeno.

A valve actuated by an electromagnetic coil, typically with only two states: open and closed.

Elektronická obrana **Electronic defence**

Použití elektromagnetické energie k poskytnutí ochrany a k zajištění užitečného využití elektromagnetického spektra (zahrnuje ochranu sil, prostorů apod.).

Use of electromagnetic energy to provide protection and to secure useful utilisation of the electromagnetic spectrum (includes protection of forces, spaces, etc.).

Elektronické paměťové médium **Electronic storage medium**

Zařízení, na které lze nahrát datové soubory a přenášet je mezi počítači.

A device, on which data files may be recorded and transferred among computers.

Elektronická pošta **Electronic mail (email)**

Textová, hlasová, zvuková nebo obrazová zpráva poslaná prostřednictvím veřejné sítě elektronických komunikací, která může být uložena v síti nebo v koncovém zařízení uživatele, dokud ji uživatel nevyzvedne.

Text, voice or picture message sent using public network of electronic communications, which can be stored in the network or enduser terminal until collected by the user.

Elektronické prostředky **Electronic means**

Zejména síť elektronických komunikací, elektronická komunikační zařízení, koncová zařízení, automatické volací a komunikační systémy, telekomunikační a elektronická pošta.

Primarily a network of electronic communications, electronic communication equipment, terminals, automatic call and communication systems, telecommunication and electronic mail.

Elektronický archiv **Electronic archive**

Dlouhodobé úložiště informací uchovávaných v elektronické podobě. Elektronické archivy mohou být přístupné online nebo off-line. Záložní systémy (např. pásky, virtuální pásky atd.) nejsou považovány za elektronické archivy, ale spíše za systémy pro ochranu dat (tj. mechanismy obnovy dat po havárii a zajištění kontinuity provozu).

Long-term repository of electronically stored information. Electronic archives can be accessed online or offline. Backup systems (e.g. tape, virtual tape, etc.) are not considered to be electronic archives, but rather data protection systems (i.e. mechanisms for disaster recovery and business continuity).

Elektronický boj **Electronic warfare**

Vojenská činnost, která využívá elektromagnetické energii na podporu útočných a obranných akcí k dosažení útočné a obranné převahy. Je to vedení boje v prostředí používajícím elektromagnetické záření. Je samostatnou disciplínou, ale jako jeden z prvků působí na podporu kybernetické obrany v rámci **NNEC**.

*Military activity using electromagnetic energy in support of offensive and defensive actions in order to achieve offensive and defensive supremacy. This means engaging in fighting in the environment using electromagnetic radiation. It is a separate discipline but as one of the elements, it supports cyber security within **NNEC**.*

Elektronický důkaz **Electronic evidence**

Informace nebo data uložená či přenášená v binárním tvaru, na které je možné se spolehnout jako na důkaz.

Information or data, stored or transmitted in binary form that may be relied on as evidence.

Elektronický podpis **Electronic signature**

Podpis učiněný elektronickou formou, který má stejnou právní váhu jako vlastnoruční podpis, splňuje-li zákonné podmínky (např. eIDAS v EU, NIST-DSS v USA nebo ZertES ve Švýcarsku). Na rozdíl od ***Digitálního podpisu***, který je založen na kryptografických prostředcích, je elektronický podpis právní koncept.

*A signature made in an electronic form that has the same legal effect as a handwritten signature, if legal conditions are met (e.g. eIDAS in EU, NIST-DSS in the USA or ZertES in Switzerland). Unlike the **Digital signature,** which is based on cryptography, the electronic signature is a legal concept.*

Elektronicky uložená informace **Electronically Stored Information (ESI)**

Jakákoliv data nebo informace z libovolného zdroje, jejichž existence v určitém čase je prokázána uložením na elektronickém médiu. Například jde o e-maily, poznámky, dopisy, tabulky, databáze, dokumenty, prezentace a ostatní elektronické formáty, které se běžně nacházejí na počítači, ale i operační systém, aplikace a metadata spojená se soubory (např. časové značky, historii změn, typ souboru atd.)

Data or information of any kind and from any source, whose temporal existence is evidenced by being stored in, or on, any electronic medium. ESI includes traditional e-mail, memos, letters, spreadsheets, databases, office documents, presentations, and other electronic formats commonly found on a computer. ESI also includes operating systems, applications, and file-associated metadata (such as timestamps, revision history, file type, etc.).

Elektronický útok **Electronic attack**

Použití elektromagnetické energie pro účely útoku. Zahrnuje zbraně se směrovanou energií, vysoce výkonné mikrovlnné a elektromagnetické pulsy a RF zařízení.

Use of electromagnetic energy for the purposes of an attack. Includes weapons with directed energy, high-power microwave and electromagnetic pulses and RF equipment.

Eliptická křivka **Elliptic curve**

Kubická křivka E bez singulárního bodu. Poznámka: Množina bodů E spolu s vhodně definovanou operací pro pole, které zahrnuje všechny koeficienty rovnice popisující E, se nazývá definiční pole E. Tvar rovnice kubické křivky použité k definici eliptické křivky se liší v závislosti na poli.

Cubic curve E without a singular point. Note: The set of points E together with an appropriately defined operation for a field that includes all coefficients of the

equation describing E is called the definition field of E. The form of a cubic curve equation used to define an elliptic curve varies depending on the field.

Emulace **Emulation**

Použití systému zpracování dat k napodobení jiného systému zpracování dat; napodobující systém přijímá stejná data, provádí stejné programy a vykazuje stejné výsledky jako napodobovaný systém.

Use of a data processing system to emulate another data processing system; emulating system receives the same data, runs the same programmes and exhibits the same results as the emulated system.

Energeticky nezávislé úložiště *Energy-independent storage*

Úložiště, které uchová svůj obsah i v případě odpojení elektrické energie.

Storage that retains its contents even after power is removed.

Entita **Entity**

Určitá osoba, skupina, zařízení nebo proces.

A specific person, group, device or process.

Evropská kritická infrastruktura **European critical infrastructure**

Kritická infrastruktura na území České republiky, jejíž narušení by mělo závažný dopad i na další členský stát Evropské unie.

Critical infrastructure in the territory of the Czech Republic whose infringement would result in a serious impact also on another member of the European Union.

Extranet **Extranet**

Rozšíření intranetu organizace, zejména prostřednictvím veřejné síťové infrastruktury, které umožňuje sdílení zdrojů mezi organizací a dalšími organizacemi či osobami, které nemají plný přístup do intranetu organizace.

Extension of an organisation's Intranet, especially over the public network infrastructure, enabling resource sharing between the organisation and other organisations and individuals that it deals with by providing limited access to its Intranet.

Failover **Failover**

Automatické přepnutí na záložní systém či proces v okamžiku selhání předchozího pro dosažení velmi krátké doby výpadku a zvýšení spolehlivosti.

Automatic switch to a backup system or process at the instant of failure of the previous one in order to achieve a very short time of outage and increase in reliability.

Falešné ticho, chybné zamítnutí **False negative**

IDPS systém nehlásí žádný poplach v okamžiku, kdy probíhá útok.

IDPS system reports no alert when there is an attack.

Falešný poplach, chybné přijetí **False positive**

IDPS systém hlásí poplach v okamžiku, kdy neprobíhá žádný útok.

IDPS system reports an alert when there is no attack.

Federovaná identita **Federated identity**

Identita, kterou lze využít ve vice doménách, a která obsahuje vice totožností.

Identity for use in multiple domains, and which contains more identities.

File transfer protocol **File transfer protocol (FTP)**

Internetový standard (RFC 959) pro přenos souborů mezi klientem a serverem.

An Internet standard (RFC 959) for transferring files between a client and a server.

Firewall **Firewall**

Bezpečnostní bariéra umístěná mezi dvě síťová prostředí – může být tvořena jedním zařízením, nebo souborem více komponent a technik – skrz kterou musí projít veškerý provoz z jedné sítě do druhé a obráceně, ale pouze provoz autorizovaný podle lokální bezpečnostní politiky je propuštěn skrz. Firewall může být softwarový i hardwarový nebo kombinace obojího.

*A security barrier placed between network environments — consisting of a dedicated device or a composite of several components and techniques — through which all traffic from one network environment traverses to another, and vice versa, and only authorised traffic, as defined by the local security policy, is allowed to pass. A **firewall** can be implemented as hardware or software, or a combination of both.*

Firmware **Firmware**

Program ovládající **hardware**.

*Programme controlling **hardware**.*

FIRST **Forum for incident response and security teams (FIRST)**

Celosvětově působící asociace, která spojuje přibližně 200 pracovišť typu **CSIRT** / **CERT**.

*Worldwide organisation uniting about 200 workplaces of the **CSIRT/CERT** type.*

Forenzní analýza / vyšetřování **Forensic analysis / investigation**

Vyšetřovací postup nad digitálními daty používaný k získávání důkazů o aktivitách uživatelů (útočníků) v oblasti informačních a komunikačních technologií.

Investigation procedures on digital data to obtain proofs about the activities of users (attackers) in the area of information and communication technologies.

Freeware **Freeware**

Proprietární software, který je obvykle distribuován bezplatně (či za symbolickou odměnu). Někdy hovoříme o typu softwarové licence. Podmínky bezplatného používání a šíření jsou definovány v licenční smlouvě. Autor si u freewaru zpravidla ponechává autorská práva.

Proprietary software usually distributed free (or for a symbolic reward). We speak sometimes about a kind of software licence. Conditions for the free use and distribution are defined in the licence agreement. The author of the freeware usually retains the copyright.

Function block (Funkční bloky) **Function Block**

Grafický programovací jazyk. Programování probíha spojováním funkčních bloků. Tato reprezentace je součást normy IEC 61113-3.

Graphic programming language. Programming is done by combining functional blocks. This representation is part of IEC 61113-3.

Fyzické aktivum **Physical asset**

Viz **Hmotný majetek**

*See **Physical asset***

Fyzické řízení přístupu **Physical access control**

Použití fyzických mechanizmů k zajištění řízení přístupu (např. umístění počítače v uzamčené místnosti). Více **Access Control**.

*Use of physical mechanisms to enable control of access (e.g. placing the computer in a locked room). See **Access Control**.*

Fyzikální generator náhodných čísel **Hardware (Physical) random number generator**

Hardwarové zařízení, které využívá náhodnost fyzikálního jevu (např. nepředvídatelnost chování atomárních a subatomárních procesů, náhodnost rozpadu radioaktivního materiálu nebo častěji náhodnost bílého šumu šumové diody) ke generování náhodné posloupnosti čísel. Takový generátor bývá označován jako „Pravý generátor náhodných čísel“ (TRNG).

A hardware device using the randomness of a physical phenomenon (for example, unpredictability in the behaviour of atomic and subatomic processes, randomness of radioactive material decay or more often the randomness of the white noise of a noise diode) to generate a random sequence of numbers. Such a generator is usually denoted as „true random number generator“ (TRNG).

Garant aktiva **Asset guarantor**

Definovaná bezpečnostní role v souladu se zákonem o kybernetické bezpečnosti, představující fyzickou osobu, pověřenou k zajištění rozvoje, použití a bezpečnosti aktiva. Jde o obdobnou roli, jakou je vlastník aktiva podle řady norem ISO/IEC 27 000.

Security role defined in accordance with the law on cyber security and representing a natural person commissioned to develop, utilise and secure an asset. It is a role similar to that of the asset owner in a number of standards ISO/IEC 27 000.

Garant aplikace **Application owner**

Více **Vlastník aplikace**.

*See **Application owner**.*

Generátor náhodných čísel **Random number generator (RBG)**

HW nebo SW zařízení (případně kombinace obojího), které generuje řadu náhodných čísel, které nemají žádnou vzájemnou závislost a není možno na základě vygenerovaných čísel předikovat následující číslo. Generátor může být založen na náhodném fyzikálním jevu nebo na okamžité náhodě zpracované matematickým algoritmem. Kvalita produkce generátoru náhodných čísel se ověřuje statistickou analýzou. Kvalita generátoru je rozhodující při generování např. symetrických kryptografických klíčů, na jejichž náhodnosti závisí bezpečnost šifrování.

An HW or SW device (or a combination of both) which generates a sequence of random numbers. These numbers are mutually independent, and it is impossible to predict the next number from the preceding ones. The generator can be based on a random physical phenomenon or a contingency processed by a mathematical algorithm. The quality of the random number generator is verified by statistical analysis. This quality is decisive in the generation of, for example, symmetric cryptographic keys, on whose randomness depends encryption security.

Generátor pseudonáhodných čísel **Pseudo-random number generator (CPRBG)**

Deterministický program, který generuje statisticky kvalitní posloupnost čísel. V důsledku determiničnosti těchto programů se generovaná posloupnost začne po určité periodě opakovat. Vstupními daty pro pseudonáhodné generátory jsou náhodné posloupnosti zvané „random seed“, které jednoznačně určují další běh programu (generátoru). Jako „random seed“ mohou být použita data získaná v HW systému (např. teplota, čas) nebo výstupní posloupnost z fyzikálního generátoru (TRNG).

A deterministic programme which generates a statistically random sequence of numbers. As such programmes are deterministic, the generated sequence starts to repeat itself with a period. Input data for the pseudo-random generators are random sequences called „random seed“, which uniquely determine the course of the programme (generator). Data obtained from an HW system (e.g., temperature,

time) or an output sequence from a physical generator (TRNG) can serve as the „random seed".

Generické TLD **Generic TLD**

Více **TLD**.

*See **TLD.***

Globální síť **Wide Area Network (WAN)**

Určitá fyzická nebo logická síť, která zprostředkovává datovou komunikaci většímu počtu nezávislých uživatelů, kteří obvykle využívají různé lokální sítě (LAN), a která se zpravidla rozkládá nad větší geografickou oblastí než LAN.

A physical or logical network that provides data communications to a larger number of independent users than are usually served by a local area network (LAN) and that is usually spread over a larger geographic area than that of a LAN.

GNU / GPL **GNU / GPL**

Všeobecná veřejná licence GNU – licence pro svobodný software vyžadující, aby byla odvozená díla dostupná pod stejnou licencí.

General public licence GNU – licence for free software requesting that related creations be available under the same licence.

GPG **GNU privacy guard (GPG)**

Bezplatná verze **PGP**. Viz **PGP**.

*Free version of **PGP**. See **PGP**.*

Grey hat **Grey hat**

Osoba, která podle své činnosti je něco mezi hackerem **White hat** a **Black hat**, protože zneužívá bezpečnostní slabinu systémů nebo produktu k tomu, aby veřejně upozornila na jejich zranitelnost. Avšak prozrazení takovýchto citlivých informací může být příležitostí k páchání trestné činnosti osobám typu **Black hat**.

*An individual who according to the activity stands between **White hat** and **Black hat** hackers, since the individual abuses security weakness of systems or a product to publicly draw attention to their vulnerability. However, publicising this sensitive*

information may be an opportunity for persons of the Black hat character to commit criminal acts.

Hack / Hacking **Hack / Hacking**

(1) Záměrné vniknutí do počítačového systému bez povolení od jeho uživatele nebo vlastníka.
(2) Podařené, neobvyklé, nápadité, či rychlé vyřešení problému využitím programu či počítačového systému způsobem, který jeho tvůrce nezamýšlel.

(1) Intentionally accessing a computer system without the authorisation of the user or the owner.
(2) A fitting, unusual, witty, or fast solution of an issue using a programme or a computer system in a way that its designer did not intend.

Hacker **Hacker**

Osoba:
(1) která se zabývá studiem a prozkoumáváním detailů programovatelných systémů nejčastěji pro intelektuální zvídavost a tuto schopnost si neustále zdokonaluje (White hat),
(2) kterou baví programování a která dobře a rychle programuje,
(3) která je expertem pro určitý operační systém nebo program, např. UNIX. Pojem Hacker se často nesprávně používá pro osoby, které zneužívají svých znalostí při pronikání do informačního systému a tak porušují zákon. Více **Cracker**.

Person:
(1) who engages in the study and analysis of details of programmable systems most often for an intellectual inquisitiveness and keeps on improving this ability (White hat);
(2) who enjoys programming and who programs well and fast;
*(3) who is an expert for a certain operating system or a programme, e.g. UNIX. The idea of Hacker is often improperly used for persons who abuse their knowledge during breaking into an information system and thus break the law. See **Cracker**.*

Hackers for hire **Hackers for hire (H4H)**

Akronym pro hackery, kteří nabízejí své služby jiným kriminálním, teroristickým nebo extremistickým skupinám (najmutí hackeři).

Acronym for hackers who offer their services to other criminal, terrorist or extremist groups (hired hackers).

Hactivismus **Hactivism**

Politicky nebo sociálně motivovaný Hacking.

Hacking for a politically or socially motivated purpose.

Hardwarový bezpečnostní modul **Hardware security module (HSM)**

Hardwarová implementace zabezpečeného kryptoprocesoru využívajícího certifikát a soukromý klíč k zajištění bezpečného ověřování.

Hardware implementation of a secure crypto-processor using an certificate and a private key to provide secure authentication.

Hash autentizační kód zprávy **Hash message authentication code (HMAC)**

Autentizační kód zprávy založený na funkci hash (více **Hash funkce**)

*Authentication code of a message based on a hash function (see **Hash function**).*

Hash funkce **Hash function**

Jednosměrná matematická transformace vstupních dat (textu) do souboru (otisk, hash). Matematicky je prakticky nereálné získat z otisku zpět vstupní data. Tato funkce je využívána v aplikacích zabezpečení dat (například autentizace, digitální podpis, kontrola integrity). Porušení bezpečnosti hash funkce je označováno jako kolize.

A one-way mathematical transformation of input data (text) into a file (digest, hash). It is computationally practically unrealistic to get the original data back from the hash return. This function is used in applications of data security (eg. authentication, digital signature, integrity check). Security infringement of a hash function is denoted a collision.

Havarijní plán **Contingency plan**

Plán pro záložní postupy, odezvu na nepředvídanou událost a obnovu po havárii.

Plan for backup procedures, response to an unforeseen event and recovery after a contingency.

Havarijní postup **Contingency procedure**

Postup, který je alternativou k normálnímu postupu zpracování pro případ, že nastane neobvyklá, ale předpokládaná situace.

Procedure, which is an alternative to the normal procedure in case of an occurrence of an unusual but assumed situation.

Heslo **Password**

Řetězec znaků používaný k ověření identity nebo k ověření oprávnění k přístupu.

String of characters used to authenticate an identity or to verify access authorisation.

High-tech kriminalita

Trestná činnost, v rámci které slouží vyspělá technika jako cíl, prostředí nebo nástroj pachatele. High-tech kriminalita může být chápána jako: (1) jakákoliv trestná činnost spáchaná pomocí vyspělé techniky, včetně případu, kdy je např. vyspělá technika použita při padělání peněz nebo cenných listin; (2) kybernetická kriminalita spáchaná pomocí vyspělé techniky, nebo proti vyspělé technice.

Criminal activity focused on advanced technology as the objective, means or instrument of the perpetrator. High-tech crime is considered: (1) any criminal activity using high technology, including the case when, for example, a computer system is used for money or securities counterfeiting; (2) cyber criminality using high technology or against high technology.

Hmotný majetek **Physical asset**

Hmatatelný majetek movitý i nemovitý. Hmotným majetkem se zpravidla myslí hotovost, zařízení, materiál a nemovitosti vlastněné jednotlivcem nebo organizací. Software je považován za majetek nehmotný.

Asset that has a tangible or material existence. Physical assets usually refer to cash, equipment, inventory and properties owned by the individual or organisation. Software is considered an intangible asset.

Hodnocení rizik **Risk evaluation**

Proces porovnání výsledků analýzy rizika s kritérii rizika k určení, zda riziko a/nebo jeho závažnost jsou přijatelná (akceptovatelná) nebo tolerovatelná.

Process of comparing the results of risk analysis with risk criteria to determine whether the risk and/or its magnitude is acceptable or tolerable.

Hodnocení zranitelností **Vulnerability assessment**

Proces identifikace, kvantifikace a prioritizace (nebo hodnocení) zranitelností systému.

Process of identifying, quantifying, and prioritising (or ranking) the vulnerabilities in a system.

Hodnocení zranitelností a řízení zranitelností **Vulnerability assessment and vulnerability management (VA/VM)**

Viz **Hodnocení zranitelností** a **Řízení zranitelností**.

*See **Vulnerability assessment** and **Vulnerability management**.*

Hodnota majetku **Assets value**

Objektivní vyjádření obecně vnímané hodnoty nebo subjektivní ocenění důležitosti (kritičnosti) majetku, popř. kombinace obou přístupů.

Objective expression of a generally perceived value or a subjective evaluation of the importance (criticality) of an asset, or a combination of both approaches.

Hodnotitel **Assessor**

Osoba, která vede a provádí posouzení dopadů na soukromí. Poznámka: hodnotiteli může v rámci jeho týmu pomáhat jeden nebo více dalších interních nebo externích odborníků.

Person who leads and conducts a privacy impact assessment. Note: The assessor may be supported by one or more other internal and/or external experts as part of their team.

Honeypot **Honeypot**

Obecný název pro systém, který se používá k nalákání útočníka a k jeho přesvědčení, aby strávil čas zpracováním informací, které se zdají být velmi hodnotné, ale ve skutečnosti jsou uměle vyrobené a pro oprávněného uživatele bezcenné.

Generic term for a decoy system used to lure the attacker to spend time on information that appears to be very valuable, but actually is fabricated and would not be of interest to a legitimate user.

Horká linka **Help desk**

On-line (zpravidla telefonická) služba, kterou nabízí automatizovaný informační systém a prostřednictvím které mohou uživatelé získat pomoc v oblasti použití společných či specializovaných služeb systému.

Online (as a rule, telephone) service offered by an automated information system and through which users can get help for using shared or specialised services of the system.

Host **Host**

Systém nebo počítač v TCP/IP síti, který má přidělenu síťovou adresu.

A system or computer in a TCP/IP-based network with an assigned network address.

Hromadné rozesílání nevyžádané pošty **Spamming**

Hromadné rozesílání nevyžádaných zpráv elektronickými prostředky – nejčastěji elektronickou poštou.

Mass distribution of unsolicited messages by electronic means – most often by electronic mail.

Hrozba **Threat**

Potenciální příčina nechtěného incidentu, jehož výsledkem může být poškození systému nebo organizace.

Potential cause of an unwanted incident, which may result in damage to a system or organisation.

Hypertext transfer protocol (HTTP) **Hypertext transfer protocol (HTTP)**

Aplikační protokol pro distribuované, kolaborativní, multimediální informační systémy. HTTP je základem datových přenosů pro celosvětovou síť WWW.

An application protocol for distributed, collaborative, hypermedia information systems. HTTP is the foundation of data communication for the World Wide Web.

Hypertext transfer protocol secure (HTTPS) **Hypertext transfer protocol secure (HTTPS)**

Široce používaný komunikační protokol pro bezpečnou komunikaci přes počítačovou síť, zvlášť široce používán na Internetu. Technicky se nejedná o protokol jako takový, spíše je výsledkem prostého vrstvení protokolu HTTP na protokol **SSL/TLS** a tak dodává standardní komunikaci **HTTP** ještě bezpečnostní možnosti.

*A widely used communications protocol for secure communication over a computer network, with especially wide deployment on the Internet. Technically, it is not a protocol in and of itself; rather, it is the result of simply layering the Hypertext Transfer Protocol (**HTTP**) on top of the **SSL/TLS** protocol, thus adding the security capabilities of **SSL/TLS** to standard HTTP communications.*

Hypervisor **Hypervisor**

Počítačový software, který vytváří a spouští jeden nebo více virtuálních počítačů.

Computer software that creates and runs one or more virtual machines.

Charakteristika viru **Virus signature**

Jedinečný bitový řetězec, který dostatečným způsobem virus identifikuje, a který může být využit skenovacím programem pro detekci přítomnosti viru.

Unique bit string which sufficiently identifies the virus and which can be used by a scanning programme to detect virus presence.

Chat **Chat**

Způsob přímé (on-line) komunikace více osob prostřednictvím Internetu.

Way of direct (online) communication of several persons using the Internet.

Chyba **Bug**

Programátorská chyba, která v software způsobuje bezpečnostní problém. Útočník může využít chybu pro ovládnutí počítače, znefunkčnění nebo chybné chování běžící služby, modifikaci dat apod.

A programming error, which causes a security problem in software. The attacker can utilise the bug to control the computer, make a running service dysfunctional or running improperly, to modify data and similar.

Chybný přístup **Failure access**

Neautorizovaný a obvykle neúmyslný přístup k datům v systému zpracování dat, který je výsledkem selhání hardware nebo software.

Unauthorised and usually unintentional access to data in a data processing system, which is the result of hardware or software failure.

ICMP záplava **ICMP flood**

Útok využívající protokol ICMP. Nejčastěji se využívají pakety ICMP echo (Ping), které slouží ke zjišťování, zda je vzdálené (cílové) zařízení dostupné. Zasláním velkého počtu těchto ICMP zpráv (nebo velkých ICMP echo paketů) může být docíleno zahlcení vzdáleného systému a jeho zpomalení nebo úplnou nedostupnost. Jedná se o velmi lehce proveditelný útok typu **DDoS**.

*An attack using the ICMP protocol. Most often used are ICMP echo (Ping) packets, which serve to establish if the remote (target) equipment is available. Sending out a large number of these ICMP messages (or large ICMP echo packets) may result in clogging the remote system and its slowdown or total unavailability. This is a simply executed attack of the **DDoS** type.*

Identifikace **Identification**

Proces, během kterého je určitá entita v dané doméně odlišena od ostatních entit. V proběhu identifikace jsou ověřeny předložené, nebo viditelné atributy entity. Identifikace je zpravidla součástí výměny informací mezi entitou, doménovými službami a využívanými zdroji. Identifikace může proběhnout opakovaně, i když je entita v síti známá.

A process when a certain entity in a given domain is differentiated from the other entities. Submitted or visible attributes of the entity are verified during the identification. Usually, the identification is part of information exchange among the entity, domain services and used resources. Identification may be made repeatedly even though the entity is known in the network.

Identifikace uživatele / ID uživatele **User identification / User ID**

Znakový řetězec nebo vzorec používaný systémem zpracování dat k identifikaci uživatele.

Character string or a formula used by a data processing system for user identification.

Identifikace rizik **Risk identification**

Proces zjišťování, rozpoznávání a popisování rizik.

Process of finding, recognising, and describing risks.

Identifikační předmět **Identity token**

Předmět používaný pro zjištění a ověření (autentizaci) identity.

Token used to find out and verify (authenticate) the identity.

Identifikátor / ID **Identifier / ID**

Informace o identitě, která v dané doméně jednoznačně rozlišuje mezi entitami.

Identity information that unambiguously distinguishes one entity from another one in a given domain.

Identifikovatelnost **Identifiability**

Stav, který vede k přímé nebo nepřímé identifikaci zadavatele osobních údajů na základě daného souboru osobních údajů.

Condition which results in a personally identifiable information principal being identified, directly or indirectly, on the basis of a given set of personally identifiable information.

Identita **Identity**

Sada vlastností, které jednoznačně určují konkrétní objekt – věc, osobu, událost.

Set of properties, which uniquely define a definite object – a thing, person, and event.

Incident **Incident**

(1) (bezpečnostní incident) Jedno či více nechtěných nebo neočekávaných porušení bezpečnosti (bez ohledu na to, zda jsou, nebo nejsou tresně právní povahy), které mohou s významnou pravděpodobností vést k narušení provozu nebo ohrožení bezpečnosti informací.
(2) (provozní incident) Neplánované přerušení služby, snížení kvality služby nebo událost, která zatím neovlivnila službu poskytovanou zakázníkovi.

(1) (Security incident) A single or a series of unwanted or unexpected information security breaches (whether of criminal nature or not) that have a significant

probability of compromising business operations or threatening information security. (2) (Operational incident) An unplanned interruption to a service, a reduction in the quality of a service or an event that has not yet impacted the service to the customer.

Informace **Information**

Každý znakový projev, který má smysl pro komunikátora i příjemce.

Any sign expression, which makes sense for the communicator and receiver.

Informace o autentizaci **Authentication information**

Informace použitá k ustavení validity prohlašované identity dané entity.

Information used to establish validity of proclaimed identity of a given entity.

Informace řízení přístupu **Access control information (ACI)**

Jakákoliv informace použitá pro účely řízení přístupu, včetně kontextových informací.

Any information used for the purpose of access control including context information.

Informační (kybernetická) společnost **Information (cyber) society**

Společnost schopná využívat a využívající informační a komunikační technologie. Základem je neustálá výměna znalostí a informací a práce s nimi za předpokladu schopnosti jim rozumět. Tato společnost pokládá vytváření, šíření a manipulaci s informacemi za nejvýznamnější ekonomické a kulturní aktivity.

A society capable of utilising, and indeed utilising, information and communication technologies. The basis is an incessant exchange of knowledge and information and handling them under the assumption of understanding these. This society considers creation, distribution and manipulation of information as the most significant economic and cultural activity.

Informační a komunikační technologie **Information and communication technology (ICT)**

Veškerá technika, která se zabývá zpracováním a přenosem informací, tj. zejména výpočetní a komunikační technika a její programové vybavení.

Any technology dealing with processing and transfer of information, in particular computing and communication technology and software.

Informační aktivum **Information asset**

Znalosti a data, která mají pro organizaci hodnotu (význam).

Knowledge and data of value (importance) to an organisation.

Informační kriminalita **Information Criminality**

Trestná činnost, pro kterou je určující vztah k software, k datům, respektive uloženým informacím, respektive veškeré aktivity, které vedou k neautorizovanému čtení, nakládání, vymazání, zneužití, změně nebo jiné interpretaci dat.

Criminal activity with a determined relation to software, data, more precisely to stored information, more precisely all activities resulting in unauthorised reading, handling, erasing, abusing, changing or other data interpreting.

Informační operace **Information operation (IO)**

Plánovaná, cílevědomá a koordinovaná činnost prováděná na podporu politických a vojenských cílů operace, k ovlivnění rozhodovacího procesu možného protivníka a jeho spojenců působením na jeho informace, informační procesy a komunikační infrastrukturu při současném využívání a ochraně vlastních informací a komunikační infrastruktury. IO jsou výhradně vojenskou aktivitou (činností), která má koordinovat vojenské informační aktivity, jejichž cílem je ovlivnit myšlení (vůli), chápání a možnosti protivníka nebo potencionálního protivníka. Veškeré informační aktivity by měly být vedeny v souladu s cíli vojenské operace, a zároveň je podporovat.

Planned, goal-oriented and coordinated activity done in support of political and military objectives of operation, to influence the decision-making process of a possible adversary and its allies by affecting its information, information processes and communication infrastructure and at the same using information and protection for own information and communication infrastructure. IO is exclusively a military activity, which has to coordinate military information activities with the objective of influencing the thinking (will), understanding and capabilities of the adversary or potential adversary. All information activities should be conducted in

line with the objectives of the military operation and to support them at the same time.

Informační potřeba **Information need**

Pochopení podstaty věci nezbytné pro řízení cílů, záměrů, rizik a problémů.

Insight necessary to manage objectives, goals, risks and problems.

Informační systém **Information system**

Funkční celek zabezpečující cílevědomé a systematické shromažďování, zpracovávání, uchovávání a zpřístupňování informací a dat. Zahrnuje datové a informační zdroje, nosiče, technické, programové a pracovní prostředky, technologie a postupy, související normy a pracovníky.

A functional unit enabling goal-oriented and systematic acquisition, processing, storage and access to information and data. Includes data and information sources, media, hardware, software and utilities, technologies and procedures, related standards and personnel.

Information assurance **Information assurance**

Soubor opatření k dosažení požadované úrovně důvěry v ochranu komunikačních, informačních a jiných elektronických i ne-elektronických systémů a informací ukládaných, zpracovávaných nebo přenášených v těchto systémech s ohledem na důvěrnost, integritu, dostupnost, neodmítnutelnost a autentičnost.

Set of measures to achieve the required level of confidence in the protection of communication, information and other electronic as well non-electronic systems and information stored, processed or transferred in these systems with regard to confidentiality, integrity, availability, undeniability and authenticity.

Informatizace společnosti **Informatisation of society**

Proces prosazování nové gramotnosti ve společnosti založené na zvládnutí nových metod práce s počítačem, s informacemi a informačními technologiemi.

Process of promoting new literacy in a society focused on adopting new methods of work with computers, information and information technology.

Infoware **Infoware**

Aplikace pro informatickou podporu klasických bojových akcí, respektive jako soubor aktivit, které slouží k ochraně, vytěžení, poškození, potlačení nebo zničení informací nebo informačních zdrojů, s cílem dosáhnout významné výhody v boji nebo vítězství nad konkrétním protivníkem. Pojem Infoware nelze zaměňovat s termínem Infowar, tj. informační válka.

Application for the automatic support of classical battle events, more precisely a set of activities serving to protect, mine out, damage, suppress or destroy information or information sources, with the objective of achieving a significant advantage in a battle or victory over a concrete adversary. The notion of Infoware must not be mistaken with the notion Infowar that is information war.

Infrastruktura jako služba **Infrastructure as a Service (IaaS)**

Schopnost poskytnout spotřebiteli zpracování, ukládání, sítě, a jiné základní výpočetní zdroje, přičemž spotřebitel na nich může umisťovat a provozovat libovolný software, včetně operačních systémů a aplikací. Spotřebitel nekoordinuje ani neřídí základní cloudovou infrastrukturu ale řídí operační systémy, ukládání do paměťových medií, a aktivní aplikace; může mít omezené řízení vybraných síťových komponent (například, hostitelský **firewall**).

*The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, including operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host **firewalls**).*

Infrastruktura veřejných klíčů **Public Key Infrastructure (PKI)**

V kryptografii se jedná o označení infrastruktury pro správu a distribuci veřejných klíčů z asymetrické kryptografie. PKI díky přenosu důvěry umožňuje používat pro ověření elektronického podpisu cizí veřejné klíče, aniž by bylo nutné každý z nich individuálně prověřovat. Přenos důvěry lze realizovat buď pomocí certifikační autority (X.509), nebo pomocí důvěrných sítí (např. PGP).

This in cryptography denotes infrastructure for the management and distribution of public keys from asymmetric cryptography. PKI, thanks to the transfer of confidence, enables the use of unfamiliar public keys for the verification of electronic signature without having to verify each individually. The transfer of

confidence can be implemented either using the certification authority (X.509) or by the trusted network (e.g. PGP).

Inicializační vektor **Initialisation vector**

Inicializační vektor nastavuje příslušný algoritmus vždy do jiného (náhodného) počátečního stavu, což i při stejném tajném klíči umožňuje generovat vždy jinou heslovou posloupnost. Jedná se o unikátní vygenerovaný proud dat, v případě proudových šifer je to vektor a u blokových šifer je to „nultý blok". Inicializační vektor bývá přenášen v otevřené podobě a umožňuje stejné počáteční nastavení šifrátorů.

Initialisation vector puts the appropriate algorithm always into a different (random) initial state, and thus even with the same secret key generates in each case a different output sequence. It is a uniquely generated data stream, in case of stream cyphers it is a vector, and with block cyphers, it is the „zero block". Initialising vector tends to be transferred openly and allows the same initial setting of cypher devices.

Insider **Insider**

Nebezpečný uživatel (zaměstnanec, stážista), který zneužívá svého legálního přístupu do komunikačního a informačního systému organizace zejména k neoprávněnému odcizování citlivých dat a informací.

Dangerous user (employee, intern) who abuses a legal access to the communication and information system of an organisation, in particular in order to perform unauthorised pilferage of sensitive data and information.

Integrita **Integrity**

Vlastnost přesnosti a úplnosti.

The property of accuracy and completeness.

Integrita dat **Data integrity**

Jistota, že data nebyla změněna. Přeneseně označuje i platnost, konzistenci a přesnost dat, např. databází nebo systémů souborů. Bývá zajišťována kontrolními součty, hašovacími funkcemi, samoopravnými kódy, redundancí, žurnálováním atd. V kryptografii a v zabezpečení informací všeobecně integrita znamená platnost dat.

Assurance that data were not changed. In the figurative sense denotes also the validity, consistency and accuracy of data, e.g. databases or file systems. It tends to be implemented by checksums, hash functions, self-correcting codes, redundancy, journalling, etc. In cryptography and information security in general, integrity means data validity.

Integrita sítě **Network integrity**

Funkčnost a provozuschopnost propojených sítí elektronických komunikací, ochrana těchto sítí vůči poruchám způsobeným elektromagnetickým rušením nebo provozním zatížením.

Functionality and operaoperability of interconnected networks of electronic communications, protection of these networks against failures caused by electromagnetic jamming or operational loading.

Integrita systému **System Integrity**

Kvalita systému zpracování dat plnicího svůj provozní účel a zabraňující přitom neautorizovaným uživatelům provádět změny zdrojů nebo používat zdroje a zabraňující autorizovaným uživatelům provádění nesprávných změn zdrojů nebo je nesprávně používat. Vlastnost, že systém vykonává svou zamýšlenou funkci nenarušeným způsobem, bez záměrné nebo náhodné neautomatizované manipulace se systémem.

Quality of a data processing system fulfilling its operational purpose and at the same time preventing unauthorised users from making changes in resources or from using the resources or from improper use of these. Property that a system performs its intended function without disruption, without intentional or accidental non-automated system manipulation.

Inteligentní electronické zařízení (IED) **Intelligent electronic device (IED)**

"Chytrý" senzor, který má „chytré" funkce pro sběr dat, jejich přenos na další zařízení a lokální zpracování a řízení. Jedno zařízení může obsahovat analogový vstupní senzor, analogový výstup, řídicí funkce na nejnižší úrovni, komunikační systém a programovou paměť. Pomocí IED lze v rámci SCADA systému provádět automatické řízení na místní úrovni.

A "smart" sensor containing the intelligence required to acquire data, communicate to other devices, and perform local processing and control. It could combine an analogue input sensor, analogue output, low-level control capabilities,

a communication system, and programme memory in one device. The use of IEDs in SCADA systems for automatic control at the local level.

Inteligentní síť **Smart Grid**

Silová elektrická a komunikační síť, která umožňuje regulovat výrobu a spotřebu elektrické energie v reálném čase, jak v místním, tak v globálním měřítku.

A power electrical and communications network that allows real-time control of power generation and consumption, both locally and globally.

Internet **Internet**

Globální systém propojených počítačových sítí, které používají standardní internetový protokol (TCP/IP). Internet slouží miliardám uživatelů po celém světě. Je to síť sítí, která se skládá z milionů soukromých, veřejných, akademických, obchodních a vládních sítí, s místním až globálním rozsahem, které jsou propojeny širokou škálu elektronických, bezdrátových a optických síťových technologií.

A global system of interconnected computer networks which use the standard internet protocol (TCP/IP). Internet serves billions of users around the world. It is a network of networks consisting of millions of private, public, academic, commercial and government networks, with a local to global outreach, that are all interconnected by a wide range of electronic, wireless and optical network technologies.

Internet control message protocol **Internet control message protocol (ICMP)**

Jedná se o služební protokol, který je součástí ***IP*** protokolu. Jeho hlavním úkolem je zasílání chybových hlášení ohledně dostupnosti služeb, počítačů nebo routerů. K těmto účelům se využívá například nástroj ping nebo traceroute.

*This is a service protocol, which is part of the **IP** protocol. Its main mission is to report error messages regarding the availability of services, computers or routers. For these purposes, ping or tracerout instruments are used, for example.*

Internet Protocol (IP) **Internet protocol (IP)**

Protokol, pomocí kterého spolu komunikují všechna zařízení na Internetu. Dnes nejčastěji používaná je jeho čtvrtá revize (IPv4), postupně se však bude přecházet na novější verzi (IPv6).

Protocol by which all equipment in the Internet mutually communicate. Today, the most used is the fourth revision (IPv4); however, step by step there will be a transition to a newer version (IPv6).

Internet věcí **Internet of things (IoT)**

Síť fyzických objektů („věcí“) se zabudovanými senzory, softwarem a dalšími technologiemi za účelem propojení a výměny dat s jinými zařízeními a systémy přes internet.

A network of physical objects ("things") embedded with sensors, software, and other technologies for the purpose of connecting and exchanging data with other devices and systems over the internet.

Internetová brána **Internet gateway**

Vstupní místo pro přístup k internetu.

Entry point to access the internet.

Internetová kriminalita **Internet crime**

Kriminální činnost, která využívá internetové služby či aplikace, cílí na internetové služby či aplikace, nebo využívá internet jako zdroj, nástroj nebo cíl zločinu.

Criminal activity where services or applications in the Internet are used for or are the target of a crime, or where the Internet is the source, tool, target, or place of a crime.

Internetová společnost pro přidělování jmen a čísel na internetu **Internet corporation for assigned names and numbers (ICANN)**

Nezisková asociace odpovědná za řízení přidělování doménových jmen a ***IP adres***, zachování provozní stability internetu, podporu hospodářské soutěže, k dosažení širokého zastoupení globální internetové komunity, a rozvíjet vhodné politiky a standardy, a rozvíjet své poslání prostřednictvím řízení zespoda – nahoru, a procesech konsensu.

The non-profit organisation responsible for the administration of domain names assignment as well IP addresses, for the maintenance of operational stability of internet, support of economic competition, achievement of a broad representation of the global internet community, and which develops its mission by bottom-to-top management and consensual processes.

Internetové služby **Internet services**

Služby poskytované uživateli, které zajišťují přístup na internet prostřednictvím přidělené IP adresy, které zpravidla obsahují ověření totožnosti, autorizaci a služby DNS.

Services provided to a user to enable access to the Internet via an assigned IP address, which typically include authentication, authorisation and domain name services.

Interoperabilita **Interoperability**

Schopnost společně působit při plnění stanovených cílů, neboli schopnost systémů, jednotek či organizací poskytovat služby jiným systémům, jednotkám či organizacím a akceptovat je od nich a používat takto sdílené služby pro efektivní společnou činnost.

Capability to act jointly in fulfilling set objectives, or the capability of systems, units or organisations to provide services to other systems, units or organisations and accept these from them and thus use shared services for an effective common activity.

Intranet **Intranet**

„Privátní“ (interní) počítačová síť využívající klasické technologie Internetu, která umožňuje zaměstnancům organizace efektivně vzájemně komunikovat a sdílet informace.

„Private” (internal) computer network using the classical Internet technology making it possible for employees of an organisation to communicate effectively and share information.

IP adresa **IP address**

Číslo, které jednoznačně identifikuje síťové rozhraní v počítačové síti, která používá IP (internetový protokol) slouží k rozlišení síťových rozhraní připojených k počítačové síti. V současné době nejrozšířenější verze IPv4 používá 32b číslo zapsané dekadicky po osmicích bitů (např. 123.234.111.222).

Number, which uniquely identifies a network interface, which uses IP (internet protocol) and serves for the differentiation of interfaces connected in the computer network. At present, the most widespread version IPv4 uses a number of 32 bits written in decimal in groups of eight bits (e.g. 123.234.111.222).

IP maškaráda **IP masquerading**

Mechanismus umožňující připojit do **Internetu** velké množství zařízení, pro které nejsou k dispozici tzv. veřejné **IP** adresy. Takováto zařízení dostanou přiděleny tzv. privátní **IP** adresy a přístup do Internetu se realizuje pomocí mechanismu překladu adres (NAT, Network Address Translation).

*The mechanism, which allows connecting to **the Internet** a large number of devices for which no so-called public **IP** addresses are available. These devices are assigned so-called private IP addresses, and access to the Internet is implemented through the mechanism of address translation (NAT, Network Address Translation).*

IPSec **IPSec**

Bezpečnostní rozšíření **IP** protokolu založené na autentizaci a šifrování každého IP datagramu. Jedná se o zabezpečení na síťové vrstvě. IPSec je definován v řadě RFC vydaných IETF, základními jsou 2401 a 2411.

*A security-based extension of the **IP** protocol predicated on authentication and encryption of each **IP** datagram. It is secured at the network layer. IPSec is defined in a number of RFCs issued by IETF, the fundamental ones are 2401 and 2411.*

IRC **Internet relay chat (IRC)**

Forma živé (real-time) komunikace textových zpráv (chat) nebo synchronní konference. Jedná se o systémy určené zejména pro skupinové komunikace v diskusních fórech, tzv. kanály, ale také umožňuje one-to-one (jedna-ku-jedné) komunikace přes soukromou zprávu, jakož i chat a přenos dat prostřednictvím přímého Klient-s-klientem (client-to-client). Dnes již není tolik používán, nahradili jej novější nástroje jako Skype, ICQ nebo Jabber.

A form of live (real-time) communication of text messages (chat) or synchronous conferences. These are systems intended primarily for group communications in discussion forums, so-called channels, but it also enables one-to-one communication via a private message, as well as a chat and data transfer using direct client-to-client. Today, it is not used so much; it has been replaced by newer instruments such as Skype, ICQ or Jabber.

IT síť **IT network**

Systém geograficky rozptýlený tvořený propojenými IT systémy pro výměnu dat, obsahující různé složky propojených IT systémů a jejich rozhraní s datovými a komunikačními sítěmi, které je doplňují.

Geographically distributed system formed by interconnected IT systems for information exchange and containing different components of the interconnected systems and their interfaces with data communication networks, which complement them.

IT systém **IT system**

Soubor zařízení, metod, dat, metadat, postupů a případně osob, který je uspořádán tak, aby plnil funkce při zpracování informací.

Set of devices, methods, data, metadata, procedures and sometimes persons that are arranged to fulfil some functions during information processing.

Jednosměrná brána **Unidirectional Gateway**

Zařízení skládající se z hardware a software. Hardwarová část zajišťuje jednosměrný přenos dat z jedné sítě do druhé, přitom přenos dat opačným směrem je fyzicky vyloučený. Softwarová část zajišťuje replikace databází a emuluje protokolové servery a zařízení.

A device consisting of hardware and software. The hardware permits a unidirectional data flow from one network to another, while data transfer in the opposite direction is physically impossible. The software part replicates databases and emulates protocol servers and devices.

Jednosměrná funkce **One-way function**

Funkce, která umožňuje pro určitý vstup snadno vypočítat výstup, a zároveň je z daného výstupu matematicky neproveditelné odvodit odpovídající vstup.

Function with the property that it is easy to compute the output for a given input but it is mathematically infeasible to find an input for a given output.

Jednosměrná hash funkce **One-way hash function**

Funkce, která transformuje libovolný řetězec bitů na řetězec bitů s pevnou délkou, a má následující dvě vlastnosti: z určitého vstupu lze matematicky odvodit právě jeden výstup; z daného výstupu není matematicky proveditelné odvodit odpovídající vstup.

A function, which maps strings of bits to fixed-length strings of bits, satisfying the following two properties: for a given input, one and only one output can be derived mathematically; from a given output, it is mathematically infeasible to find a corresponding input.

Jednotná identita **Single-sign-on identity, SSO identity**

Identita, která má jedno potvrzení o totožnosti, které může být ověřeno relying party ve více doménách.

Identity that includes a single identity assertion that can be verified by a relying party in multiple domains.

Jmenný server **Domain name system server (DNS server)**

Viz **DNS server**.

*See **Domain name system server**.*

Kerberos **Kerberos**

Kerberos je autentizační protokol pro počítačové sítě, který pracuje na základě „tiketů“ a umožňuje, aby uzly komunikující na nezabezpečené síti si mohly vzájemně dokázat svoji identitu bezpečným způsobem. Návrháři jej cílili zejména na model klient-server a poskytuje vzájemnou autentizaci-jak uživatel tak i server si vzájemně ověří svoji identitu. Zprávy protokolu Kerberos jsou chráněny proti odposlechu a útokům opakování.

Kerberos is a computer network authentication protocol which works by „tickets“ to allow nodes communicating over a non-secure network to prove their identity to one another in a secure manner. Its designers aimed it primarily at a client-server model, and it provides mutual authentication—both the user and the server verify each other's identity. Kerberos protocol messages are protected against eavesdropping and replay attacks.

Keylogger (Keystroke logger) **Keylogger (Keystroke logger)**

Software, který snímá stisky jednotlivých kláves, bývá však antivirem považován za virus, v případě softwaru se jedná o určitou formu spyware, ale existují i hardwarové keyloggery. Často se používá pro utajený monitoring všech aktivit na PC, jenž je pro ostatní uživatele neviditelný a chráněný heslem. Umožňuje automatické zaznamenávání všech stisků kláves (psaný text, hesla apod.), navštívených www stránek, chatů a diskuzí přes ICQ, MSN apod., spouštěných aplikací, screenshotů práce s počítačem, práce uživatele se soubory a další. Zaznamenaná data mohou být skrytě odesílána emailem.

Software reading when individual keys are pushed; may, however, be regarded as a virus by an antivirus programme, in case of software it may be a certain form of spyware but there are even hardware keyloggers. It is often used for secret monitoring of all PC activities, is invisible for other users and protected by a password. It enables automatic logging of all keystrokes (written text, passwords, etc.), visits to www pages, chats and discussions over ICQ, MSN and similar, running applications, screenshots of computer work, user file handling and other. Logged data could be secretly sent by email.

Klepání na porty **Port Knocking**

Označuje v počítačových sítích metodu, jak si z nedůvěryhodného počítače otevřít přístup do počítače nebo počítačové sítě chráněné ***firewallem*** bez nutnosti se na počítač s ***firewallem*** přihlásit a jako administrátor jeho nastavení změnit. Tento způsob umožňuje mít ***firewall*** vůči nedůvěryhodným počítačům zdánlivě úplně uzavřený a přesto mít možnost pomocí speciální utajené sekvence paketů jeho nastavení změnit. Metoda umožňuje vyhnout se zneužití bezpečnostních chyb v programech obsluhujících trvale otevřené porty.

*Denotes a method in computer networks how to gain access from an untrusted computer into a computer or computer network protected by a **firewall**, without the need to sign on with the computer protected by a **firewall** and change the setting like an administrator. This way creates a semblance that the **firewall** is closed to untrusted computers and yet gives a chance of changing the setting by a special secret sequence. The method bypasses abuse of security errors in programmes serving permanently open ports.*

Klíč **Key**

Posloupnost symbolů, která řídí operace kryptografické transformace (např. šifrování, dešifrování, výpočet kryptografické kontrolní funkce, výpočet podpisu nebo ověření podpisu).

Sequence of symbols that controls the operations of a cryptographic transformation (e.g. encryption, decryption, cryptographic check function computation, signature calculation, or signature verification).

Klíč pro šifrování klíčů **Key encryption key (KEK)**

Kryptografický klíč, který se používá k šifrování, nebo dešifrování dalších klíčů.

Cryptographic key that is used for the encryption or decryption of other keys.

Kód autentizace zprávy **Message authentication code**

Bitový řetězec, který je funkcí dat (v zašifrovaném nebo nezašifrovaném tvaru) a tajného klíče a je připojen k datům, aby umožnil autentizaci dat.

Bit string, which is a function of data (in an encrypted or plain form) and the secret key, and is attached to data in order to authenticate them.

Kombinovaný útok **Blended attack**

Útok, který se snaží maximalizovat závažnost poškození a rychlost nákazy kombinací více útočných metod.

Attack that seeks to maximize the severity of damage and speed of contagion by combining multiple attacking methods.

Kompromitace **Compromising**

Porušení informační bezpečnosti, které může mít za následek modifikaci programů nebo dat, jejich zničení, nebo jejich dostupnost pro neautorizované entity.

Compromise of information security, which may result in programme or data modification, their destruction, or their availabilty to unauthorised entities.

Komunikace rizika **Risk communication**

Výměna nebo sdílení informací o riziku mezi tím, kdo rozhoduje a ostatními zúčastněnými stranami.

Exchange or sharing of information between the decision-maker and other participating parties.

Komunikační systém **Communication system**

Systém, který zajišťuje přenos informací mezi koncovými účastníky. Zahrnuje koncové komunikační zařízení, přenosové prostředí, správu systému, personální obsluhu a provozní podmínky a postupy. Může zahrnovat i prostředky kryptografické ochrany.

System, which provides for the transfer of information among end users. It includes end communication devices, transfer environment, system administration, handling by personnel and operational conditions and procedures. It may also include means of cryptographic protection.

Koncové zařízení **Endpoint device**

Síťově připojené technické zařízení **ICT**, jako jsou stolní počítače, notebooky, chytré telefony, tablety, tencí klienti, tiskárny nebo jiný specializovaný hardware včetně inteligentních měřičů a zařízení **IoT**.

*Network connected **ICT** hardware device like desktop computers, laptops, smart phones, tablets, thin clients, printers or other specialized hardware including smart meters and **IoT** devices.*

Konfigurace (systému nebo zařízení) **Configuration (of a system or device)**

Krok v systémovém návrhu, např. výběr funkčních prvků, návrh jejich rozmístění a vzájemného propojení.

Step in system design; for example, selecting functional units, assigning their locations, and defining their interconnections.

Konfigurační databáze **Configuration management database (CMDB)**

Úložiště dat používané pro záznam atributů konfiguračních položek a vztahů mezi konfiguračními položkami po celou dobu jejich životního cyklu.

Data warehouse used for records of configuration items' attributes and relations among configuration items during their whole life cycle.

Konfigurační položka **Configuration item (CI)**

Prvek, který musí být řízen za účelem dodávání služby nebo služeb.

Element, which must be controlled in order to deliver a service or services.

Kontaktní bod **Point of contact (PoC)**

Určená organizační role nebo funkce, která slouží jako koordinátor nebo místo kde se sbíhají informace týkající se aktivit v oblasti řízení incidentů.

Defined organisational role or function serving as the coordinator or focal point of information concerning incident management activities.

Kontaminace **Contamination**

Vložení dat s určitou bezpečnostní klasifikací nebo bezpečnostní kategorií do nesprávné bezpečnostní kategorie.

Input of data with a certain security classification or security category into a wrong security category.

Kontinuita bezpečnosti informací **Information security continuity**

Procesy a postupy k zajištění nepřetržitého provozování bezpečnosti informací.

Processes and procedures for ensuring continued information security operations.

Kontinuita činností organizace **Business continuity**

Způsobilost organizace trvale dodávat produktu nebo služby na přijatelné předem definované úrovni následně po incidentu narušení chodu.

Capability of the organisation to continue delivery of products or services at acceptable predefined levels following disruptive incident.

Kontinuita služeb **Service continuity**

Schopnost řídit rizika a události, které by mohly mít vážný dopad naslužby s cílem nepřetržitě dodávat služby na dohodnutých úrovních.

Capability to manage risks and events which could seriously impact services, with the objective of providing continuous services at the agreed levels.

Krádež totožnosti / krádež identity **Identity theft**

Výsledek úspěšného předstírání cizí totožnosti.

Result of a successful false claim of identity.

Kritéria rizika **Risk criteria**

Daný rámec, na jehož základě se hodnotí závažnost rizika.

Terms of reference against which the significance of risk is evaluated.

Kritická informační infrastruktura **Critical information infrastructure**

Komplex informačních a komunikačních systémů (naplňující stanovená průřezová kritéria a odvětvová kritéria v oblasti kybernetické bezpečnosti), jejichž nefunkčnost by mohla způsobit závažný dopad na bezpečnost státu, zabezpečení základních životních potřeb obyvatelstva, zdraví osob nebo ekonomiku státu.

The complex of information and communication systems (meeting the defined criteria across and inside the branches of cyber security) whose dysfunctionality would result in a serious impact on state security, provision of the basic daily needs of the population, public health or the economy of state.

Kritická infrastruktura **Critical infrastructure**

Systémy a služby, jejichž nefunkčnost nebo špatná funkčnost by měla závažný dopad na bezpečnost státu, jeho ekonomiku, veřejnou správu a v důsledku na zabezpečení základních životních potřeb obyvatelstva.

Systems and services whose dysfunctionality or wrong functionality would result in a serious impact on state security, its economy, public administration and in the end on the provision of the basic daily needs of the population.

Kritická komunikační infrastruktura (státu) **Critical communication infrastructure (of the state)**

Komplex komunikačních systémů, služeb nebo sítí elektronických komunikací (naplňující stanovená průřezová kritéria a odvětvová kritéria v oblasti kybernetické bezpečnosti), jejichž nefunkčnost by mohla způsobit závažný dopad na bezpečnost státu, zabezpečení základních životních potřeb obyvatelstva, zdraví osob nebo ekonomiku státu.

The complex of communication systems, services or networks (meeting the defined criteria across and inside the branches of cyber security) whose dysfunctionality would result in a serious impact on state security, provision of the basic daily needs of the population, public health or the economy of the state.

Kritické aktivum **Critical asset**

Aktivum, které může mít přímý vliv na výrobu nebo přenos, skladování a distribuci elektrické energie, plynu, ropy a tepla.

Asset which can have a direct impact on production or generation, transmission, storage and distribution of electric power, gas, oil and heat.

Krize **Crisis**

Situace, ve které je významným způsobem narušena rovnováha mezi základními charakteristikami systému na jedné straně a postojem okolního prostředí na straně druhé.

A situation where the equilibrium among the basic components of the system on the one hand, and approach of the environment on the other hand, is disrupted seriously.

Krizová připravenost **Crisis preparedness**

Příprava opatření k řešení vlastních krizových situací a k podílu na řešení krizových situací ve svém okolí.

Preparation of measures to solve own crisis situations and partially participate in solving crisis situations in the neighbourhood.

Krizová situace **Crisis / Emergency situation**

Mimořádná událost podle zákona o integrovaném záchranném systému, narušení kritické infrastruktury nebo jiné nebezpečí, při nichž je vyhlášen stav nebezpečí, nouzový stav nebo stav ohrožení státu (dále jen „krizový stav“).

The emergency as per the law on an integrated emergency system, compromise of the critical infrastructure, or any other danger when a state of hazard, state of emergency, or threat to the state is announced (henceforth only "emergency").

Krizové opatření **Crisis measure**

Organizační nebo technické opatření určené k řešení krizové situace a odstranění jejích následků, včetně opatření, jimiž se zasahuje do práv a povinností osob.

Organisational or technical measure to solve a crisis situation and remedy its consequences, including measures interfering with the rights and obligations of people.

Krizové plánování **Crisis planning**

Aktivita příslušných orgánů krizového řízení zaměřená na minimalizaci (prevenci) možnosti vzniku krizových situací. Hledání nejvhodnějších způsobů protikrizové intervence, optimalizaci metod a forem zvládání těchto nežádoucích jevů (tj. redukci dopadů krizových situací) a stanovení nejracionálnějších a ekonomicky nejvýhodnějších cest obnovy postižených systémů a jejich návratu do nového běžného stavu.

The activity of the relevant bodies of crisis management aimed at minimising (prevention of) the origin of crises. Searching for the most suitable ways of anti-crisis intervention, optimisation of methods and forms to handle these unwanted phenomena (that is, reduction of the impacts of crises) and establishing the most

rational and economical ways of recovery for the affected systems and their return into the normal daily state.

Krizové řízení **Crisis management**

Souhrn řídicích činností orgánů krizového řízení zaměřených na analýzu a vyhodnocení bezpečnostních rizik a plánování, organizování, realizaci a kontrolu činností prováděných v souvislosti s přípravou na krizové situace a jejich řešením, nebo ochranou kritické infrastruktury.

Collection of management activities of the bodies of crisis management aimed at the analysis and evaluation of security risks and planning, organisation, implementation and verification of activities conducted in connection with preparation for crises and their solution or protection of critical infrastructure.

Krizový plán **Crisis plan**

Souhrnný plánovací dokument, který zpracovávají zákonem stanované subjekty, a který obsahuje souhrn opatření a postupů k řešení krizových situací.

Aggregate planning document elaborated by entities set forth by law and which contains a set of measures and procedures to solve crises.

Krizový stav **Crisis state**

Legislativní opatření vyhlašované Parlamentem ČR (stav ohrožení státu a válečný stav), vládou ČR (nouzový stav) nebo hejtmanem kraje / primátorem (stav nebezpečí) za účelem řešení krizové situace.

The legislative measure announced by the Parliament of the Czech Republic (threat to the state, and the state of war), by the Government of the Czech Republic (state of emergency) or governor of the region/mayor (state of danger), to solve a crisis.

Kryptografický algoritmus **Cryptographic algorithm**

Přesně definovaná výpočetní procedura, která na základě vstupních dat a zpravidla i kryptografického klíče vytváří určitý výstup. Obvykle se využívá k šifrování, nebo dešifrování dat.

A well-defined computational procedure that takes variable inputs, which may include cryptographic keys, and produces an output. It is usually used for data encryption or decryption.

Kryptografický iniciační klíč **Crypto Ignition Key (CIK)**

Fyzický (obvykle elektronický) nosič pro ukládání klíčů, určen pro ukládání, dopravu a ochranu kryptografických klíčů a iniciačních údajů. Obsahuje část klíčové proměnné, bez které není kryptografický prostředek schopen šifrovat a dešifrovat data. Kryptografický prostředek bez vloženého kryptografického iniciačního klíče neobsahuje otevřené kryptografické klíče případně ani další utajovaná data.

Physical (usually electronic) token to store keys, intended for the storing, transport and protection of cryptographic keys and initialising data. It contains part of key material without which the encryption device cannot encrypt and decrypt data. A cryptographic device without the inserted CIK does not contain open cryptographic keys nor other secret data.

Kryptografický klíč **Cryptographic key**

Posloupnost symbolů řídicích provedení kryptografické transformace. Kryptografický klíč může obsahovat kromě náhodné datové posloupnosti i další data, především data pro zabezpečení integrity, dobu platnosti, název a číslo klíče.

Sequence of symbols that controls the operation of a cryptographic transformation. The cryptographic key can contain, in addition to a random sequence of data, other data to ensure the integrity, time of validity, name and number of key.

Kryptografický prostředek **Cryptographic device**

Kryptografický prostředek (šifrátor) je zařízení (HW a SW) využívající k transformaci (šifrování a dešifrování) dat matematické metody a postupy s využitím kryptografických algoritmů a kryptografických klíčů. Funkce šifrování dat je u tohoto zařízení dominantní. Funkci šifrování / dešifrování může zabezpečovat i kryptografický modul (HW, SW), který může být součástí jiného zařízení.

Cryptographic device (encryptor) is a hardware and software device using mathematical methods and procedures together with cryptographic algorithms and cryptographic keys, in order to transform (encrypt and decrypt) data. The encryption function is the dominant one for this device. The encryption/decryption function can be implemented also by a cryptographic (HW and SW) module which may be part of another device.

Kryptografický protokol **Cryptographic protocol**

Protokol, který provádí bezpečnostní funkci pomocí kryptografie.

Protocol which performs a security-related function using cryptography.

Kryptografický útok **Cryptanalytic attack**

Útok na určitou šifru, který využívá vlastností dané šifry.

Attack against a cipher that makes use of properties of the cipher.

Kryptografie **Cryptography**

Nauka o šifrování – disciplína, která zahrnuje zásady, prostředky a metody pro transformaci dat aby byl ukryt jejich sémantický obsah, zabráněno jejich neautorizovanému použití nebo zabráněno jejich nezjištěné modifikaci.

Science of cryptography – a discipline covering the principles, means and methods to transform data in order to conceal their semantic content, to prevent an unauthorised use or prevent unrecognised modification.

Kybergrooming (Child grooming) **Cybergrooming (Child grooming)**

Chování uživatelů internetových komunikačních prostředků (chat, ICQ atd.), kteří se snaží získat důvěru dítěte a s cílem ho zneužít (zejm. sexuálně) či zneužít k nelegálním aktivitám.

The behaviour of users of internet communication instruments (chat, ICQ, et al.) who try to get the trust of a child to either abuse the child (especially sexually) or misuse the child for illegal activity.

Kybernetická bezpečnost **Cyber security**

(1) Souhrn právních, organizačních, technických a vzdělávacích prostředků směřujících k zajištění ochrany kybernetického prostoru.
(2) Zajištění důvěrnosti, integrity a dostupnosti informací v kybernetickém prostoru.

(1) Collection of legal, organisational, technological and educational means aimed at protecting cyberspace.
(2) Preservation of confidentiality, integrity and availability of information in the cyberspace.

Kybernetická hrozba **Cyber threat**

Potenciální příčina nežádoucího kybernetického bezpečnostního incidentu, který může mít za následek poškození systému, lidí, společnosti, organizace nebo jiných subjektů v kyberprostoru.

Potential cause of an unwanted cybersecurity incident, which can result in harm to a system, people, society, organization, or other entities in cyberspace.

Kybernetická kriminalita **Cyber crime**

Trestná činnost kdy jsou služby nebo aplikace v kybernetickém prostoru nástrojem nebo cílem útoku, případně trestná činnost v rámci které je kybernetický prostor zdrojem, nástrojem, cílem nebo místem trestného činu.

A criminal activity where services or applications in the cyberspace are used for or are the target of a crime, or where the cyberspace is the source, tool, target, or place of a crime.

Kybernetická obrana **Cyber defence**

Obrana proti kybernetickému útoku a zmírňování jeho následků. Také rezistence subjektu na útok a schopnost se účinně bránit.

Defence against a cyber attack and mitigation of its consequences. Also, resistance of the subject towards an attack and a capability to defend itself effectively.

Kybernetická ochrana **Cyber protection**

Stav bezpečí proti fyzickým, sociálním, duchovním, finančním, politickým, emocionálním, pracovním, psychologickým, vzdělávacím nebo jiným následkům selhání, poškození, závady, nehody, útoku či jiné nežádoucí události v kybernetickém prostoru.

The condition of being protected against physical, social, spiritual, financial, political, emotional, occupational, psychological, educational or other types or consequences of failure, damage, error, accidents, harm or any other event in the cyberspace which could be considered non-desirable.

Kybernetická operace **Cyber operations**

Využití kybernetických schopností anebo kyberprostoru s primárním účelem dosáhnout cílů.

The employment of cyber capabilities or cyberspace with the primary purpose of achieving objective.

Kybernetická strategie **Cyber strategy**

Obecný postup k rozvoji a využití schopností pracovat v kybernetickém prostoru, integrovaný a koordinovaný s ostatními operačními oblastmi k dosažení nebo podpoře dosažení stanovených cílů pomocí identifikovaných prostředků, metod a nástrojů v určitém časovém rozvrhu.

The general approach to the development and use of capabilities to operate in cyberspace, integrated and coordinated with other areas of operation, to achieve or support the set objectives by using identified means, methods and instruments in a certain timetable.

Kybernetická špionáž **Cyber espionage**

Získávání strategicky citlivých či strategicky důležitých informací od jednotlivců nebo organizací za použití či cílení prostředků IT. Používá se nejčastěji v kontextu získávání politické, ekonomické nebo vojenské převahy.

Obtaining strategically sensitive or strategically important information from individuals or organisations by using or targetting IT means. It is used most often in the context of obtaining political, economic or military supremacy.

Kybernetická válka **Cyber war, Cyber warfare**

Použití počítačů a Internetu k vedení války v kybernetickém prostoru. Soubor rozsáhlých, často politicky či strategicky motivovaných, souvisejících a vzájemně vyvolaných organizovaných kybernetických útoků a protiútoků.

Use of computers and the Internet to wage a war in cyberspace. System of extensive, often politically or strategically motivated, related and mutually provoked organized cyber attacks and counterattacks.

Kybernetické pojištění **Cyber-insurance**

Pojištění, které kryje nebo snižuje finanční ztráty pojištěného způsobené kybernetickým incidentem.

Insurance that covers or reduces financial loss to the insured caused by a cyber-incident.

Kybernetické riziko **Cyber-risk**

Riziko způsobené kybernetickou hrozbou.

Risk caused by a cyber-threat.

Kybernetický incident **Cyber-incident**

Kybernetický incident, který zahrnuje ztrátu bezpečnosti informací nebo má dopad na obchodní operace.

Cyber-event that involves a loss of information security or impacts business operations.

Kybernetický prostor **Cyberspace**

Digitální prostředí umožňující vznik, zpracování a výměnu informací, tvořené informačními systémy, a službami a sítěmi elektronických komunikací.

Digital environment enabling the origin, processing and exchange of information, made up of information systems and the services and networks of electronic communications.

Kybernetický protiútok **Cyber counterattack**

Útok na IT infrastrukturu jako odpověď na předchozí kybernetický útok. Používá se nejčastěji v kontextu politicky či vojensky motivovaných útoků.

Attack on IT infrastructure as a response to a previous cyber attack. It is used most often in the context of either politically or militarily motivated attacks.

Kybernetický útok **Cyber attack**

Útok na IT infrastrukturu za účelem způsobit poškození a získat citlivé či strategicky důležité informace. Používá se nejčastěji v kontextu politicky či vojensky motivovaných útoků.

Attack on IT infrastructure having the objective of causing damage and obtaining sensitive or strategically important information. It is used most often in the context of either politically or militarily motivated attacks.

Kybernetika **Cybernetics**

Věda, která se zabývá obecnými principy řízení a přenosu informací ve strojích, živých organismech a společenstvích. K popisu používá zejména matematický aparát. Je založena na poznatku, že některé procesy probíhající v živých organismech jsou popsány stejnými rovnicemi jako analogické procesy v technických zařízeních.

The science dealing with general principles of information management and transmission in machines, living organisms and communities. It uses mainly the apparatus of mathematics in its specifications. It is based on the knowledge that some processes in the living organisms are described by the same equations as analogue processes in technological devices.

Kyberstalking **Cyberstalking**

Nejrůznější druhy sledování a obtěžování s využitím elektronického média (zejm. prostřednictvím elektronické pošty a sociálních sítí), jejichž cílem je např. vzbudit v oběti pocit strachu. Informace o oběti pachatel získává nejčastěji z webových stránek, fór nebo jiných hromadných komunikačních nástrojů. Často je taková aktivita pouze mezistupněm k trestnému činu, který může zahrnovat výrazné omezování osobních práv oběti nebo zneužití chování oběti k provedení krádeže, podvodu, vydírání apod.

Various kinds of stalking and harassment using electronic media (especially using emails and social networks), the objective being for example to instil a feeling of fear in the victim. The culprit obtains information about the victim most often from web pages, forums, or other mass communication tools. Often such activity is merely an intermediate step to a criminal act which may include a substantial limitation of human rights of the victim, or misuse the behaviour of the victim to steal, defraud, blackmail, etc.

Kyberterorismus **Cyber terrorism**

Trestná činnost páchaná za primárního využití či cílení prostředků IT s cílem vyvolat strach či neadekvátní reakci. Používá se nejčastěji v kontextu extremisticky, nacionalisticky a politicky motivovaných útoků.

Criminal activity done using or targeting primarily IT means with the objective of creating fear or inadequate response. It is used most often in the context of attacks having an extremist, nationalistic or politically motivated character.

Ladder (žebřík) **Ladder**

Druh grafického programovacího jazyka. Spočívá ve spojování napájecí a výstupní sběrnice pomocí logických funkcí. Též bývá označován jako jazyk kontaktních schémat. Tato reprezentace je součást normy IEC 61113-3.

Type of graphical programming language. It consists of connecting the supply and output bus with logic functions. It is also referred to as the language of contact schemes. This representation is part of IEC 61113-3.

Lamer **Lamer**

Osoba, zpravidla úplný začátečník, který se nevyzná v dané IT problematice.

Person, usually a complete beginner, who is unfamiliar with the given IT issues.

Léčka **Entrapment**

Úmyslné umístění zjevných závad do systému zpracování dat za účelem detekce pokusů o průnik nebo pro zmatení protivníka, které závady by měl využít.

Intentional placement of obvious defects into a data processing system in order to detect penetration attempts, or to deceive an adversary who should use the defect.

Leetspeak **Leetspeak**

Jazyk, který nahrazuje písmena latinské abecedy čísly a tisknutelnými znaky ASCII. Používá se hodně na internetu (chat a online hry). Tento počítačový dialekt zpravidla anglického jazyka nemá pevná gramatická pravidla a slova je možné tvořit také jejich zkracováním, např. vynecháním písmen nebo zkomolením („nd“ – end, „U“ – you, „r“ – are).

Language replacing the letters of the Latin alphabet by numerals and printable ASCII characters. It is used quite a lot on the Internet (chat and online games). This computer dialect, usually of the English language, has no fixed grammatical rules and words may be formed by shortening, e.g. by omissions of letters or corruption ("nd" – end, "U" – you, "r" – are).

Legální elektronický důkaz **Legal digital evidence**

Elektronický důkaz, který je akceptován v rámci soudního řízení.

Digital evidence, which is accepted in a judicial process.

Licence **Licence**

Oprávnění a také dokument, který toto oprávnění zaznamená.

Permission as well as the document recording that permission.

Log **Log**

Zkrácený výraz pro Log file.

Shortened expression for Log file.

Logická bomba **Logical bomb**

Škodlivá logika, která působí škodu systému zpracování dat a je spuštěna určitými specifickými systémovými podmínkami. Program (podmnožina Malware), který se tajně vkládá do aplikací nebo operačního systému, kde za předem určených podmínek provádí destruktivní aktivity. Logická bomba se skládá ze dvou základních částí: rozbušky a akce. Předem specifikovanou podmínkou startující logickou bombu může být například konkrétní datum (výročí určité události – např. „Virus 17. listopad“). V tomto případě se jedná o typ tzv. časované bomby (Time Bomb).

Harmful logic causing damage to a data processing system and being triggered by certain specific system conditions. Programme (a subset of Malware) which is secretly put into applications or into an operating system where, under predetermined conditions, it performs destructive activities. The logical bomb is composed of two basic components: trigger and action. Predetermined specified condition triggering the logic bomb may be, for example, a fixed date (anniversary of a certain event – for example "Virus 17 November"). In this case, the type is a so-called time bomb.

Logické řízení přístupu **Logical access control**

Použití mechanizmů týkajících se dat nebo informací k zajištění řízení přístupu.

Use of mechanisms related to data or information to enable control of access.

Lokální internetový registr **Local internet registry (LIR)**

Jedná se o organizaci působící obvykle v rámci jedné sítě, které je přidělen blok IP adres od RIR. LIR přiděluje bloky IP adres svým zákazníkům připojeným do dané sítě. Většina LIR jsou poskytovatelé internetových služeb, podniky či akademické instituce. Související výrazy – RIR.

The organisation, usually active in one network, which is assigned a block of IP addresses from RIR. LIR assigns the IP address blocks to its customers connected to the given network. Most LIRs are internet service providers, companies or academic institutions. Related expressions – RIR.

Lokální síť (LAN) **Local area network (LAN)**

Označení pro malé sítě, obvykle v rámci administrativně jednotných celků – firem, budov, společenství, které jsou budované za účelem snadného sdílení prostředků (IS, dat, služby, zařízení) a umožňují efektivní ochranu a nežádoucích jevů.

The term for small networks, usually within administratively uniform aggregates – companies, buildings, communities, which are formed with the aim to facilitate sharing of means (IS, data, services, equipment) and to enable effective protection against undesirable phenomena.

MAC adresa **MAC address**

MAC = Media Access Control. Jedinečný identifikátor síťového zařízení, který je přidělen výrobcem.

MAC = Media Access Control. Unique identifier of a network device allotted by the manufacturer.

Management bezpečnostních informací a událostí **Security information and event management (SIEM)**

Systém, jehož úkolem je sběr, analýza a korelace dat – událostí v síti. SIEM systémy kombinují metody detekce a analýzy anomálních událostí v síti, poskytují informace použitelné k řízení sítě a provozovaných služeb.

A system whose task is to acquire, analyse and correlate data – events in the network. SIEM systems combine the methods of detection and analysis of abnormal events in the network, provide information usable for network management and operated services.

Manipulování **Tampering**

Úmyslné provedení nebo umožnění změny digitálních důkazů (tj. úmyslné nebo záměrné poškození).

Act of deliberately making or allowing change(s) to digital evidence (i.e. intended or purposeful spoliation).

Master Terminal Unit **Master Terminal Unit (MTU)**

Viz **Řídicí server**.

*See **Control Server.***

Maškaráda IP **IP Masquerade**

Mechanismus skrývání nebo předstírání jiné IP adresy, která takto vystupuje jako jiná identita.

A mechanism of hiding, or pretending, another IP address, and thus posing as another identity.

Maximální přijatelná doba narušení **Maximum tolerable period of disruption (MTPD)**

Doba, po kterou by mohly trvat nepříznivé dopady, které by mohly narůstat jako výsledek neposkytování produktu/služby nebo provádění činností, než by se staly nepřijatelnými (viz též maximální přípustný výpadek).

Time, it would take for adverse impacts, which might arise as a result of not providing a product/service or performing activities, to become unacceptable (see also maximum acceptable outage).

Metadata **Metadata**

Metadata jsou data, která poskytují informaci o jiných datech.

Metadata are data that provide information about other data.

Maximální přípustný výpadek **Maximum acceptable outage (MAO)**

Doba, po kterou by mohly trvat nepříznivé dopady, které by mohly narůstat jako výsledek neposkytování produktu/služby nebo provádění činností, než by se staly nepřijatelnými (viz též maximální přijatelná doba narušení).

Time, it would take for adverse impacts, which might arise as a result of not providing a product/service or performing an activity, to become unacceptable (see also a maximum tolerable period of disruption).

Minimání odhalení **Minimal disclosure**

Princip v oblasti řízení identit omezit předání informace o identitě třetí straně na minimální možnou úroveň, která je nutná pro daný účel.

Principle of identity management to restrict the transfer of identity information to a third party to the minimum possible level required for a particular purpose.

Minimální úroveň chodu organizace **Minimum business continuity objective (MBCO)**

Minimální úroveň služeb a/nebo produktů, která je přijatelná pro organizaci, aby dosahovala svých cílů organizace během narušení.

Minimum level of services and/or products that is acceptable to the organisation to achieve its business objectives during a disruption.

Množina dat, sada dat **Dataset**

Soubor dat.

Collection of data.

Model životního cyklu **Life cycle model**

Model množiny procesů a činností týkajících se životního cyklu, které mohou být uspořádány do etap, který mimo jiné slouží jako společný základ pro komunikaci a porozumění.

A model of a set of processes and activities concerned with the life cycle that may be organised into stages, which also acts as a common reference for communication and understanding.

Modem **Modem**

Zařízení, které slouží k převodu sériových digitálních dat z určitého koncového zařízení na analogový signál, který je následně přenesen prostřednictvím telefonním sítě na jiné koncové zařízení a tam je dekódován.

A device used to convert serial digital data from an end device to an analogue signal then transmitted over a telephone network to another end device and decoded there.

Monitorovací prostředky **Monitoring means**

Nástroje a prostředky pro monitorování provozu systému.

Tools and means to monitor system operation.

Monitorování **Monitoring**

Určení stavu systému, procesu nebo činnosti. Pozn. K určení stavu může být potřebné provádět kontrolu, dohled nebo kritické pozorování.

Determining the status of a system, a process or an activity. Note: To determine the status there may be a need to check, supervise or critically observe.

Monitorování sítě na dálku **Remote Network Monitoring (RMON)**

Monitorování sítě na dálku (RMON) je součást MIB modulu, obsaženého v SNMP, který obsahuje specifikaci k monitorování jednotlivých síťových uzlů.

RMON is a part of the MIB module contained in SNMP which contains the specification to monitor individual network nodes.

Motion Control Network **Motion Control Network**

Specifická síť, která umožňuje aplikacím řídit pohyb součástí určité průmyslové sestavy včetně sekvencování, kontroly rychlosti, regulace a přírustkového pohybu.

A specific network enabling the applications to control the movement of parts of specific industrial settings, including sequencing, speed control, regulation and incremental motion.

Náhodné číslo, náhodný bit **Random number, random bit**

Parametr měnící se v čase, jehož hodnotu nelze předvídat v obsahu a čase..

A parameter varying in time whose value cannot be predicted for content or time.

Náprava **Correction**

Akce vedoucí k odstranění zjištěné neshody.

Action to eliminate a detected nonconformity.

Nápravné opatření **Corrective action**

Činnost vedoucí k odstranění příčiny neshody a k zabránění opakovaného výskytu.

Action to eliminate the cause of a noncompliance and prevent recurrence.

Národní autorita **National authority**

Státní úřad odpovědný za problematiku kybernetické bezpečnosti (gestor).

State authority responsible for the issues of cyber security (guarantee).

Narušení **Disruption**

Incident očekávaný nebo náhodný neočekávaný nebo útok na ICT infrastrukturu, který naruší běžný chod organizace v určité lokalitě.

An incident, whether anticipated or a random unanticipated or an attack on ICT infrastructure, which disrupts the normal course of operations at a specific location.

Narušení bezpečnosti informací **Information security breach**

Narušení bezpečnosti, které vede k nežádoucímu zničení, ztrátě, změně, vyzrazení nebo zpřístupnění přenášených, uložených nebo jinak zpracovávaných chráněných informací.

Compromise of security that leads to the undesired destruction, loss, alteration, disclosure of, or access to, protected information transmitted, stored or otherwise processed.

Narušení dat **Data breach**

Narušení bezpečnosti, které vede k náhodnému nebo nezákonnému zničení, ztrátě, změně, neoprávněnému zveřejnění nebo přístupu k přenášeným, uloženým nebo jinak zpracovávaným chráněným údajům.

Compromise of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to protected data transmitted, stored or otherwise processed.

Narušení soukromí, narušení ochrany osobních údajů **Privacy breach**

Více ***Porušení soukromí***.

*See **Privacy breach**.*

Následek **Consequence**

Výsledek události působící na cíle.

Outcome of an event affecting objectives.

NATO CCD COE — **NATO Cooperative cyber defence centre of excellence**

NATO středisko pro spolupráci v kybernetické obraně (Filtry tee 12, Tallinn 10132, Estonsko, http://www.ccdcoe.org).

NATO centre for cooperation in cyber security (Filters tee 12, Tallinn 10132, Estonia, http://www.ccdcoe.org).

NATO CDMA — **NATO Cyber defence management authority**

Úřad NATO pro správu kybernetické obrany, jehož smyslem je zastřešovat a propojovat existující schopnosti kybernetické obrany v rámci Aliance.

NATO authority to manage cyber defence with the aim of providing an umbrella and interconnections for existing capabilities of cyber defence within the Alliance.

NATO CIRC – Technické centrum — **NATO computer incident response capability – Technical centre (NCIRT TC)**

Centrum technické podpory NATO CIRC – druhá úroveň. Zajišťuje schopnost reakce na incidenty, sledování incidentů, obnovení systémů a poskytuje přímou technickou podporu a pomoc provoznímu a bezpečnostnímu managementu provozovaných informačních systémů NATO.

NATO CIRC technical support centre – second level. It enables the capability to respond to incidents, monitor incidents, perform system recovery, and provides direct technical support and help to the operational and security management of the operational NATO information systems.

Neautorizovaný přístup — **Unauthorised Access**

Logický nebo fyzický přístup do sítě, systému, aplikace, k datům nebo k jinému zdroji bez povolení.

A logical or physical access without permission to a network, system, application, data, or other resources.

Nepopiratelnost — **Non-repudiation**

Schopnost prokázat výskyt údajné události nebo činnosti a zapojení entit, které ji vyvolaly.

Ability to prove the occurrence of a claimed event or action and its originating entities.

Neshoda **Nonconformity**

Nesplnění požadavku.

Non-fulfilment of a requirement.

Neustálé zlepšování **Continual improvement**

Opakovaná činnost vedoucí ke zvyšování výkonnosti.

Recurring activity to enhance performance.

Nevyžádaná pošta **Spam**

Nevyžádaná reklamní pošta, nebo jiné nevyžádané sdělení, zpravidla komerčního charakteru, které je šířeno Internetem. Nejčastěji se jedná o nabídky afrodisiak, léčiv nebo pornografie. Není-li systém dostatečně zabezpečen, může nevyžádaná pošta tvořit značnou část elektronické korespondence.

Unsolicited mail such as commercials, or another unsolicited message, usually of a commercial character, which is distributed on the Internet. Most often these are offers for aphrodisiacs, medicaments or pornography. Unless the system is adequately protected, unsolicited mail can make up a substantial part of the electronic correspondence.

Nežádoucí jednání **Adverse actions**

Akce provedené agentem hrozby na aktivu.

Actions performed by a threat agent on an asset.

Ničení klíčů **Key destruction**

Služba, která zaručuje bezpečné zničení klíčů, které nejsou nadále potřebné.

A service for the secure destruction of keys that are no longer needed.

Období přístupu **Access period**

Časové období, během něhož je povolen přístup k určitému objektu.

Time period during which access to a certain object is allowed.

Obecné zahlcení **Generic traffic flood**

Forma útoku typu **DDoS**.

*Form of a **DDoS** attack.*

Object Linking and Embedding (OLE) pro Procesní řízení (OPC) **Object Linking and Embedding (OLE) for Process Control (OPC)**

Skupina otevřených standardů, které zajišťují spolupráci mezi nesourodými provozními zařízeními, automatizací/řízením a provozními systémy.

A set of open standards developed to promote interoperability between disparate field devices, automation/control, and business systems.

Obnova dat **Data restoration/ Data recovery**

Akt znovuvytvoření či znovuzískání dat, která byla ztracena, nebo byla narušena jejich integrita. Metody zahrnují kopírování dat z archívu, rekonstrukci dat ze zdrojových dat, nebo opakované ustavení dat z alternativních zdrojů.

The act of re-creation, or reacquisition, of data lost, or whose integrity was compromised. Methods include copying from an archive, restoration of data from source data, or repeated establishment of data from alternative sources.

Obnova po havárii ICT **ICT Disaster Recovery**

Schopnost ICT prvků organizace plnit své klíčové provozní funkce na přijatelné úrovni během určeného časového úseku bezprostředně po narušení.

The ability of the ICT elements of an organisation to support its critical business functions to an acceptable level within a predetermined period following a disruption.

Obranná infrastruktura **Defence infrastructure**

Soubor objektů, staveb, pozemků a zařízení včetně nezbytných služeb, výrobních a nevýrobních systémů potřebných k zajištění jejich provozu, bez ohledu na formu vlastnictví a způsob využití, jejichž zničení, narušení nebo omezení jejich činnosti by za stavu ohrožení státu nebo za válečného stavu ohrozilo plnění úkolů: (1) Ozbrojených sil České republiky při realizaci Plánu obrany ČR a operačních plánů včetně mobilizačních opatření, (2) zpracovatelů při realizaci jejich dílčích plánů obrany a ostatních prvků bezpečnostního systému ČR, (3) spojeneckých ozbrojených sil při realizaci jejich operačních plánů, (4) ochrany obyvatelstva.

Set of objects, buildings, ground plots and equipment including necessary services, production and non-production systems needed to ensure their operation, regardless of the form of ownership and the way of utilisation; whose destruction, damage or limitation of activity would, under situation of threat to the state or a state of war, put in danger fulfilment of tasks: (1) of Armed Forces of the Czech Republic (CZE) during the implementation of the Plan of defence of CZE as well as operational plans including plans for mobilisation, (2) of experts during implementation of their partial plans of defence and other elements of security system of CZE, (3) of allied armed forces during the implementation of their operational plans, (4) of protection of population.

Obtížná zjistitelnost **Stealth**

Zabránění nebo omezení možnosti zjištění (identifikace) objektu.

Prevention or limitation of object's identification.

Odborná způsobilost **Competence**

Způsobilost používat znalosti a dovednosti k dosažení zamýšlených výsledků.

Ability to apply knowledge and skills to achieve intended results.

Odborník na systém řízení bezpečnosti informací (SŘBI) **Information security management system (ISMS) professional**

Osoba, která zavádí, implementuje, udržuje a neustále zlepšuje jeden nebo více procesů systému řízení bezpečnosti informací.

Person who establishes, implements, maintains and continuously improves one or more information security management system processes.

Odhad rizika **Risk estimation**

Proces k určení hodnot pravděpodobnosti a následků rizika.

Process to determine values of probability and consequences of risk.

Odhalení **Disclosure**

V kontextu IT obvykle používáno k vyjádření faktu, že byla odhalena data, informace nebo mechanismy, které na základě politik a technických opatření měly zůstat skryty.

In IT context it is usually used for the expression of the fact that data, information or mechanisms were disclosed which should be hidden on the basis of policies and technical measures.

Odmítnutí služby **Denial of service (DoS)**

Odmítnutí služby je technika útoku na internetové služby nebo stránky, při níž dochází k přehlcení požadavky a k pádu nebo nefunkčnosti a nedostupnosti systému pro ostatní uživatele a to útokem mnoha koordinovaných útočníků.

Denial of service is the technique of attack by many coordinated attackers on the internet services or pages resulting in flooding by requests and breakdown or unfunctionality or unavailability of the system for other users.

Odolnost systému **Resilience of a system**

Schopnost organizace, systému či počítačové sítě bez úhony přestát pokus o narušení. **Odolnost systému** je spůsobilost systému spolehlivě pracovat bez ohledu na to, jaké vlivy na něj působí z okolí systému. Systém s touto spůsobilostí se bude chovat efektivne tehdy, když některé z jeho parametrů mají náhodný charakter a jsou odlišné od těch, které se predpokladali.

The ability of an organisation, system or computer network to withstand without any harm any attempt of disruption. The resilience of a system is its capability to operate reliably without regard to impacts from the outside. A system with such a capability behaves effectively if some of its parameters have a random character and are different from the supposed ones.

Odposlech **Wiretapping**

Jedná se o jakýkoliv odposlech telefonního přenosu nebo konverzace provedený bez souhlasu obou stran, pomocí přístupu na samotný telefonní signál.

This is any tapping of a telephone transmission or conversation done without the consent of both parties, by accessing the telephone signal proper.

Odposlech / Nežádoucí odposlech **Eavesdropping**

Neautorizované zachytávání informací.

Unauthorised catching of information.

Odposlech webu **Webtapping**

Sledování webových stránek, které pravděpodobně obsahují utajované nebo citlivé informace, a lidí, jež k nim mají přístup.

Monitoring of web pages, which may contain classified or sensitive information, and of people, who have access to them.

Odpovědnost **Accountability**

Vlastnost, která zaručuje, že je možné zpětně vysledovat veškeré aktivity určité entity. Odpovědnost vyplývá z povinnosti plnit činnosti a úkoly dané popisem současných a minulých aktivit.

A property that ensures that the actions of an entity can be traced uniquely back to the entity. The accountability follows from the obligation to perform activities and tasks given by current and past activities.

Odvětvová kritéria **Sector criteria**

Technické nebo provozní hodnoty k určování prvku kritické infrastruktury v odvětvích energetika, vodní hospodářství, potravinářství a zemědělství, zdravotnictví, doprava, komunikační a informační systémy, finanční trh a měna, nouzové služby a veřejná správa.

Technological or operational values to determine an element of critical infrastructure in the sectors of energy, water management, food and agriculture, health, transport, communication and information systems, financial market and currencies, emergency services and public administration.

Ochrana dat **Data protection**

Administrativní, technická, procedurální, personální nebo fyzická opatření implementovaná za účelem ochrany dat před neautorizovaným přístupem nebo porušením integrity dat.

Administrative, technological, procedural, staffing or physical measures implemented in order to protect data against an unauthorised access or against corruption of data integrity.

Ochrana kritické infrastruktury **Critical infrastructure protection**

Opatření zaměřená na snížení rizika narušení funkce prvku kritické infrastruktury.

Measures aimed at lowering the risk of corruption of an element of the critical infrastructure.

Ochrana před kopírováním **Copy protection**

Použití speciální techniky k detekci nebo zamezení neautorizovaného kopírování dat, software a firmware.

Use of a special technique for the detection or prevention of unauthorised copying of data, software and firmware.

Ochrana souboru **File protection**

Implementace vhodných administrativních, technických nebo fyzických prostředků k ochraně před neautorizovaným přístupem, modifikací nebo vymazáním souboru.

Implementation of suitable administrative, technological or physical means for the protection against unauthorised access, modification or erasure of a file.

Ochrana soukromí **Privacy protection**

Konkrétní volby uskutečněné subjektem osobně identifikovatelných informací (PII), jak by jeho PII měly být zpracovávány pro konkrétní účel.

Specific choices made by a personally identifiable information (PII) principal about how their PII should be processed for a particular purpose

Online služba **Online service**

Služba, která je nasazena na hardware, software nebo jejich kombinaci a je poskytována prostřednictvím komunikační sítě. Za online služby se považuje např. internetový vyhledávač, online zálohování dat, internetový e-mail nebo software jako služba (SaaS).

A service which is implemented by hardware, software or a combination of these, and provided over a communication network. Online services include, for example,

a search engine, online backup services, Internet-hosted email, and software as a service (SaaS).

Opatření **Measure**

Prostředky modifikující riziko, včetně politik, strategií, postupů, směrnic, obvyklých postupů (praktik) nebo organizačních struktur, které mohou být administrativní, technické, řídicí nebo právní povahy.

A measure that is modifying risk, including all policies, strategies, procedures, directives, usual procedures (practices) or organisational structures, which may be of an administrative, technological, management or legal character.

Opatření aplikační bezpečnosti **Application Security Control (ASC)**

Datová struktura, která obsahuje přesný výčet a popis bezpečnostních úkonů a s nimi spojených kontrolních měření, které jsou prováděny v určitém bodě životního cyklu aplikace.

A data structure containing a precise enumeration and description of security activities and the associated verification measurement to be performed at a specific point in an application's life cycle.

Opatření ochrany soukromí **Measures to protect privacy**

Opatření, která ošetřují rizika porušení soukromí snížením pravděpodobnosti jejich výskytu nebo snížením jejich následků.

Measures that treat privacy risks by reducing their likelihood or their consequences.

Open software foundation **Open software foundation (OSF)**

Nezisková organizace založená v roce 1988 na základě zákona „U. S. Cooperative Research Act of 1984“ proto, aby vytvořila otevřenou normu pro realizaci operačního systému UNIX.

A not-for-profit organization founded in 1988 under the U.S. National Cooperative Research Act of 1984 to create an open standard for an implementation of the UNIX operating system.

Operační systém **Operating system**

Programové prostředky, které řídí provádění programů a které mohou poskytovat různé služby, např. přidělování prostředků, rozvrhování, řízení vstupů a výstupů a správu dat. Příkladem operačního systému je systém MS Windows, LINUX, UNIX, Solaris apod.

Software which controls programme executions and which can offer various services, e.g. assignment of devices, scheduling, control of input and output and data administration. Examples of operating systems are the MS-DOS system, LINUX, UNIX, Solaris, and others.

Oprávnění, přístupové oprávnění **Privilege, Access right / Permission**

Oprávnění určitého subjektu využívat určitý zdroj.

Authorisation of a subject to access a resource.

Organizace **Organisation**

Osoba nebo skupina osob, které mají své vlastní funkce s odpovědnostmi, pravomocemi a vztahy, pomocí nichž mohou dosáhnout svých cílů.

Person or group of people that has its own functions with responsibilities, authorities and relationships to achieve its objectives.

Organizační opatření **Organisational Measures**

Procesy, které shromažďují a využívají informace k hodnocení výkonu různých organizačních zdrojů, jako jsou lidské, fyzické, finanční a také organizace jako celek ve světle sledovaných organizačních strategií, přičemž ovlivňují chování organizačních zdrojů při implementaci organizačních strategií.

Processes that collect and use the information to evaluate the performance of various organisational resources, as human, physical, financial ones, as well as of the organisation as a whole in the light of the organisational strategies and while doing so, they influence the behaviour of information resources during the implementation of organisational strategies.

Orgán správy a řízení **Governing body**

Osoba nebo skupina osob zodpovědných za výkonnost a konformitu organizace.

Person or group of people who are accountable for the performance and conformance of the organisation.

Osobně identifikovatelné informace (údaje) **Personally identifiable information (data) (PII)**

Jakákoli informace, která může být použita k určení totožnosti subjektu PII, kterého se týká, nebo může být přímo nebo nepřímo spojena se subjektem PII.

Any information that can be used to identify the PII principal to whom such information relates, or is or might be directly or indirectly linked to a PII principal.

Osobní počítač **Computer, personal computer (PC)**

V souladu se zněním CSN 36 9001 se jedná o „stroj na zpracování dat provádějící samočinné posloupnosti různých aritmetických a logických operací". Jinými slovy: stroj charakterizovaný prací s daty, která probíhá podle předem vytvořeného programu uloženého v jeho paměti.

In accordance with the wording of CSN 36 9001 this is "a data processing machine executing independent sequences of various arithmetic and logical operations." In other words: a machine characterised by processing data according to a previously created programme stored in its memory.

Osobní identifikační číslo (PIN) **Personal identification number (PIN)**

Číselný kód, který se používá k ověření totožnosti.

Numeric code used to authenticate an identity.

Osobní údaje **Personal data**

Veškeré informace o identifikované nebo identifikovatelné fyzické osobě (tj. subjektu údajů); identifikovatelnou fyzickou osobou je fyzická osoba, jejíž totožnost lze přímo či nepřímo určit, zejména odkazem na určitý identifikátor, například jméno, identifikační číslo, adresu, síťový identifikátor nebo na jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby.

Any information relating to an identified or identifiable natural person (i.e. data subject); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Otevřené bezpečnostní prostředí **Open-security environment (OSE)**

Prostředí, ve kterém je ochrana dat a zdrojů před náhodnými nebo úmyslnými činy dosažena použitím normálních provozních postupů.

Environment where data and source protection against accidental or intentional acts is achieved by using standard operational procedures.

Otevřený komunikační systém **Open communication system**

Představuje (zahrnuje) globální počítačovou síť včetně jejích funkcionalit, podporovanou jak soukromými společnostmi, tak veřejnými institucemi.

It represents (includes) a global computer network including all its functions and supported both by private companies and public institutions.

Otisk **Digest**

Výsledek hash operace.

Result of a hash operation.

Outsourcování **Outsourcing**

Pořízení služeb (včetně produktů anebo bez nich), které využívají zdroje dodavatele k podpoře určitého organizačního procesu namísto zdrojů vlastních.

Acquisition of services (with or without products) in support of a business function for performing activities using supplier's resources rather than the acquirer's.

Ověření totožnosti **Authentication**

Poskytnutí záruky, že udávaná charakteristika určité entity je správná.

Provision of assurance that a claimed characteristic of an entity is correct.

Ověření totožnosti dat **Data authentication**

Proces používaný k ověření integrity dat (např. ověření, že přijatá data jsou identická s odeslanými daty, ověření, že program není infikován virem).

Process used to verify data integrity (verification that received and sent data are identical, verification that programme is not infected by a virus, for example).

Ověření totožnosti entity / identity **Entity / identity Authentication**

Ověření, že určitá entita je tou entitou, za kterou se vydává. Autentizace entity.

A verification that an entity is the one claimed.

Ověření totožnosti klíče **Key authentication**

Proces k ověření totožnosti (autentizace) entity uživatele, kterým nemusí nutně být pouze člověk. Uživatel je pokládán za oprávněného, pokud prokáže znalost, oprávněné vlastnostnictví klíče.
Proces ověření, že daný veřejný klíč určité osoby skutečně patří této osobě.

A process to verify the identity (authentication) of a user, the user not necessarily being human. A user is considered authenticated if the ownership of a key is justified.
Process of verification that the public key truly belongs to that person.

Ověření totožnosti zprávy **Message authentication**

Ověření, že zpráva byla odeslána pravým původcem zamýšlenému příjemci a že tato zpráva nebyla při přenosu změněna. Ověření totožnosti zdroje informací – odesílatele zprávy. Častým způsobem se stává využití digitálního podpisu.

Verification that message was sent by the alleged originator to the intended receiver and that this message was not changed in transmission. Verification of the identity of information source-sender of the message. Frequently, digital signature is used.

Ovladač DC Serva **DC Servo Driver**

Ovladač určený pro stejnosměrné servomotory, který vysílá příkazy do motoru a získává údaje o otáčkách či úhlu motoru z enkodéru nebo resolveru.

A driver that works specifically for direct-current servo motors. It transmits commands to the motor and receives feedback from the servo motor resolver or encoder.

Paket **Packet**

Blok dat přenášený v počítačových sítích, které používají technologii "přepojování paketů". Paket se skládá z řídicích dat a z uživatelských dat. Řídicí data obsahují informace nutné k doručení paketu (adresa cíle, adresa zdroje, kontrolní součty,

informace o pořadí paketu). Uživatelská data obsahují ta data, která mají doručena do cíle (cílovému adresátovi).

Block of data transferred in computer networks and using the technology of "packet switching". A packet consists of control data and user data. Control data contain information necessary for packet delivery (destination address, source address, checksums, and information on packet priority). User data contain those data items, which should be delivered to the target (destination addressee).

Pár klíčů **Key pair**

Dvojice sestávající z veřejného klíče a privátního klíče pro asymetrickou šifru.

Pair consisting of a public key and a private key associated with an asymmetric cipher.

Pasivní hrozba **Passive threat**

Hrozba zpřístupnění informací, aniž by došlo ke změně stavu systému zpracování dat nebo počítačové sítě.

The threat of making access to data without actually changing the state of the data processing system or the computer network.

Páteřní síť **Core network**

Ústřední část telekominikační sítě, která poskytuje různé služby zákazníkům, připojených přes přístupovou síť.

The central part of a telecommunication network that provides various services to customers who are connected by the access network.

Penetrační testování **Penetration testing**

Zkoumání funkcí počítačového systému a sítí s cílem najít slabá místa počítačové bezpečnosti tak, aby bylo možno tato slabá místa odstranit.

Analysis of functions of a computer system and networks with the objective of finding out weak spots in computer security so that these could be removed.

Periferní zařízení **Peripheral equipment**

Zařízení, které je řízeno počítačem a může s ním komunikovat, např. jednotky vstupu/výstupu a pomocné paměti.

Equipment controlled by a computer and able to communicate with it, e.g. input/output devices and auxiliary memory.

Pharming (rhybaření) **Pharming**

Podvodná metoda používaná na Internetu k získávání citlivých údajů od obětí útoku. Principem je napadení ***DNS*** a přepsání ***IP*** adresy, což způsobí přesměrování klienta na falešné stránky internetbankingu, e-mailu, sociální sítě, atd. po zadání ***URL*** do prohlížeče. Tyto stránky jsou obvykle k nerozeznání od skutečných stránek banky a ani zkušení uživatelé nemusejí poznat tuto záměnu (na rozdíl od příbuzné techniky phishingu).

The fraudulent method used on the Internet to obtain sensitive data from the victim of the attack. The principle is an attack on DNS and rewriting the IP address, which results in redirecting the client to a false address of internet banking, email, social network, etc., after inserting the URL into the browser. These pages are as a rule indistinguishable from the real pages of a bank and even experienced users may not recognise this change (unlike the related technique of phishing).

Phishing („rybaření", „rhybaření", „házení udic") **Phishing**

Podvodná metoda, usilující o zcizování digitální identity uživatele, jeho přihlašovacích jmen, hesel, čísel bankovních karet a účtu apod. za účelem jejich následného zneužití (výběr hotovosti z konta, neoprávněný přístup k datům atd.). Vytvoření podvodné zprávy, šířené většinou elektronickou poštou, jež se snaží zmíněné údaje z uživatele vylákat. Zprávy mohou být maskovány tak, aby co nejvíce imitovaly důvěryhodného odesílatele. Může jít například o padělaný dotaz banky, jejíchž služeb uživatel využívá, se žádostí o zaslání čísla účtu a PIN pro kontrolu (použití dialogového okna, předstírajícího, že je oknem banky – tzv. spoofing). Tímto způsobem se snaží přistupující osoby přesvědčit, že jsou na známé adrese, jejímuž zabezpečení důvěřují (stránky elektronických obchodů atd.). Tak bývají rovněž velice často zcizována například čísla kreditních karet a jejich PIN.

A fraudulent method having the objective of stealing the digital identity of a user, the sign-on names, passwords, bank account numbers and accounts etc. to subsequently misuse these (drawing cash from the account, unauthorised access to data etc.). Creation of a fraudulent message distributed mostly by electronic mail trying to elicit the mentioned data from the user. The messages may be masqueraded to closely imitate a trustworthy sender. It may be a forged request from a bank whose services the user accesses with a request to send the account number and PIN for a routine check (use of the dialogue window purporting to be

a bank window – so-called spoofing). Thus the fraudster tries to convince accessing persons that they are at the right address, whose security they trust (pages of electronic shops etc.). Also, very often credit card numbers and PINS are stolen in this fashion.

Phreaker **Phreaker**

Osoba provádějící „hacking“ prostřednictvím telefonu. Používáním různých triků manipulujících se službami telefonních společností.

Person doing "hacking" on the phone, using various tricks manipulating the services of telephone companies.

Phreaking **Phreaking**

Napojení se na cizí telefonní linku v rozvodnicích, veřejných telefonních budkách nebo přímo na nadzemní/podzemní telefonní vedení, díky čemuž lze: (1) volat zadarmo kamkoliv, (2) surfovat zadarmo po internetu a (3) odposlouchávat cizí telefonní hovory. Platba za hovor jde samozřejmě na účet oběti (registrovaného uživatele linky anebo telekomunikační společnosti). Za phreaking se považuje i nabourávání se různými metodami do mobilní sítě nebo výroba odposlouchávacích zařízení.

Denotation for tapping into a somebody else's telephone line in distribution panels, public telephone booths or directly in the ground/below ground telephone lines and thanks to these: (1) it is possible to call anywhere free of charge, (2) surf the internet free of charge, and (3) listen to somebody else's telephone conversations. Payment for the call is of course at the cost of the victim (registered user of the line, or the telephone company). Tapping into a mobile network by using various methods or the manufacture of listening devices are also considered phreaking.

Ping **Ping**

Nástroj používaný v počítačových sítích pro testování dosažitelnosti počítače nebo cílové sítě přes IP sítě. Ping měří čas návratu odezvy a zaznamenává objem ztracených dat (packets).

Instrument used in computer networks for testing computer availability over IP networks. Ping measures the time of response and records the volume of lost data (packets).

Ping smrti **Ping of death**

Typ útoku na počítač, který zahrnuje chybně odeslaný nebezpečný **ICMP** paket, např. odesílání IP paketu většího než maximální velikost IP paketu, který zhroutí cílový počítač nebo odesláním paketu docílí překročení maximální velikosti **IP** paketů, což způsobí selhání systému.

*Type of an attack on a computer, which includes a dangerous **ICMP** packet sent in error e.g. a packet sent larger than the maximum size of IP packet which collapses the target computer, or, by sending the packet the attacker exceeds the maximum size of **IP** packets which results in the failure of the system.*

Pivoting **Pivoting**

Využití systému, který se útočníkovi úspěšně povedlo napadnout, k napadení dalších systémů ve společné síti.

Use of a system that has been successfully attacked, to attack other systems in the shared network.

Plán bezpečnosti **Security Plan**

Oficiální dokument, který poskytuje přehled bezpečnostních požadavků na informační systém a popisuje realizovaná, nebo plánovaná bezpečnostní opatření, která tyto požadavky splňují.

A formal document that provides an overview of the security requirements for the information system and describes the security controls in place or planned for meeting those requirements.

Plán/program bezpečnosti informací **Information Security Programme / Plan**

Oficiální dokument, který poskytuje přehled bezpečnostních požadavků na informační bezpečnost organizací a popisuje realizovaná, nebo plánovaná bezpečnostní opatření, která tyto požadavky splňují.

A formal document that provides an overview of the security requirements for an organisation-wide information security programme and describes the programme management controls and common controls in place or planned for meeting those requirements.

Plán kontinuity činností **Business continuity plan (BCP)**

Dokumentované postupy, které provádí organizace, aby reagovala, obnovila, pokračovala a zotavila své činnosti na předem stanovenou úroveň provozu po narušení.

Documented procedures that guide organisations to respond, recover, resume, and restore to a pre-defined level of operation following disruption.

Plán obnovy / Havarijní plán **Disaster recovery plan / Contingency plan**

Plán pro záložní postupy, odezvu na nepředvídanou událost a obnovu po havárii.

Plan for backup procedures, response to an unforeseen event and recovery after a disaster.

Plán obnovy po havárii ICT **ICT disaster recovery plan (ICT DRP)**

Jasně definovaný a zdokumentovaný plán, který obnoví schopnosti ICT, když dojde k narušení. Poznámka: V některých organizacích se nazývá plán kontinuity ICT.

Clearly defined and documented plan which recovers ICT capabilities when a disruption occurs. Note: It is called ICT continuity plan in some organizations.

Plán řízení rizik **Risk management plan**

Schéma v rámci managementu rizik specifikující přístup, dílčí části managementu a zdroje, které se mají použít k managementu rizik.

Scheme in the framework of risks specifying access, parts of management and sources to be used for risk management.

Platforma jako služba **Platform as a Service (PaaS)**

Možnost daná uživateli umístit do infrastruktury cloudu uživatelské či získané aplikace vytvořené pomocí programovacích jazyků, knihoven, služeb a nástrojů vytvořených uživatelem. Uživatel neřídí ani neovládá základní strukturu cloudu včetně sítě, serverů, operačních systémů nebo ukládacích zařízení, ale řídí rozmístěné aplikace a případně nastavené konfigurace pro aplikační prostředí.

The capability provided to the user to deploy onto the cloud infrastructure user-made or acquired applications created by programming languages, libraries, services, and tools supported by the user. The user does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.

Plošné visílání **Broadcast**

Viz **Broadcast**

*See **Broadcast***

Počítačová / Kybernetická šikana **Cyberbullying**

Druh šikany, který využívá elektronické prostředky, jako jsou mobilní telefony, e-maily, pagery, internet, blogy a podobně k zasílání obtěžujících, urážejících či útočných mailů a SMS, vytváření stránek a blogů dehonestujících vybrané jedince nebo skupiny lidí.

Type of bullying using electronic means such as mobile phones, emails, pagers, internet, blogs and similar for sending harassing, offending or attacking emails and text messages, the creation of pages and blogs defaming selected individuals or groups of people.

Počítačová bezpečnost **Computer security (COMPUSEC)**

Obor informatiky, který se zabývá zabezpečením informací v počítačích (odhalení a zmenšení rizik spojených s používáním počítače). Počítačová bezpečnost zahrnuje:
(1) zabezpečení ochrany před neoprávněným manipulováním se zařízeními počítačového systému,
(2) ochranu před neoprávněnou manipulací s daty,
(3) ochranu informací před krádeží (nelegální tvorba kopií dat) nebo poškozením,
(4) bezpečnou komunikaci a přenos dat (kryptografie),
(5) bezpečné uložení dat,
(6) dostupnost, celistvost a nepodvrhnutelnost dat.
Je to také zavedení bezpečnostních vlastností hardwaru, firmwaru a softwaru do počítačového systému, aby byl chráněn proti neoprávněnému vyzrazení, úpravě, změnám nebo vymazání skutečností nebo aby jim bylo zabráněno nebo proti odmítnutí přístupu. Ochrana dat a zdrojů před náhodnými nebo škodlivými činnostmi.

Branch of informatics dealing with securing of information in computers (discovering and lowering risks connected to the use of the computer). Computer security includes:
(1) enabling protection against unauthorised manipulation with the devices of a computer system,
(2) protection against unauthorised data manipulation,
(3) protection of information against pilferage (illegal creation of data copies),
(4) secure communication and data transfer (cryptography),

(5) secure data storage,
(6) availability, integrity and authenticity of data.
It is also the introduction of security properties of hardware, firmware and software into the computer system so that it is protected against unauthorised disclosure, amendments, changes or erasure of facts or to prevent these, or against access denial — protection of data and sources against accidental or harmful activities.

Počítačová kriminalita / Kybernetická kriminalita **Computer crime / Cyber crime**

Zločin spáchaný pomocí systému zpracování dat nebo počítačové sítě nebo přímo s nimi spojený.

Crime committed using a data processing system or computer network or directly related to them.

Počítačová síť **Computer network**

Soubor počítačů spolu s komunikační infrastrukturou (komunikační linky, technické vybavení, programové vybavení a konfigurační údaje), jejímž prostřednictvím si (počítače) mohou vzájemně posílat a sdílet data.

A collection of computers together with a communication infrastructure (communication lines, hardware, software and configuration data) through which they (computers) can send and share data with each other.

Počítačové obtěžování **Cyber harassment**

Internetové obtěžování (i jednotlivý případ), zpravidla obscénní či vulgární povahy. Často bývá součástí cyberstalkingu. Více také **Cyberstalking**.

*Internet harassment (even an individual case) usually of an obscene or vulgar character. It is often part of cyberstalking. See also **Cyberstalking**.*

Počítačový podvod **Computer fraud**

Podvod spáchaný pomocí systému zpracování dat nebo počítačové sítě nebo přímo s nimi spojený.

Fraud committed using a data processing system or computer network or directly related to them.

Počítačový virus **Computer virus**

Počítačový program, který se replikuje připojováním své kopie k jiným programům. Může obsahovat část, která ho aktivuje, pokud dojde ke splnění

některých podmínek (např. čas) v hostitelském zařízení. Šíří se prostřednictvím Internetu (elektronická pošta, stahování programů z nespolehlivých zdrojů), pomocí přenosných paměťových médií apod. Toto dělá za účelem získání různých typů dat, zcizení identity, znefunkčnění počítače, atd.

A computer programme, which replicates itself by attaching its copies to other programmes. It may contain a part which activates it when certain conditions are met (e.g. time) in the host device. It is distributed using the Internet (electronic mail, downloading programmes from unreliable sources), using mobile storage media and others. This is done to obtain various types of data, for identity theft, for putting the computer out of operation, etc.

Podepisování **Signing**

Proces vytváření podpisu, jehož vstupem je zpráva a podpisový klíč signatáře a výstupem je podpis.

Signature generation process that takes a message and a signing key of a signer to produce a signature.

Podnikový informační systém **Enterprise Resource Planning (ERP) System**

Systém, kerý propojuje informace napříč podnikem včetně řízení lidských zdrojů, financí, výroby a logistiky a rovněž zajišťuje propojení organizace s jejími zákazníky a dodavateli.

A system that integrates enterprise-wide information including human resources, financials, manufacturing and logistics as well as connects the organisation to its customers and suppliers.

Podrobná inspekce paketů **Deep packet inspection (DPI)**

Forma filtrování paketů v počítačové síti, která prohlíží datovou část (a možná také hlavičku) paketu při průchodu inspekčním bodem, a hledá nesoulad s protokolem, viry, spam, průniky nebo také definovaná kriteria pro rozhodnutí, zda paket může projít či zda je nutné přesměrování na jiné místo určení, nebo za účelem sběru statistických informací.

A form of computer network packet filtering that examines the data part (and possibly also the header) of a packet as it passes an inspection point, searching for protocol non-compliance, viruses, spam, intrusions, or defined criteria to decide whether the packet may pass or if it needs to be routed to a different destination, or, for collecting statistical information.

Podsíť **Subnet**

Segment sítě, který sdílí společnou složku adresy.

Segment of a network that shares a common address component.

Podstoupení rizik **Risk retention**

Přijetí břemene ztráty nebo prospěchu ze zisku vyplývajícího z určitého rizika.

Accepting the burden of a loss or benefit from profit ensueing from a certain risk.

Podvod **Scam**

Podvod nebo zneužití důvěry.

Fraud or confidence trick.

Podvržení IP adresy **IP spoofing**

Podvržení zdrojové IP adresy u zařízení (počítače), které iniciuje spojení (s příjemcem) za účelem zatajení skutečného odesilatele. Tato technika bývá využívána především v útocích typu **DoS**.

*Spoofing of the source IP address on a device (a computer) which triggers connection (with a recipient) in order to hide the real sender. This technique is used particularly in attacks of **DoS** type.*

Pokročilá a trvalá hrozba **Advanced persistent threat (APT)**

Typickým účelem APT je dlouhodobé a vytrvalé infiltrování a zneužívání cílového systému za pomoci pokročilých a adaptivních technik (na rozdíl od běžných jednorázových útoků).

Typical purpose of APT is a long-term and persistent infiltration into, and abuse of, the target system using advanced and adaptive techniques (unlike usual single attacks).

Politika **Policy**

Celkový záměr a směrování organizace, formálně vyjádřené jejím vrcholovým vedením.

The overall intention and direction of an organisation, as formally expressed by its top management.

Politika ochrany soukromí **Privacy protection policy**

Celková koncepce, pravidla a závazky, formálně vyjádřené správcem osobně identifikovatelných informací (PII), které se týkají zpracování PII v konkrétním prostředí.

Overall concepts, rules and commitment, as formally expressed by the personally identifiable information (PII) controller related to the processing of PII in a particular setting.

Politika řízení přístupu **Access control policy**

Soubor zásad a pravidel, která definují podmínky pro poskytnutí přístupu k určitému objektu.

Set of principles and rules, which define conditions to provide access to a certain object.

Politika řízení rizik **Risk management policy**

Prohlášení o celkových záměrech a směrování organizace týkající se řízení rizik.

Statement on the overall intentions and direction of an organisation related to risk management.

Poplašná zpráva **Hoax**

Snaží se svým obsahem vyvolat dojem důvěryhodnosti. Informuje např. o šíření virů nebo útočí na sociální cítění adresáta. Může obsahovat škodlivý kód nebo odkaz na internetové stránky se škodlivým obsahem.

It tries to create an impression of trustworthiness by its content. It informs, for example, about the spread of viruses or it inveighs against the social feeling of the addressee. It may contain harmful code or a link to internet pages with harmful content.

Port **Port**

Používá se při komunikaci pomocí protokolů **TCP** či **UDP**. Definuje jednotlivé síťové aplikace běžící v rámci jednoho počítače. Může nabývat hodnot v rozmezí 0 – 65535. Například webové stránky jsou obvykle dostupné na portu 80, server pro odesílání mailové pošty na portu 25, ftp server na portu 21. Tyto hodnoty je

možné změnit a u některých síťových služeb správci někdy záměrně nastavují jiná než běžně používaná čísla portů kvůli zmatení případného útočníka.

It is used for communication using the TCP or UDP protocols. It defines the individual net applications running on one computer. It may take on values in the range 0 – 65535. For example, web pages are usually accessible on port 80, server to send out electronic mail on port 25, FTP server on port 21. These values may be changed, and with some network services, the administrators sometimes set other than normally used port numbers to deceive a potential attacker.

Port scanner **Port scanner**

Program na testování otevřených portů.

Programme to test open ports.

Port Trunking / Teaming **Port Trunking / Teaming**

Linkové agregace několika fyzických portů, které dohromady vytváří jeden logický kanál.

Linked aggregation of several physical ports making up one logical channel.

Portál **Portal**

Informace (obsahové oblasti, stránky, aplikace, data z vnějších zdrojů) soustředěná v jednom ústředním místě, ke kterým je přístup prostřednictvím webového prohlížeče.

Information (content regions, pages, applications, and data from external sources) concentrated in one central place, which can be accessed using a web browser.

Portál veřejné správy **Public sector portal**

Informační systém vytvořený a provozovaný se záměrem usnadnit veřejnosti dálkový přístup k pro ni potřebným informacím z veřejné správy a komunikaci s ním.

Information system created and operated with the intention of facilitating remote access to, and communication with, the necessary information from the public administration.

Porušení, prolomení **Breach**

Ohrožení či zneužití bezpečnosti informací nebo porušení politiky bezpečnosti informací.

A breach or an abuse of information security or a breach of a security policy.

Porušení ochrany osobních údajů **Personal data breach**

Porušení ochrany a zabezpečení osobních údajů, které vede k náhodnému nebo protiprávnímu zničení, ztrátě, změně, prozrazení nebo zveřejnění přenášených, uložených nebo jinak zpracovávaných osobních údajů.

A breach of protection and security of personal data leading to the accidental or unlawful destruction, loss, alteration, disclosure or publication of personal data transmitted, stored or otherwise processed.

Porušení ochrany údajů **Breach of Data Protection**

Porušení bezpečnosti, úmyslné i neúmyslné, které vede ke zničení, ztrátě, změně, neoprávněném odhalení nebo zpřístupnění chráněných dat během jejich přenosu, uložení nebo zpracování.

A breach of security, intentional or unintentional that leads to the destruction, loss, alteration, unauthorised disclosure of, or access to, protected data during transmission or procession.

Porušení soukromí **Privacy breach**

(1) Stav, kdy při zpracování osobně identifikovatelné informace není dodržen jeden nebo více požadavků na ochranu soukromí.
(2) Porušení zabezpečení, které vede k náhodnému nebo protiprávnímu zničení, ztrátě, změně, prozrazení, nebo zveřejnění přenášených, uložených nebo jinak zpracovávaných osobních údajů.

(1) A state where personally identifiable information is processed in violation of one or more relevant privacy safeguarding requirements.
(2) A breach of security leading to the accidental or unlawful destruction, loss, alteration, disclosure of, or publication of personal data transmitted or otherwise processed.

Porušení zabezpečení osobních údajů **Privacy breach**

Více ***Porušení soukromí***.

See **Privacy breach**.

Pořízení bitového obrazu **Imaging**

Proces vytvoření bitové kopie elektronického paměťového média.

Process of creating a bitwise copy of an electronic storage medium.

Poskytovatel aplikačních služeb **Application service provider**

Provozovatel, který poskytuje hostované softwarové řešení poskytující aplikační služby, které zahrnuje modely poskytování založené na webu nebo klient-server. Příklad: Provozovatelé online her, poskytovatelé kancelářských aplikací a poskytovatelé online úložišť.

Operator who provides a hosted software solution that provides application services which includes web based or client-server delivery models. Example: Online game operators, office application providers and online storage providers.

Poskytovatel služby **Service provider**

Každá fyzická nebo právnická osoba, která poskytuje některou ze služeb informační společnosti.

Any natural or legal person providing any of the services of the information society.

Poskytovatel služby autorizačních údajů **Credential service provider (CSP)**

Důvěryhodná entita spojená s určitou doménou, která odpovídá za správu pověření vydaných v této doméně.

Trusted entity related to a particular domain responsible for management of credentials issued in that domain.

Poskytovatel služeb internetu **Internet service provider (ISP)**

Organizace, která poskytuje uživatelům internetové služby a umožňuje svým zákazníkům přistupovat k internetu.

The organisation that provides Internet services to users and enables its customers access to the Internet.

Poskytovatel služeb veřejného cloudu **Public cloud service provider**

Strana, která zpřístupňuje cloudové služby podle modelu veřejného cloudu.

Party which makes cloud services available according to the public cloud model

Posouzení rizik (ochrany) soukromí **Privacy risk assessment**

Celkový proces identifikace rizika, analýzy rizika a hodnocení rizika s ohledem na zpracování osobně identifikovatelných informací (PII); viz též posouzení vlivu na ochranu osobních údajů.

An overall process of risk identification, risk analysis and risk evaluation with regard to the processing of personally identifiable information (PII); see also data protection impact assessment.

Postoj k riziku **Risk attitude**

Přístup organizace k posuzování rizika a případně zabývání se rizikem, k spoluúčasti, převzetí nebo odmítání rizika.

Approach of an organisation towards assessing risk and, also, dealing with risk, sharing risk, taking over or refusal of risk.

Postup **Procedure**

Specifikovaný způsob provádění činnosti nebo procesu.

Specified method of executing an activity or process.

Postup výměny klíčů **Key exchange procedure**

Procedura ustavení společného kryptografického klíče. Metoda využívá asymetrickou kryptografii. Tato metoda umožňuje přes nezabezpečený kanál vytvořit mezi komunikujícími stranami symetrický šifrovací klíč bez předchozí výměny tajného šifrovacího klíče.

Procedure to establish a common cryptographic key. The method uses asymmetric cryptography. This method allows establishing a symmetric enciphering key among the communicating parties using an insecure channel, without the need for prior exchange of a secret enciphering key.

Posuzování rizika **Risk assessment**

Celkový proces identifikace rizika, analýzy rizika a hodnocení rizika.

Overall process of risk identification, risk analysis and risk evaluation.

Poškození dat **Data corruption**

Náhodné nebo záměrné porušení integrity dat.

Accidental or intentional corruption of data integrity.

Potenciální elektronický důkaz **Potential electronic evidence**

Informace nebo data, uložená nebo přenesená v binárním tvaru, u kterých proces analýzy doposud neprokázal, že jsou relevantní pro vyšetřování.

Information or data, stored, or transmitted in binary form, for which it has not yet been determined, through the process of analysis, to be relevant to the investigation.

Povolení přístupu **Access permission**

Všechna přístupová práva subjektu vzhledem k určitému objektu.

All access rights of a subject related to a certain object.

Potvrzení správnosti **Validation**

Potvrzení prostřednictvím objektivních důkazů, že byly splněny požadavky pro konkrétní zamýšlené použití nebo aplikaci.
Poznámka 1: Validace se provádí s cílem zajistit, aby proces odpovídal svému účelu, tj. aby bylo zajištěno, že proces, jak je implementován, poskytuje očekávané výsledky konzistentním, opakovatelným a reprodukovatelným způsobem.

Confirmation, through the provision of objective evidence, that the requirements for a specific intended use or application have been fulfilled
Note 1 to entry: Validation is carried out on a process to ensure that it is fit for purpose, i.e. to ensure that the process, as implemented, produces expected results in a consistent, repeatable, and reproducible manner.

Požadavek **Requirement**

Potřeba nebo očekávání, které jsou stanovené, obecně předpokládané nebo závazné.

Need or expectation that is stated, generally implied or obligatory.

Požadavky na službu **Service requirement**

Potřeby zákazníka a uživatelů služby včetně požadavků na úroveň služby a potřeby poskytovatele služby.

Needs of customers and users of services, including requirements for the service level and the needs of a service provider.

Požadavky na zabezpečení (ochrany) soukromí **Privacy safeguarding requirements**

Soubor požadavků, které musí organizace vzít v úvahu při zpracování osobně identifikovatelných informací, s ohledem na ochranu soukromí osobně identifikovatelných informací.

Set of requirements an organisation has to take into account when processing personally identifiable information with respect to the privacy protection of personally identifiable information

Pracovní stanice **Workstation**

Funkční jednotka, obvykle se specifickými výpočetními schopnostmi, která obsahuje uživatelské vstupní a výstupní jednotky, např. programovatelný terminál nebo samostatný počítač.

Functional unit, usually with specific computing capabilities, having user input and output devices, such as. a programmable terminal or a stand-alone computer.

Pravděpodobnost, možnost výskytu **Likelihood**

Možnost, že něco nastane.

The possibility of something happening.

Pretexting **Pretexting**

Druh sociálního inženýrství spočívající ve vytváření a využívání smyšleného scénáře, s cílem přesvědčit oběť k učinění potřebné akce, či k získání potřebné informace. Jedná se o skloubení lži s pravdivou informací, získanou dříve.

One kind of social engineering. It creates and uses fictitious screenplay with the objective of convincing the victim to perform the required action or to obtain the required information.

Prevence průniku **Intrusion prevention**

Formální process aktivního působení s cílem předcházet narušení.

Formal process of actively responding to prevent intrusions.

Prioritní volání **Priority call**

Telefonní volání uskutečněné specifickým koncovým zařízením v případě nouze, které by mělo být přednostně odbaveno omezením veřejného provozu.

A phone call by specific terminals in the event of emergencies, which should be handled with priority by restricting public calls.

Privátní IP adresa **Private IP address**

Skupiny ***IP*** adres definované v RFC 1918 jako vyhrazené pro použití ve vnitřních sítích. Tyto IP adresy nejsou směrovatelné z internetu. Jedná se o následující rozsahy: 10.0.0.0 – 10.255.255.255, 172.16.0.0 – 172.31.255.255 a 192.168.0.0 – 192.168.255.255.

*Groups of **IP** addresses defined under RFC 1918 as reserved for use in internal networks. These IP addresses are not routed from the internet. Here are these ranges: 10.0.0.0 – 10.255.255.255, 172.16.0.0 – 172.31.255.255 and 192.168.0.0 – 192.168.255.255.*

Problém **Problem**

Primární příčina jednoho nebo více incidentů.

Primary cause of one or more incidents.

Proces **Process**

Soubor aktivit majících vzájemný vztah nebo vzájemně na sebe působících a přeměňujících vstupy na výstupy.

Set of interrelated or interacting activities, which transforms inputs into outputs.

Proces řízení rizik **Risk management process**

Systematické uplatňování politik řízení, postupů a praktik pro sdělování, konzultování, určování kontextu a zjišťování, analyzování, hodnocení, ošetřování, monitorování a přezkoumávání rizik.

Systematic application of management policies, procedures and practices to the activities of communicating, consulting, establishing the context and identifying, analysing, evaluating, treating, monitoring and reviewing risk.

Procesní řízení **Process Control**

Disciplína, věnující se architektuře, mechanismům a algoritmům, které řídí výstupy specifického procesu v žádaných mezích. K tomuto cíli se využívají prostředky průmyslové automatizace.

A discipline devoted to architecture, mechanisms and algorithms that control the output of a specific process within the required limits. For this purpose, industrial automation tools are used.

Profil rizik **Risk profile**

Popis jakéhokoliv souboru rizik.

Description of any set of risks.

Program **Programme**

Syntaktická jednotka vyhovující pravidlům určitého programovacího jazyka; skládá se z popisů (deklarací) a příkazů nebo instrukcí nutných pro splnění určité funkce či vyřešení určité úlohy nebo problému.

Syntactic unit satisfying the rules of a certain programming language; it consists of descriptions (declarations) and commands or instructions necessary to fulfil some function or solve some task or problem.

Programovatelný logický automat (PLC) **Programmable logic controller (PLC)**

Původně malý průmyslový počítač vytvořený k provádění logických operací spouštěných na elektronických zařízeních (relé, spínače, mechanické časovače / čitače). Časem se vyvinul v řídicí jednotku schopnou řídit komplexní procesy, která se využíví ve SCADA a DCS systémech. V prostředí SCADA jsou často využívány jako výrobní zařízení, protože jsou dostupnější, univerzálnější, flexibilnější a konfigurovatelnější než speciální RTU. Někdy jsou PLC využívány namísto RTU a v tom případě se jim tak také často říká.

A small industrial computer originally designed to perform the logic functions executed by electrical hardware (relays, switches and mechanical timer/counters). They have evolved into controllers with the capability of controlling complex processes, and they are used substantially in SCADA and DCS systems. In SCADA environments, PLCs are often used as field devices because they are more economical, versatile, flexible and configurable than special-purpose RTUs. Sometimes PLCs are implemented as field devices to serve as RTUs; in this case, the PLC is often referred to as an RTU.

Prohlášení o aplikovatelnosti **Statement of applicability**

Dokumentované prohlášení popisující cíle opatření a opatření, které jsou relevantní a aplikovatelné na ISMS dané organizace. Z pohledu vyhlášky o kybernetické bezpečnosti dokumentované prohlášení obsahující přehled bezpečnostních opatření požadovaných touto vyhláškou, která (a) nebyla aplikována, včetně odůvodnění, (b) byla aplikována, včetně způsobu plnění.

Documented statement describing the objectives of measures and the measures, which are relevant and applicable for the ISMS of a given organisation. From the point of view of the Cyber Security Ordinance, a documented statement containing an overview of the security measures required by this Ordinance that (a) have not been applied, including justification, (b) have been applied, including the method of implementation.

Prohlášení o úrovni služeb **Service level declaration (SLD)**

Specifikace nabízených služeb, která se může měnit na základě individuálních dohod podle aktuálních potřeb jednotlivých uživatelů. Jedná se tedy o podrobnější SLA. Více ***SLA***.

*Specification of the offered services, which may change on the basis of individual agreements according to the actual needs of individual customers. Hence, a more detailed SLA. See **SLA**.*

Projekt ISMS **ISMS project**

Strukturované činnosti přijaté organizací k implementaci ISMS.

Structured activities undertaken by an organisation to implement an ISMS.

Prokázání totožnosti **Identity proofing / Initial entity authentication**

Forma ověření totožnosti, entity předložením průkazu totožnosti, která je podmínkou pro udělení přístupových práv.

A form of authentication based on producing an identity card that is the condition for access rights.

Prolamovač **Cracker**

Viz **Cracker**

*See **Cracker***

Prolamovač hesel **Password cracker**

Program určený ke zjištění, prolomení hesel, kódů, klíčů.

A programme designed to crack passwords, codes, keys.

Proniknutí / průnik **Penetration**

Neautorizovaný přístup k počítačovému systému, síti nebo službě.

Unauthorised access to a computer system, network or service.

Prostý text, otevřený text **Plain text, clear text**

Informace, která není šifrovaná.

Information that is not encrypted.

Protokol kostry grafu **Spanning Tree Protocol (STP)**

Protokol kostry grafu (STP) je síťový protokol, který v ethernetových místních sítích s mosty zajišťuje topologii bez smyček. Hlavní účel protokolu STP je zabránit tvorbě smyček a následného vyzařování broadcastů. Kostra grafu také dovoluje takový návrh, aby se aktivovaly náhradní (redundantní) spoje pro automatický přechod na náhradní spoje v případě přerušení aktivní cesty, bez nebezpečí smyček, nebo potřeby ruční aktivace/deaktivace těchto náhradních spojů.

The Spanning Tree Protocol (STP) is a network protocol that ensures a loop-free topology for any bridged Ethernet local area network. The basic function of STP is

to prevent bridge loops and the broadcast radiation that results from them. Spanning tree also allows a network design to include spare (redundant) links to provide automatic backup paths if an active link fails, without the danger of bridge loops, or the need for manual enabling/disabling of these backup links.

Prostředky informační války **Information warfare**

Integrované využití všech vojenských možností, které zahrnuje zajištění informační bezpečnosti, klamání, psychologické operace, elektronický boj a ničení. Podílejí se na něm všechny druhy průzkumu, komunikační a informační systémy. Cílem informační války je bránit informačnímu toku, ovlivňovat a snižovat účinnost nebo likvidovat systém velení a řízení protivníka a současně chránit vlastní systémy velení a řízení před podobnými akcemi ze strany protivníka.

Integrated use of all military capabilities including information security, deception, psychological operations, electronic warfare, and destruction. All forms of reconnaissance, communication and information systems contribute to it. The objective of information warfare is to put obstacles in the flow of information, influence and decrease efficiency or liquidate the system of command and control of the adversary, and at the same time to protect own systems of command and control from similar actions of an adversary.

Protiopatření **Countermeasure**

Činnost, zařízení, postup, technika určena k minimalizaci zranitelnosti.

Activity, equipment, procedure, technology intended to minimise vulnerability.

Protokol **Protocol**

Úmluva nebo standard, který řídí nebo umožňuje připojení, komunikaci, a datový přenos mezi počítači, obecně koncovými zařízeními. Protokoly mohou být realizovány hardwarem, softwarem, nebo kombinací obou.

Agreement or standard, which controls or enables a link, communication and data transfer among computers, in general among end devices. Protocols can be implemented by hardware, software, or a combination of both.

Protokol ARP **Address resolution protocol (ARP)**

Protokol definovaný v dokumentu RFC 826 umožňuje převod síťových adres (**IP**) na hardwarové (**MAC**) adresy. ARP neužívá autentizace, takže ho lze zneužít k útokům např. typu MITM.

*Protocol defined in the document RFC 826 enables the translation of network addresses (**IP**) to hardware (**MAC**) addresses. ARP does not use authentication. Hence it cannot be misused for attacks, e.g. of the MITM type.*

Proudová šifra **Stream Cipher**

Typ symetrické šifry kdy jsou otevřená data transformována po bitech /typicky sčítána funkcí XOR s bity generovaného hesla/. Heslo je generováno kryptografickým algoritmem v závislosti na kryptografickém klíči. Aby nebyla generována od počátku stejná posloupnost, je proces generování modifikován inicializačním vektorem. Pokud je proces generování hesla dále modifikován daty z předešlé části zašifrované zprávy je tato šifra nazývána samosynchronní. Pokud proces generování nezávisí na předešlé části zašifrované zprávy, hovoříme o synchronní proudové šifře.

Symmetric encryption system with the property that the encryption algorithm involves combining a sequence of plaintext symbols with a sequence of keystream symbols one symbol at a time, using an invertible function. Two types of stream cypher can be identified: synchronous stream cyphers and self-synchronous stream cyphers, distinguished by the method used to obtain the keystream.

Prověření **Verification**

Prokazatelné potvrzení, že stanovené požadavky byly splněny.

A demonstrable confirmation that specified requirements have been fulfilled.

Provozní dokumentace **Operational documentation**

Dokumentace informačního systému veřejné správy, která popisuje funkční a technické vlastnosti informačního systému.

Documentation of the information system of public administration describing the functional and technological features of the information system.

Provozní opatření **Operational controls**

Je to procesní akt, kterým se určitá konkrétní věc nekončí, pouze se zabezpečují některé záležitosti v zájmu jejího vyřízení. Tím se liší od rozhodnutí. Může mít formu nařízení, rozkazu či jiných normativních aktů.

It is a process act by which a certain affair does not terminate; only some issues are taken care of to expedite matters. This differentiates it from a decision. It may have the form of a directive, order or other normative acts.

Provozní prostředí **Operational environment**

Veškerý software a hardware, včetně operačního systému a hardwarové platformy, který je nezbytný k tomu, aby určitý modul pracoval bezpečně.

Set of all software and hardware including the operating system and hardware platform required for the module to operate securely.

Provozní datová sběrnice **Fieldbus**

Digitální, sériová, velkokapacitní, obousměrná datová sběrnice nebo komunikační cesta nebo spojení mezi nízkoúrovňovými průmyslovými zařízeními, jako jsou snímače, převodníky, akční členy, lokální regulátory a dokonce i zařízení pro operátorská pracoviště. Použití provozní sběrnice eliminuje potřebu kabeláže mezi řídicí jednotkou a každým zařízením. Použitý protokol umožňuje zasílat zprávy přes síť provozní sběrnice s identifikací každého jednotlivého senzoru v síti.

A digital, serial, multi-drop, a two-way data bus or communication path or link between low-level industrial field equipment such as sensors, transducers, actuators, local controllers, and even control room devices. Use of fieldbus technologies eliminates the need for point-to-point wiring between the controller and each device. A protocol is used to define messages over the fieldbus network with each message identifying a particular sensor on the network.

Provozní zařízení **Field Device**

Zařízení, které je připojené na provozní straně ICS. Jde například o RTU, PLC, akční členy, senzory, HMI a s nimi spojené komunikační sítě.

Equipment that is connected to the field side on an ICS. Types of field devices include RTUs, PLCs, actuators, sensors, HMIs, and associated communications.

Provozovatel informačního systému veřejné správy **Operator of the information system of public administration.**

Subjekt, který provádí alespoň některé informační činnosti související s informačním systémem. Provozováním informačního systému veřejné správy může správce pověřit jiné subjekty, pokud to jiný zákon nevylučuje.

Subject performing at least some of the activities related to the information system. The administrator of the information system of public administration can commission other subjects unless prohibited by law.

Proxy Server **Proxy Server**

Server, který zabezpečuje, zajišťuje, odbavuje požadavky od svých klientů jejich přeposíláním na jiné servery.

A server that services the requests of its clients by forwarding those requests to other servers.

Proxy trojan **Proxy trojan**

Maskuje ostatní počítače jako infikované počítače. Umožňuje útočníkovi zneužít napadený počítač pro přístup k dalším počítačům v síti, čímž pomáhá útočníkovi skrýt jeho skutečnou identitu.

Masks other computers as infected. Enables the attacker to abuse the infected computer for an access to other computers in the network and thus aids the attacker to hide its identity.

Prozrazení **Disclosure**

Viz **Odhalení**

*See **Disclosure***

Průběžný proces **Continuous Process**

Proces, který probíhá nepřetržitě na rozdíl od dávkového, přerušovaného nebo sekvenčního zpracování.

A process that operates on the basis of a continuous flow, as opposed to batch, intermittent, or sequenced operations.

Průkaz totožnosti **Proof of identity, Evidence of identity**

Informace o totožnosti entity vyžadované pro ověření její totožnosti. Průkaz totožnosti obsahuje informace týkající se žadatele, které jsou nezbytné pro úspěšné ověření jeho totožnosti.

Identity information for an entity required for authentication of that entity. Identity evidence includes information related to a claimant that is needed for a successful authentication.

Průmyslový počítač **Industrial computer (IPC)**

Počítač, jehož kryt i vnitřní konstrukce je provedena v průmyslové úpravě. Průmyslovou úpravou je myšlena mechanicky upravená konstrukce. Je odolný proti prachu, vodě a mechanickému poškození. Účelem je zvýšení životnosti komponentů citlivých zejména na prach, vlhkost či otřesy a jiná mechanická namáhaní. Často je součástí krytu dotykový displej.

A computer, the cover and inner construction of which are made in the industrial modification. Industrial modification means a mechanically modified structure for its resistance to dust, water, and mechanical damage. The goal is to increase the life of components that are particularly sensitive to dust, humidity or vibrations and other mechanical stress. Often, the touch screen is a part of the cover.

Průmyslový řídicí systém **Industrial Control System (ICS)**

Řídicí systém používaný v průmyslu a kritické infrastruktuře, například systém pro dispečerské řízení a sběr dat (SCADA), distribuovaný řídicí systém (DCS), programovatelný řídicí automat (PLC). ICS se skládá z kombinace řídicích komponent (např. elektrických, hydraulických, pneumatických) které společně zajišťují dosažení určitého průmyslového cíle (např. výroby, dopravy materiálu, přenosu energie).

A control system, including supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and other control system configurations such as Programmable Logic Controllers (PLC) often found in the industrial sectors and critical infrastructures. An ICS consists of combinations of control components (e.g., electrical, mechanical, hydraulic, pneumatic) that act together to achieve an industrial objective (e.g., manufacturing, transportation of matter or energy).

Průnik **Intrusion**

Nepovolený, ilegální přístup do počítačové sítě, nebo do určitého systému připojenému do sítě, tj. úmyslný či náhodný nepovolený přístup do určitého informačního systému včetně nekalé činnosti proti informačnímu systému, nebo nepovoleného využití zdrojů dostupných v rámci informačního systému.

Unauthorised, illegal access to a network or a network-connected system, i.e., deliberate or accidental unauthorised access to an information system, or unauthorised use of resources within an information system.

Průřezová kritéria **Cross-section criteria**

Soubor hledisek pro posuzování závažnosti vlivu porušení funkce prvku kritické infrastruktury s mezními hodnotami, které zahrnují rozsah ztrát na životě, dopad na zdraví osob, mimořádně vážný ekonomický dopad nebo dopad na veřejnost v důsledku rozsáhlého omezení poskytování nezbytných služeb nebo jiného závažného zásahu do každodenního života.

A set of viewpoints to assess how serious is the corruption of an element in the critical infrastructure with bounds that include the scope of life losses, impact on the health of people, extraordinary serious economic impact or impact on the public due to an extensive limitation of providing the necessary services or any other serious intervention into the daily life.

Prvek kritické infrastruktury **Element of the critical infrastructure**

Zejména stavba, zařízení, prostředek nebo veřejná infrastruktura, určené podle průřezových a odvětvových kritérií; je-li prvek kritické infrastruktury součástí evropské kritické infrastruktury, považuje se za prvek evropské kritické infrastruktury.

Building, equipment, device or public infrastructure, in particular, determined using the cross-criteria and sector criteria; if the element in the critical infrastructure is a part of the critical European infrastructure, it is considered to be an element of the critical European infrastructure.

Prvek služby **Service component**

Samostatný celek služby, který, když se spojí s dalšími celky, zajišťuje dodávku celé služby.

Independent component of a service which, when united with other components provides the whole service.

Předčasně ukončené spojení **Aborted connection**

Spojení ukončené dříve nebo jiným způsobem, než je předepsáno. Často může umožnit neoprávněným entitám neautorizovaný přístup.

Connection terminated earlier, or in another way, than prescribed. It can often provide unauthorised access to unauthorised persons.

Předmět auditu **Audit scope**

Rozsah a vymezení auditu.

Extent and boundaries of an audit.

Předmět přezkoumání **Review object**

Určitá entita, předmět, osoba, která je podrobena kontrole, přezkoumávána.

A specific centity, object, person and other, subject to review.

Předpoklad (k něčemu) **Predisposing Condition**

Určitá podmínka v rámci organizace, organizačních procesů, struktury nebo informačního systému či podnikatelského prostředí, která ovlivňuje (zvyšuje, nebo snižuje) pravděpodobnost, že jedna nebo více hrozeb, pokud se projeví, povedou k nežádoucím následkům nebo budou mít negativní dopad na procesy a majetek organiazce, jednotlivce, další organizace nebo státu.

A condition that exists within an organisation, a mission/business process, enterprise architecture, or information system including its environment of operation, which contributes to (increases or decreases) the likelihood that one or more threats, once initiated, will result in undesirable consequences or adverse impact to organisational operations and assets, individuals, other organisations, or the state.

Přechod **Transition**

Činnosti týkající se přesunutí nové nebo změněné služby do či z provozní prostředí.

Activity related to a shift of new or altered service into or out of the operational environment.

Překlad síťových adres **Network address translation (NAT)**

Mechanismus umožňující přístup více počítačů z lokální sítě do Internetu pod jedinou veřejnou IP adresou. Počítače z lokální sítě mají přiděleny tzv. privátní IP

adresy. Hraniční prvek takové lokální sítě zajišťuje překlad privátních IP adres na veřejnou. Více také **Private IP address**.

*The mechanism enabling access of several computers from a local network to the Internet under one public IP address. Computers from the local address are assigned so-called private IP addresses. The border element of such a local network provides for the translation of a private IP address to a public one. See also **Private IP address**.*

Přenos rizik **Risk transfer**

Sdílení nákladů ze ztrát s jinou stranou nebo sdílení prospěchu ze zisku vyplývajícího z rizika.

Sharing of costs with another party or sharing of benefits from profit flowing from risk.

Přesměrovávače **Re-dial, Pharming crime ware**

Programy (podmnožina Malware), jejichž úkolem je přesměrovat uživatele na určité stránky namísto těch, které původně hodlal navštívit. Na takových stránkách dochází k instalaci dalšího Crimeware (viru), nebo touto cestou dojde ke značnému zvýšení poplatku za připojení k Internetu (prostřednictvím telefonních linek se zvýšeným tarifem).

Programmes (subset of Malware) whose task is to redirect users to certain pages instead of those originally intended to be visited. On these pages there is an installation of other Crimeware (virus), or there is a substantial increase in the Internet connection fee (using telephone lines with a higher rate).

Přetečení zásobníku **Buffer Overflow**

Podmínka v rozhraní systému, která umožňuje vložit do datového zásobníku nebo úložné oblasti vice dat, než je dostupná kapacita, čímž dojde k přepsání ostatních informací. Protivníci využívají těchto podmínek k způsobení pádu systému, nebo k vložení upraveného kódu, který umožňuje získat kontrolu nad systémem.

A condition at an interface under which more input can be placed into a buffer or data holding area than the capacity allocated, overwriting other information. Adversaries exploit such conditions to crash a system or to insert a specially crafted code that allows them to gain control of the system.

Přezkoumání **Review**

Činnost prováděná k určení vhodnosti, přiměřenosti a efektivnosti předmětu přezkoumání k dosažení stanovených cílů.

Activity undertaken to determine the suitability, adequacy and efficiency of the subject matter to achieve established objectives.

Připravenost ICT na zajištění kontinuity provozu **ICT readiness for business continuity (IRBC)**

Schopnost organizace zajistit svůj provoz prostřednictvím rozpoznání narušení ICT, reakce na něj a obnovy ICT služeb.

Capability of an organisation to safeguard its business operations by detection and response to disruption and recovery of ICT services.

Přijetí rizika **Risk acceptance**

Vědomé rozhodnutí přijmout určité riziko.

Informed decision to take a particular risk.

Příklad dobré praxe, osvědčený způsob **Best practice**

Vyzkoušená metoda nebo postup, která v dané oblasti nabízí nejefektivnější řešení, které se opakovaně osvědčilo a vede k optimálním výsledkům.

Well-tested method or procedure, which in the given area offers the most effective solution, which has been repeatedly proven as right and leads towards optimum results.

Přístupové právo **Access right**

Povolení pro subjekt přistupovat ke konkrétnímu objektu pro specifický typ operace.

Permission for a subject to access a concrete object for a specific type of operation.

Přístupový bod, Bezdrátový přístupový bod **Access point / Wireless access point**

Přístroj nebo vybavení, které umožňuje bezdrátovým zařízením připojit se do metalické nebo optické sítě. Připojení využívá WLAN nebo příbuzný standard.

A device or piece of equipment that allows wireless devices to connect to a wired or optical network. The connection uses a wireless local area network (WLAN) or related standard.

Pseudonym **Pseudonym**

Alternativní název určité entity, synonyma jsou alias a vulgo (jinak zvaný). Pseudonym neumožňuje ztotožnit entitu bez použití dodatečné informace o vazbě mezi určitým pseudonym a totožností určité entity.

An alternative name of an entity, synonyms are alias and aka (also known as). Entity cannot be identified using pseudonym without additional information about connection between a pseudonym and an etity identity.

Pseudonymizace **Pseudonymisation**

Zpracování osobních údajů tak, že již nemohou být přiřazeny konkrétnímu subjektu údajů bez použití dodatečných informací, pokud jsou tyto dodatečné informace uchovávány odděleně a vztahují se na ně technická a organizační opatření, aby bylo zajištěno, že nebudou přiřazeny identifikované či identifikovatelné fyzické osobě.

The processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

Původce botnetu **Bot Herder / Bot Wrangler**

(1) Cracker, který ovládá velké množství zkompromitovaných strojů (robotů, botů, zombií).
(2) Nejvyšší počítač v hierarchii botnetu ovládající zkompromitované počítače daného botnetu.

(1) A cracker who controls a large number of compromised machines (robots, bots, zombies).
(2) The topmost computer in the botnet hierarchy controlling compromised computers of the given botnet.

Původce hrozby **Threat agent**

Původce a/nebo iniciátor úmyslných nebo náhodných hrozeb způsobených člověkem.

Originator and/or initiator of deliberate or accidental man-made threats.

Rack / Rozvaděč **Rack**

Mechanické šasi elektricky vybavené a určené k uchycení a elektrickému spojení jednotek (karet) a procesorů ICS do jednoho funkčního celku (PLC/PAC).

A mechanical chassis electrically equipped and designed to attach and electrically connect units (cards) and ICS processors into a single functional unit (PLC/PAC).

Rádiová přístupová síť **Radio access network**

Část mobilního telekomunikačního systému, která využívá technologii rádiového přístupu, jako je WCDMA nebo LTE, k zajištění přístupu zařízení koncových uživatelů k páteřní síti. Poznámka: Rádiová přístupová síť se nachází mezi koncovým uživatelským zařízením a páteřní sítí. Příkladem koncového uživatelského zařízení je mobilní telefon.

Part of a mobile telecommunication system that implements a radio access technology such as WCDMA or LTE to provide access for end-user devices to the core network. Note: The radio access network resides between the end-user device and the core network. A mobile phone is an example of an end-user device.

Rámec řízení rizik **Risk management framework**

(1) Soubor prvků poskytujících základy a organizační uspořádání pro navrhování, implementování, monitorování, přezkoumávání a neustálé zlepšování řízení rizik v celé organizaci.
(2) Řízený proces, kterým jsou do životního cyklu vývoje systémů zapojeny činnosti informační bezpečnosti a řízení rizik.

(1) Set of components providing the fundamentals and organisational arrangement for the design, implementation, monitoring, re-analysis and continuousl improvement of risk management in the whole organisation.
(2) A controlled process that integrates information security and risk management activities into the system development life cycle.

Ransomware **Ransomware**

Program, který zašifruje data a nabízí jejich rozšifrování po zaplacení výkupného (např. virus, trojský kůň).

A programme, which encrypts data and offers to decrypt them after a ransom payment (e.g., virus, Trojan horse).

Reakce na incidenty **Incident response**

Činnosti provedené s cílem zmírnit, nebo vyřešit bezpečnostní incident, včetně těch co jsou provedeny za účelem ochrany a obnovení běžných provozních podmínek informačního systému a v něm uložených informací.

Actions taken to mitigate or resolve an information security incident, including those taken to protect and restore the normal operational conditions of an information system and the information stored in it.

Redukce rizik **Risk reduction**

Činnosti ke snížení pravděpodobnosti, negativních následků nebo obou těchto parametrů spojených s rizikem.

Activity to lower the probability and lessen negative consequences, or both of these parameters linked to risk.

Redundance **Redundancy**

Obecný význam je nadbytečnost, hojnost. V **IT** se používá ve smyslu záložní. Například redundantní (záložní) zdroj napájení, redundantní (záložní) data.

*The general meaning is redundancy, abundance. In **IT** it is used in the sense of backup. For example, a redundant (backup) power supply, redundant (backup) data.*

Redundantní řidicí server **Redundant Control Server**

Záložní řídicí server, který udržuje aktuální stav určitého řídicího serveru, aby ho mohl neprodleně nahradit v případě výpadku.

A backup to the control server that maintains the current state of the control server to replace it without delay in case of outage.

Regionální Internetový Registr **Regional internet registry (RIR)**

Organizace starající se o přidělování rozsahů veřejných IP adres, autonomních systémů v její geografické působnosti. V současnosti existuje pět RIRů: RIPE NCC – Evropa a blízký východ, ARIN – USA a Kanada, APNIC – Asijsko-pacifická oblast, LACNIC – Latinská Amerika, AfriNIC – Afrika.

The organisation looking after the assignment of public IP address ranges, autonomous systems in its geographical scope. There are five RIRs at present: RIPE NCC – Europe and Near East, ARIN – USA and Canada, APNIC – Asia – Pacific Region, LACNIC – Latin America, AfriNIC – Africa.

Registr doménových jmen **Domain name registry**

Databáze všech doménových jmen, která jsou zapsána v rozšíření domény nejvyššího řádu nebo druhé nejvyšší domény.

A database of all domain names registered in a top-level domain or second-level domain extension.

Registr identit **Identity register / IMS register**

Úložiště identit pro různé entity.

Repository of identities for different entities.

Registrační autorita **Registration authority**

Entita, která je zodpovědná za poskytování ověřených uživatelských identit certifikační autoritě.

An entity responsible for providing assured user identities to the certification authority.

Regulátor tlaku **Pressure Regulator**

Zařízení, které slouží k regulaci tlaku plynu nebo kapaliny.

A device used to control the pressure of gas or liquid.

Rekonstrukce dat **Data reconstruction**

Metoda obnovy dat analyzováním původních zdrojů.

Method of data reconstruction by analysing the original sources.

Relé **Relay**

Elektromagnetické zařízení, které přerušuje elektrický obvod fyzickým pohybem vodivých kontaktů. Výsledný pohyb může být spojen s dalším mechanismem, jako je ventil nebo jistič.

An electromagnetic device that interrupts an electrical circuit by physically moving conductive contacts. The resultant motion can be coupled to another mechanism such as a valve or breaker.

Relying party **Relying party**

Server, který poskytuje přístup do zabezpečené softwarové aplikace.

A server providing access to a secure software application.

Replay, replay útok **Replay, replay attack**

Situace, kdy je zachycená kopie legitimní transakce (datová sekvence), opětovně přehrána neautorizovaným subjektem, a to zpravidla s nelegálním úmyslem (např. pro otevření vozidla s centrálním zamykáním).

Situation when a copy of a legitimate transaction (data sequence) is intercepted, repeatedly replayed by an unauthorised subject usually with illegal intent (e.g. to open a car with a central lock).

Request For Comment (RFC) **Request for comment (RFC)**

Používá se pro označení řady standardů popisujících Internetové protokoly, systémy a další věci související s fungováním internetu. Například RFC 5321 popisuje protokol **SMTP** pro výměnu a zpracování elektronické pošty.

*It is used to denote standards describing internet protocols, systems and other items related to internet operation. For example, RFC 5321 describes the **SMTP** protocol for the exchange and processing of electronic mail.*

Riziko **Risk**

(1) Nebezpečí, možnost škody, ztráty, nezdaru.
(2) Účinek nejistoty na dosažení cílů.
(3) Možnost, že určitá hrozba využije zranitelnosti aktiva nebo skupiny aktiv a způsobí organizaci škodu.

(1) Danger, the possibility of damage, loss, failure.
(2) Effect of uncertainty on objectives.
(3) Possibility that a certain threat would utilise the vulnerability of an asset or group of assets and cause damage to an organization.

Riziko bezpečnosti informací **Information security risk**

Souhrn možností, že hrozba využije zranitelnost aktiva nebo skupiny aktiv a tím způsobí organizaci škodu.

Aggregate of possibilities that a threat would utilise the vulnerabilty of an asset or group of assets and thus cause damage to an organisation.

Riziko (ochrany) soukromí **Privacy risk**

Účinek nejistoty na (ochranu) soukromí.

Effect of uncertainty on (protection of) privacy.

Role **Role**

Souhrn určených činností a potřebných autorizací pro subjekt působící v informačním systému nebo komunikačním systému.

Aggregate of specified activities and necessary authorisations for a subject operating in the information or communication system.

Rootkit **Rootkit**

Programy umožňující maskovat přítomnost zákeřného software v počítači. Dokáží tak před uživatelem skrýt vybrané běžící procesy, soubory na disku, či další systémové údaje. Existují pro Windows, LINUX i UNIX.

Programmes making it possible for insidious software to mask its presence in a computer. Thus they can hide from the user selected running processes, files on disc or other system data. They exist for Windows, LINUX and UNIX.

Rovný s rovným **Peer to peer (P2P)**

Jedná se o počítačovou síť, kde spolu přímo komunikují jednotliví klienti. Tento model se dnes využívá především u výměnných sítí. S rostoucím množstvím uživatelů totiž u tohoto modelu roste celková přenosová kapacita. Zatímco u klasického modelu klient-server je tomu přesně naopak.

This is a computer network where individual clients communicate directly. This model is primarily used in interchangeable networks. Total transmission capability grows as a rule with the growing number of users in this model. In the classic model client-server this is quite the reverse.

Rozhraní **Interface**

(1) Místo a způsob propojení systémů nebo jejich částí.
(2) Nástroje pro interakci s určitou komponentou nebo modulem.

(1) Location and mode of interconnecting systems or their parts.
(2) Means of interaction with a component or module.

Rozhraní člověk-stroj (HMI) **Human-machine interface (HMI)**

Software a hardware, který umožňuje lidským operátorům sledovat stav řízeného procesu, měnit řídicí nastavení a cíle či ručně převzít řízení v případě nouze. Umožňuje rovněž inženýrovi nebo operátorovi upravovat množinu cílových hodnot nebo řídicí algoritmy a parametry řídicí jednotky. HMI zobrazuje informace o stavu výroby, historické informace, reporty a další informace operátorům, administrátorům, manažerům, obchodním partnerům a dalším pověřeným uživatelům. Umístění, platforma či rozhraní se může být velmi různorodá – HMI může být například vyhrazená část řídícího centra, laptop připojený k WLAN nebo webový prohlížeč připojený k systému přes internet.

Software and hardware that allow human operators to monitor the state of a process under control, modify control settings to change the control objective, and manually override automatic control operations in the event of an emergency. It also allows a control engineer or operator to configure set points or control algorithms and parameters in the controller. The HMI displays process status information, historical information, reports and other information to operators, administrators, managers, business partners, and other authorised users. The location, platform, and interface may vary a great deal. For example, an HMI could be a dedicated platform in the control centre, a laptop on a WLAN or a browser on any system connected to the Internet.

Rušení **Disturbance**

Nežádoucí změna vstupní proměnné, která způsobí, že řídicí systém ovlivní hodnotu řízené proměnné nepříznivým způsobem.

An undesired change in an input variable being applied to a system that tends to adversely affect the value of a controlled variable.

Řešení incidentů **Incident handling**

Činnosti spojené s odhalováním, hlášením, hodnocením, reakcí na incidenty v oblasti bezpečnosti informací, jejich řešením a poučením se z nich.

Actions of detecting, reporting, assessing, responding to, dealing with, and learning from information security incidents.

Řetězec péče (o důkazy) **Chain of custody**

Prokazatelné držení, pohyb, manipulace a umístění materiálu (především důkazů) z jednoho časového bodu do druhého.

Demonstrable possession, movement, handling, and location of material (especially evidence) from one point in time until another.

Řetězový dopis **Chain letter**

Dopis odeslaný mnoha adresátům a obsahující informaci, kterou má každý příjemce předat mnoha dalším adresátům. Často využívá nátlaku („Pokud tento dopis do 3 dnů nepošleš 25 dalším osobám, do 10 dnů tě potká něco hrozného.“).

Letter sent out to many recipients and containing information which each recipient has to pass on to many other addressees. It is a frequently used method of pressure ("If you do not send this letter to 25 other people, something terrible happens to you in 10 days").

Řídicí algoritmus **Control Algorithm**

Matematická reprezentace určité řídicí funkce.

A mathematical representation of a control action.

Řídicí jednotka **Controller**

Zařízení nebo program, které automaticky regulují řízenou proměnou.

A device or programme that automatically regulates a controlled variable.

Řídicí jednotka s jednou smyčkou **Single Loop Controller**

Řídící jednotka, která řídí jeden vemi malý či kritický process.

A controller that controls a very small or critical process.

Řídicí jednotka stroje **Machine Controller**

Řídicí systém, který elektronicky synchronizuje pohony uvnitř strojního systému namísto spoléhání se na synchronizaci prostřednictvím mechanické vazby.

A control system that electronically synchronises drives within a machine system instead of relying on synchronisation via a mechanical linkage.

Řídící prvek **Control**

Součást ICS, která slouží ke sledování, řízení a regulaci fyzického procesu. To zahrnuje veškeré řídicí servery, řídicí jednotky, akční členy, sensory a jejich podpůrné komunikační systémy.

The part of the ICS used to perform the monitoring, control and regulation of the physical process. This includes all control servers, field devices, actuators, sensors, and their supporting communication systems.

Řídicí server **Control Server**

Řídicí zařízení, které se rovněž slouží jako server, který hostuje řídicí software komunikující s řídicími jednotkami na nižších úrovních (RTU a PLC) prostřednictvím ICS sítě ve SCADA systému, často se rovněž nazývá SCADA server, MTU, nebo dohledová řídicí jednotka.

A controller that also acts as a server that hosts the control software that communicates with lower-level control devices, such as Remote Terminal Units (RTUs) and Programmable Logic Controllers (PLCs), over an ICS network. In a SCADA system, this is often called a SCADA server, MTU, or supervisory controller.

Řídicí síť **Control Network**

Síť, která propojuje dohledovou řídicí úroveň a řídicí moduly na nižších úrovních, často propojuje zařízení, které řídí fyzické procesy, a bývá kritická z hlediska času nebo bezpečnosti provozu. Řídicí síť může být rozdělena do několika zón, nebo v jedné organizaci či v jednom provozu může být více řídicích sítí.

A network that connects the supervisory control level to lower-level control modules and typically connects equipment that controls physical processes and that is time or safety critical. The control network can be subdivided into zones, and there can be multiple separate control networks within one enterprise and site.

Řídicí smyčka **Control Loop**

Řídicí smyčka se skládá z měřících senzorů, řídicí jednotky (např. PLC), akčního prvku (např. řídicího kohoutu, jističe, spínače nebo motoru) a z výměny a zpracování proměnných. Řízené proměnné jsou ze senzorů přenášeny do řídicí jednotky. Řídicí jednotka interpretuje vstupní proměnné a na základě nastavených hodnot vytváří odpovídající výstupní proměnné, které přenáší do akčních prvků. Akční prvky způsobí změnu stavu řízeného procesu, tím dojde ke změně řízených proměnných snímaných senzory a ty jsou následně přeneseny do řídicí jednotky.

A control loop consists of sensors for measurement, controller hardware such as PLCs, actuators such as control valves, breakers, switches and motors, and the communication of variables. Controlled variables are transmitted to the controller from the sensors. The controller interprets the signals and generates corresponding manipulated variables, based on set points, which it transmits to the actuators. Process changes from disturbances result in new sensor signals, identifying the state of the process, to again be transmitted to the controller.

Řídicí středisko **Control Centre**

Určité technické zařízení, nebo skupina technických zařízení, které zajišťují měření, řízení a sledování určitého procesu.

An equipment structure or group of structures from which a process is measured, controlled, and monitored.

Řídicí systém **Control System**

Systém, v rámci nějž je záměrně použito řízení a regulace k dosažení předepsaných hodnot určité proměnné. Řídicí systémy zahrnují SCADA, DCS, PLC a další typy průmyslových měřicích a řídicích systémů.

A system in which deliberate guidance or manipulation is used to achieve a prescribed value for a variable. Control systems include SCADA, DCS, PLCs and other types of industrial measurement and control systems.

Řídicí systém výroby **Process control system**

Systém, který slouží k řízení a dozorování výroby, přenosu, ukládání a distribuce elektrické energie, plynu a tepla společně s řízením podpůrných procesů.

A system that serves to control and monitor the generation, transmission, storage and distribution of electric power, gas and heat together with the control of supporting processes.

Řízená proměnná **Controlled Variable**

Určitá proměnná, kterou se řídicí systém snaží udržet na určité nastavené hodnotě. Nastavená hodnota může být konstantní, nebo proměnná.

The variable that the control system attempts to keep at the set point value. The set point may be constant or variable.

Řízení bezpečnosti informací **Information security management (ISM)**

Řízení ochrany důvěrnosti, integrity a dostupnosti informací.

Managing the preservation of confidentiality, integrity and availability of information.

Řízení identit **Identity management (IdM)**

Procesy a zásady zapojené do správy životního cyklu a hodnoty, typu a volitelných metadat atributů v identitách známých v určité doméně. Poznámka: Obecně se správa identit týká interakcí mezi stranami, při nichž se zpracovávají informace o identitách. Procesy a postupy ve správě identit případně podporují funkce orgánu pro informace o identitách, zejména pro zpracování interakce mezi subjektem, pro který je identita spravována, a orgánem pro informace o identitách.

Processes and policies involved in managing the lifecycle and value, type and optional metadata of attributes in identities known in a particular domain. Note: In general identity management is involved in interactions between parties where identity information is processed. Processes and policies in identity management support the functions of an identity information authority where applicable, in particular to handle the interaction between an entity for which an identity is managed and the identity information authority.

Řízení incidentů bezpečnosti informací **Information security incident management**

Procesy pro detekování, hlášení, posuzování incidentů bezpečnosti informací, odezvu na incidenty, řešení incidentů a poučení se z incidentů.

Processes for detecting, reporting, assessing, responding to, dealing with and learning from security incidents.

Řízení konfigurace **Configuration Control**

Proces řízení změn hardware, firmware, software a dokumentace, který zajišťuje, že systém je chráněn před nevhodnou změnou v období před implementací, po implementaci i v jejím průběhu.

Process for controlling modifications to hardware, firmware, software, and documentation to ensure the information system is protected against improper modifications before, during, and after system implementation.

Řízení kontinuity organizace **Business continuity management (BCM)**

Holistický proces řízení, který identifikuje možné hrozby a jejich dopady na chod organizace, které by mohly způsobit, kdyby se projevily, a který poskytuje rámec pro prohlubování odolnosti organizace schopnostmi účinně reagovat a tím chránit zájmy svých klíčových zainteresovaných stran, svoji pověst, značku a svoje činnosti vytvářející hodnoty.

A holistic management process that identifies potential threats to an organisation and the impacts to business operations those threats, if realised, might cause, and which provides a framework for building organisational resilience with the capability of an effective response that safeguards the interests of its key stakeholders, reputation, brand and value-creating activities.

Řízení přístupu **Access control**

Prostředky zajišťující, aby přístup k aktivům byl autorizován a omezen na základě požadavků organizace a bezpečnostních požadavků.

Means to ensure that access to assets is authorised and restricted based on business and security requirements.

Řízení přístupu dle rolí **Role-based access control (RBAC)**

Řízení přístupu na základě přístupových oprávnění k objektům, které jsou přiřazeny jako atribut určitým rolím.

Access control based on access permissions to objects, which are assigned as attributes to specific roles.

Řízení rizik **Risk management**

Koordinované činnosti pro vedení a řízení organizace s ohledem na rizika.

Coordinated activities to direct and control an organisation with regard to risks.

Řízení služeb **Service management**

Množina schopností a procesů pro vedení a řízení činností a zdrojů poskytovatele služeb pro návrh, přechod, dodávku a zlepšování služeb, aby byly naplněny požadavky služeb.

Set of capabilities and processes to manage and control the activities and sources of the service provider for the design, handover, delivery and improvement of services so that the requirements placed on them be met.

Řízení zranitelností **Vulnerability management**

Cyklická praxe pro identifikaci, třídění, opakované zprostředkování a zmírňování zranitelností. Obecně se tato praxe vztahuje na zranitelnosti programového vybavení v počítačových systémech, může však být často rozšířena na organizační chování a strategické rozhodovací procesy.

The cyclical practice of identifying, classifying, remediating, and mitigating vulnerabilities. This practice generally refers to software vulnerabilities in computing systems; however, it can also extend to organisational behaviour and strategic decision-making processes.

Sandbox **Sandbox**

Bezpečnostní mechanismus sloužící k oddělení běžících procesů od samotného operačního systému. Používá se například při testování podezřelého softwaru.

Security mechanism serving to separate running processes from the operating system proper. It is used, for example, for testing suspicious software.

SCADA **SCADA**

(1) Dispečerské řízení a sběr dat
(2) Kybernetická bezpečnost průmyslových řídicích systémů

(1) Supervisory control and data acquisition
(2) Cyber security of the industrial controlling systems.

SCADA server / Master terminal unit **SCADA server / Master Terminal Unit (MTU)**

Zařízení (master), které řídí RTU a PLC zařízení umístěné ve výrobě (slave).

A device (master) that controls RTU and PLC placed in production (slave).

Sdílené tajemství **Shared secret**

Tajemství, které se využívá v rámci ověření totožnosti určité entity a je známé pouze dané entitě a tomu, kdo ověřuje její identitu.

Secret used in authentication of an entity that is known only to the entity and the verifier.

Sdílení **Sharing**

Možnost společně a současně se dělit o jeden nebo více zdrojů informací, paměti nebo zařízení.

Possibility to have a portion at the same time of one or more information sources, memory or devices.

Secure shell **Secure shell (SSH)**

Protokol, který poskytuje bezpečný vzdálený login při použití nezabezpečené sítě.

A protocol that provides secure remote login utilising an insecure network.

Secure socket layer **Secure socket layer (SSL)**

Protokol, respektive vrstva vložená mezi vrstvu transportní (např. **TCP/IP**) a aplikační (např. **HTTP**), která poskytuje zabezpečení komunikace šifrováním a autentizaci komunikujících stran.

*Protocol or a layer inserted between the transport layer (e.g. **TCP/IP**) and the application layer (e.g. **HTTP**) which enables communication security by encryption and authentification of the communicating parties.*

Security software disabler **Security software disabler**

Zablokuje software pro zabezpečení **PC** (**Firewall**, **Antivir**).

*It blocks software to secure the **PC** (**Firewall**, **Antivirus**).*

Senzor **Sensor**

Zařízení, které měří nebo snímá určitou fyzikální vlastnost nebo veličinu a převádí ji na elektrický nebo optický signál, který může být dále vyhodnocen určitým pozorovatelem nebo zařízením.

A device that measures or reads some specific physical property or value and converts it into an electrical or optical signal, which can be evaluated by an observer or instrument.

Senzor vzdálenosti **Proximity Sensor**

Bezkontaktní čidlo se schopností detekovat určitý předmět v zadané vzdálenosti.

A non-contact sensor with the ability to detect an item within a specified range.

Server **Server**

Počítačový systém nebo program, který poskytuje služby ostatním počítačům nebo programům.

Computer system or programme that provides services to other computers or programmes.

Serverová farma **Server cluster**

Skupina síťových serverů, které jsou používány k zefektivnění vnitřních procesů tím, že distribuují zátěž mezi jednotlivé zapojené složky, aby urychlily výpočetní procesy využitím síly více serverů. Když jeden server ve farmě selže, jiný může jeho služby nahradit.

Group of network servers used to increase the efficiency of internal processes by distributing load among individual linked components to speed up computing processes by using the power of more servers. When one server in the farm fails, another one can replace it.

Service set identifier **Service set identifier (SSID)**

Jedinečný identifikátor (název) každé bezdrátové (**WiFi**) počítačové sítě.

*Unique identifier (name) of every wireless (**WiFi**) computer network.*

Servo ventil **Servo Valve**

Poháněný ventil, jehož pozice je řízena akčním členem.

An actuated valve whose position is controlled by an actuator.

Sexting **Sexting**

Elektronické rozesílání textových zpráv, fotografií či videí se sexuálním obsahem. Tyto materiály často vznikají v rámci partnerských vztahů. Takovéto materiály však mohou představovat riziko, že jeden partner z nejrůznějších pohnutek zveřejní fotografie či videa svého partnera.

Electronic distribution of text messages, photographies or videos with sexual content. These materials often originate in partner relations. Such materials, however, may represent a risk that one partner, out of various motives, would publish photographies or videos of the other partner.

Seznam pro řízení přístupu **Access control list (ACL)**

Seznam oprávnění připojený k nějakému objektu (např. diskovému souboru); určuje, kdo nebo co má povolení přistupovat k objektu a jaké operace s ním může provádět. U bezpečnostního modelu používajícího ACL systém před provedením každé operace prohledá ACL a nalezne v něm odpovídající záznam, podle kterého se rozhodne, zda operace smí být provedena.

List of permissions to grant access to an object (e.g. a disc file); it determines, who or what has the right to access the object and which operations it can do with it. In the security model using the ACL system, it searches ACL before performing any operation and looks up the corresponding record and by it makes a decision if the operation may be executed.

Shareware **Shareware**

Volně distribuovaný software, který je chráněn autorskými právy. V případě že se uživatel rozhodne tento software využívat déle, než autor umožňuje, je uživatel povinen splnit podmínky pro používání. Může jít například o zaplacení určité finanční částky, registrace uživatele, atd.

Freely distributed software protected by copyright. In case the user decides to use this software longer than the author permits, the user is obliged to satisfy conditions for use. These can be, for example, payment of a certain financial amount, user registration, etc.

Shoda **Conformity**

Splnění požadavku.

Fulfilment of a requirement.

Schopnost reagovat na počítačové hrozby (CIRC) **Computer incident response capability (CIRC)**

Schopnost v oblasti kybernetické obrany, která umožňuje rychle a efektivně reagovat na rizika a zranitelnosti v systémech, poskytuje metodiku pro oznamování a zvládání incidentů, zajišťuje podporu a pomoc provozním a bezpečnostním správcům systémů. Je součástí havarijního (krizového) plánování obnovy systémů.

A cyber defence capability, which ensures fast and effective reaction to risks and vulnerabilities in systems; provides methodology for reporting and managing

incidents; provides support and help to the operational and security managements of systems. It is part of the emergency (crisis) planning for system recovery.

Signatura viru **Virus signature**

Viz **Charakteristika viru**

*See **Virus signature***

Simple mail transfer protocol **Simple mail transfer protocol (SMTP)**

Internetový protokol určený pro přenos zpráv elektronické pošty. Popisuje komunikaci mezi poštovními servery.

Internet protocol for the transmission of messages of electronic mail. It describes communication among mail servers.

Simple Network Management Protocol **Simple Network Management Protocol (SNMP)**

Základní TCP/IP protokol pro správu sítě. Administrátoři sítě používají SNMP ke sledování a popisu dostupnosti, výkonu a miry chybovosti sítě.

The basic TCP/IP protocol for network management. Network administrators use SNMP to monitor and map network availability, performance, and error rates.

Simulace **Simulation**

Použití systému zpracování dat k vyjádření vybraných vlastností chování fyzického nebo abstraktního systému.

Use of a data processing system to extract selected properties in the behaviour of a physical or abstract system.

Síť **Network**

Množina počítačových terminálů (pracovních stanic) a serverů, které jsou vzájemně propojeny, aby si navzájem vyměňovaly data a mohly spolu komunikovat.

Set of computer terminals (workstations) and servers which are mutually interconnected in order to exchange data and communicate.

Síť botů **Botnet**

Viz **Botnet**

*See **Botnet***

Síť elektronických komunikací **Network of electronic communications**

Přenosové systémy, popřípadě spojovací nebo směrovací zařízení a jiné prostředky, včetně prvků sítě, které nejsou aktivní, které umožňují přenos signálů po vedení, rádiovými, optickými nebo jinými elektromagnetickými prostředky, včetně družicových sítí, pevných sítí s komutací okruhů nebo paketů a mobilních zemských sítí, sítí pro rozvod elektrické energie v rozsahu, v jakém jsou používány pro přenos signálů, sítí pro rozhlasové a televizní vysílání a sítí kabelové televize, bez ohledu na druh přenášené informace.

Transmission systems, or as the case may be, communication and routing equipment and other devices, including elements of the network which are not active, which make for the transmission of signals over wire lines, by radio, optical or other electromagnetic devices, including satellite networks, fixed lines with commuted circuits or packets, and mobile ground networks, networks for the distribution of electrical energy in the extent to transmit signals, networks for radio and television broadcast and networks for cable television, regardless of the type of transmitted information.

Síť uložiště **Storage Area Network (SAN)**

Síť, jejímž hlavním účelem je přenos dat mezi počítačovými systémy a úložišti a mezi úložišti navzájem. Poznámka: Síť SAN se skládá z komunikační infrastruktury, která zajišťuje fyzická připojení, a z vrstvy správy, která organizuje připojení, úložiště a počítačové systémy tak, aby byl přenos dat bezpečný a spolehlivý.

Network whose primary purpose is the transfer of data between computer systems and storage devices and among storage devices. Note: A SAN consists of a communication infrastructure, which provides physical connections, and a management layer, which organizes the connections, storage devices, and computer systems so that data transfer is secure and robust.

Síťová karta **Network Interface Card (NIC)**

Deska nebo karta plošných spojů, která je nainstalována v počítači, aby mohl být připojen k počátačové síti.

A circuit board or card that is installed in a computer so that it can be connected to a network.

Síťový analyzátor **Network sniffer**

Zařízení nebo software, které slouží k získávání informací přenášených po síti.

Device or software used to capture information flowing in networks.

Skartovat **Shred**

Zničit médium rozřezáním nebo rozbitím na malé části.

Destroy the medium by cutting or breaking it into small pieces.

Skenování portů **Port Scanning**

Využití programu pro vzdálené zjištění, které porty v určitém systému jsou otevřené (např. zda systém povolí připojení na tomto portu.)

Using a programme to remotely determine which ports on a system are open (e.g., whether the system allows connections through these ports).

Skript **Script**

Soubor instrukcí zapsaný v některém formálním jazyce, kterým je řízena činnost zařízení, programu či systému.

Set of instructions written in some formal language, which control the workings of devices, programme or system.

Skrytý kanál **Covert Channel**

Přenosový kanál, který může být použít pro přenos dat způsobem, který narušuje bezpečnostní politiku.

A transmission channel that could be used for data transfer in a way impairing security policy.

Skupina pro reakci na kybernetické bezpečnostní incidenty **Computer security incident response team (CSIRT)**

Bezpečnostní tým, jehož úkolem je pomáhat s řešením incidentů v oblasti kybernetické bezpečnosti. CSIRT poskytuje svým klientům potřebné služby při

řešení bezpečnostních incidentů a pomáhá jim při obnově systému po narušení. Aby snížily rizika incidentů a minimalizovaly jejich počet, pracoviště CSIRT poskytují svým klientům také preventivní a vzdělávací služby. Pro své klienty poskytují informace o odhalených slabinách používaných hardwarových a softwarových prostředků a o možných útocích, které těchto slabin využívají, aby klienti mohli dostatečně rychle ošetřit odhalené slabiny.

A team of experts to support the handling of cyber security incidents. CSIRT provides its clients with the necessary services for solutions to incidents and helps them in recovering the system after a disruption. To minimise incident risks and minimise their number, CSIRT offices also provide preventive and educational services. For clients, they provide information on detected weaknesses of used hardware and software instruments and about possible attacks, which make use of these weaknesses so that the clients may quickly address these weaknesses

Skupina pro reakci na kybernetické hrozby **Computer emergency response team (CERT)**

CERT je jiný užívaný název pro **CSIRT**, na rozdíl od označení **CSIRT** je CERT registrovaná ochranná známka. Více **CSIRT**.

*CERT is another name for **CSIRT**; unlike **CSIRT**, CERT is a registered trademark. See **CSIRT**.*

Slepé testování **Black box testing**

Zkoumání určitého procesu vkládáním vstupů a porovnáváním získaných výsledků s předpokládanými výstupy, které zohledňují požadavky procesu.

Examining a process using known inputs and comparing the results against predicted outputs, which reflect the requirements for the process.

Slovníkový útok **Dictionary attack**

Útok na systém, v rámci kterého jsou využívány seznamy často používaných hesel. Jedná se o poměrně rychlou metodu, úspěch záleží na velikosti slovníku a na tom, zda oběť používá heslo, které lze pomocí slovníku odhadnout.

Attack on a system that employs a search of a given list of passwords. This is a relatively fast method, depending on the size of the dictionary and whether the victim uses a password that may be detected using the dictionary.

Služba **Service**

(1) Činnost informačního systému uspokojující dané požadavky oprávněného subjektu spojená s funkcí informačního systému.
(2) Způsob jak dodat uživatelům určitou hodnotu plynoucí z využití specifických fyzickýh nebo logických zdrojů bez nutnosti dané zdroje vlastnit a nést s tím spojená rizik.

(1) Activity of the information system meeting the given requirements of an authorised subject related to the function of the operating system.
(2) Means of delivering value to users by facilitating results users want to achieve without the ownership of specific physical or logical resources and the risks related to ownership.

Služba časového razítka **Time-stamping service**

Služba poskytující důkaz, že datová položka existovala před určitým časovým okamžikem.

Service providing evidence that a data item existed before a certain point in time.

Služba elektronických komunikací **Electronic communication service**

Služba obvykle poskytovaná za úplatu, která spočívá zcela nebo převážně v přenosu signálů po sítích elektronických komunikací, včetně telekomunikačních služeb a přenosových služeb v sítích používaných pro rozhlasové a televizní vysílání a v sítích kabelové televize, s výjimkou služeb, které nabízejí obsah prostřednictvím sítí a služeb elektronických komunikací nebo vykonávají redakční dohled nad obsahem přenášeným sítěmi a poskytovaným službami elektronických komunikací; nezahrnuje služby informační společnosti, které nespočívají zcela nebo převážně v přenosu signálů po sítích elektronických komunikací.

Service usually provided for a fee, which consists wholly or predominantly of signal transmission over electronic communication networks, including telecommunication services and transmission services in networks used for radio and television broadcast and networks for cable television, excluding services which provide content using the networks and services of electronic communications or have editing supervision of the content transmitted over the networks and provided services of electronic communications; it does not include services of the information society which do not rest wholly or predominantly on the transmission of signals over networks of electronic communications.

Služba informační společnosti **Information society service**

Každá služba poskytovaná zpravidla za úplatu, na dálku, elektronicky a na individuální žádost příjemce služeb. Pro účely této definice se rozumí:
(1) „službou poskytovanou na dálku“ služba poskytovaná bez současné přítomnosti stran,
(2)„službou poskytovanou elektronicky“ služba odeslaná z výchozího místa a přijatá v místě jejího určení prostřednictvím elektronického zařízení pro zpracování (včetně digitální komprese) a uchovávání dat a jako celek odeslaná, přenesená nebo přijatá drátově, rádiově, opticky nebo jinými elektromagnetickými prostředky,
(3) „službou poskytovanou na individuální žádost příjemce služeb“ služba poskytovaná přenosem dat na individuální žádost.

Any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services. For this definition:
(1) 'at a distance' means that the service is provided without the parties being simultaneously present;
(2) 'by electronic means' means that the service is sent initially and received at its destination using electronic equipment for the processing (including digital compression) and storage of data, and entirely transmitted, conveyed and received by wire, by radio, by optical means or by other electromagnetic means;
(3) 'at the individual request of a recipient of services' means that the service is provided through the transmission of data on individual request.

Směrovač, router **Router**

Síťové zařízení, které se využívá k navázání a řízení komunikace mezi různými sítěmi výběrem cest či tras na základě využití směrovacích protokolů a algoritmů. Směrovač se obvykle využívá k připojení sítě LAN k síti WAN, či k připojení MTU a RTU ke vzdálenému síťovému médiu v rámci SCADA komunikace.

A network device that is used to establish and control the communication between different networks by selecting paths or routes based upon routing protocols and algorithms. Common uses for routers include connecting a LAN to a WAN and connecting MTUs and RTUs to a long-distance network medium for SCADA communication.

Směrnice **Guideline**

(Závazné) doporučení toho, co se očekává, že má být provedeno, aby byl dosažen určitý cíl.

A (binding) recommendation of what is expected to be done in order to achieve a certain target.

Smlouva o úrovni služeb **Service level agreement (SLA)**

Smlouva mezi poskytovatelem a příjemcem služby, která definuje parametry technické podpory a parametry poskytované služby včetně způsobu jejich měření a následků, které vyplývají z jejich nedodržení poskytovatelem služby.

A contract between the service provider and the service recipient that defines the parameters of technical support and the parameters of the service provided, including how they are measured and the consequences that result from the service provider's failure to comply with them.

Sniffer **Sniffer**

Program umožňující odposlouchávání všech protokolů, které počítač přijímá / odesílá (používá se např. pro odposlouchávání přístupových jmen a hesel, čísel kreditních karet).

Programme for the eavesdropping of all the protocols which a computer receives/sends (it is used, for example, for eavesdropping of access names or passwords, numbers of credit cards).

Sociální inženýrství **Social engineering**

Účelová manipulace lidí s cílem přimět je k provedení určité akce nebo k vyzrazení důvěrné informace.

Act of purposeful manipulation of people into performing particular actions or divulging confidential information.

Sociální síť **Social network**

Propojená skupina lidí, kteří se navzájem ovlivňují. Tvoří se na základě zájmů, rodinných vazeb nebo z jiných důvodů. Tento pojem se dnes také často používá ve spojení s internetem a nástupem webů, které se na vytváření sociálních sítí přímo zaměřují (Facebook, Lidé.cz apod.), sociální sítě se mohou vytvářet také v zájmových komunitách kolem určitých webů, například na jejich fórech.

An interconnected group of people who interact. It is formed by interests, family ties or other reasons. This idea is at present often used in connection with internet and the onset of webs which are directly targeted at social networks (Facebook, Lidé.cz etc.), social networks can also form in interest communities around certain web sites, for example at their forums.

Software (programové vybavení) **Software**

Sada programů používaných v počítači, které vykonávají zpracování dat, či konkrétních úloh. Software lze dále rozdělit na: a) systémový software – vstupně/výstupní systémy, operační systémy nebo grafické operační systémy; b) aplikační software – aplikace, jednoduché utility nebo komplexní programové systémy; c) firmware – ovládací program hardwaru.

Set of programmes used in a computer which execute data processing or a concrete task. The software can be further subdivided into a) system software – input/output devices, operating systems or graphics operation systems; b) application software – applications, simple utilities or complex programming systems; c) firmware – hardware control programme.

Software jako služba **Software as a Service (SaaS)**

Možnost daná uživateli pro použití aplikací poskytovatele, které se provozují na cloudové infrastruktuře. Aplikace jsou přístupné z různých klientských zařízení buďto přes rozhraní tenký klient, jako je web prohlížeč (například email na webu), nebo přes programové rozhraní. Uživatel neřídí ani neovládá základní cloudovou infrastrukturu jako síť, servery, operační systémy, paměťová media, nebo dokonce jednotlivé možnosti aplikací, s možnou výjimkou omezeného nastavení konfigurace aplikací.

The capability provided to the consumer to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g. web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

Software veřejné domény **Public domain software**

Software, který je umístěn do veřejné domény, jinými slovy neexistuje vůbec žádné vlastnictví, jako například autorské právo, obchodní značka či patent.

Software that has been placed in the public domain, in other words there is absolutely no ownership such as copyright, trademark, or patent.

Softwarové pirátství **Software piracy**

Neautorizované používání, kopírování nebo distribuce programového vybavení.

Unauthorised use, copying or distribution or software.

Soubor **File**

Obecná pojmenovaná množina dat. Může se jednat o dokument, multimediální data, databázi či prakticky jakýkoli jiný obsah, který je pro uživatele nebo software užitečné mít permanentně přístupný pod konkrétním jménem.

General named set of data. It can be a document, multimedia data, database or practically any other content, which the user or software may find useful to have permanently available under a concrete name.

Soubor logů **Log file**

Soubor obsahující informace o aktivitách subjektů v systému, přístup k tomuto souboru je řízen.

File containing information on the activities of subjects in the system, access to this file is controlled.

Souborový systém **File system**

Způsob organizace a uložení dat ve formě souborů tak, aby k nim bylo možné snadno přistupovat. Souborové systémy jsou uloženy na vhodném typu elektronické paměti, která může být umístěna přímo v počítači (pevný disk) nebo může být zpřístupněna pomocí počítačové sítě.

Method of organisation and storage of data in the form of files so that access to them would be easy. File systems are stored on a suitable type of electronic memory, which can be located directly in the computer (hard disc) or can be made accessible using a computer network.

Souhlas subjektu údajů **Consent of the data subject**

Svobodný, konkrétní, informovaný a jednoznačný projev vůle, kterým subjekt údajů dává prohlášením či jiným zjevným potvrzením své svolení ke zpracování svých osobních údajů.

Any freely given, specific, informed and unambiguous indication of the data subject's will by which they, by a statement or by a clear affirmative action, signify agreement to the processing of their data.

Soukromí **Privacy**

Soukromí je schopnost nebo právo jednotlivce nebo skupiny zadržovat informace o sobě. Soukromí je rovněž hmotný nebo myšlenkový prostor subjektu.

Privacy is the capability or right of an individual or group to retain information about themselves. Privacy is also the material or mental space of the subject.

Soukromý klíč **Private key**

Klíč v asymetrické kryptografii, který náleží určité entitě a měl by být znám pouze této entitě. Soukromý klíč tvoří pár s veřejným klíčem.

A key in asymmetric cryptography, which belongs to a specific entity and should be known only to this entity. It is paired with a public key.

Spalování **Incinerate**

Zničení médií úplným spálením na popel.

Destruct by burning media completely to ashes.

Spear phishing (rybaření oštěpem) **Spear phishing**

Sofistikovanější útok typu **Phishing**, který využívá předem získané informace o oběti. Díky většímu zacílení na konkrétní uživatele dosahuje tato metoda většího účinku než běžný útok typu **Phishing**. Více **Phishing**.

*More sophisticated attack than **Phishing,** which uses prior obtained information about the victim. Thanks to a more focused targeting on a concrete user this method attains higher effect than a standard attack of the **Phishing** type. See **Phishing**.*

Spojování / Fúze **Linkage / Fusion**

Účelná kombinace dat nebo informací z jednoho systému zpracování dat s daty nebo informacemi z jiného systému tak, aby bylo možné odvolat chráněnou informaci.

Useful combination of data or information from one data processing system, with data or information from another system, so as to declassify protected information.

Společná kriteria **Common Criteria**

Společná kriteria pro vyhodnocení bezpečnosti informačních technologií (ve zkratce z anglického jen Společná kriteria, Common Criteria nebo CC) je mezinárodní norma (ISO/IEC 15408) pro certifikaci počítačové bezpečnosti. V současné době jde o verzi 3.1 revizi 4. Společná kriteria tvoří rámec, v němž mohou uživatelé výpočetních systémů specifikovat své požadavky na funkčnost a spolehlivost zabezpečení (Security Functional Requirements, SFR, požadavky na

funkčnost zabezpečení, a Security Assurance Requirements, SAR, požadavky na spolehlivost), pomocí profilů ochrany (Protection Profile, PP). Uživatelé mohou pak aplikovat a činit si nároky na bezpečnostní atributy svých výrobků, a testovací laboratoře mohou vyhodnotit, zda daný výrobek opravdu splňuje tyto požadavky. Jinými slovy, Společná kriteria poskytují záruky, že procesy specifikace, implementace a vyhodnocení prvku počítačové bezpečnosti bylo provedeno standardním rigorozním a opakovatelným postupem na úrovni odpovídající cílovému prostředí použití.

The Common Criteria for Information Technology Security Evaluation (abbreviated as Common Criteria or CC) is an international standard (ISO/IEC 15408) for computer security certification. It is currently in version 3.1 revision 4. Common Criteria is a framework in which computer system users can specify their security functional and assurance requirements (SFRs and SARs respectively) through the use of Protection Profiles (PPs), vendors can then implement and/or make claims about the security attributes of their products, and testing laboratories can evaluate the products to determine if they actually meet the claims. In other words, Common Criteria assures that the process of specification, implementation and evaluation of a computer security product has been conducted in a rigorous and standard and repeatable manner at a level that is commensurate with the target environment for use.

Spolehlivost **Reliability**

Vlastnost systému a jeho částí plnit své poslání přesně a bez výpadku nebo významného snížení kvality či rozsahu.

Property of a system and its parts to perform its mission accurately and without failure or significant degradation.

Správa bezpečnosti informací **Governance of information security**

Systém, který řídí a kontroluje činnosti týkající se bezpečnosti informací organizace.

The system by which an organisation's information security activities are directed and controlled.

Správa klíčů **Key management**

Evidování, vytváření, registrování, certifikování, distribuování, zavádění, ukládání, rušení registrace, archivování, odvolávání, odvozování a ničení klíčů v souladu s určitou bezpečnostní politikou.

Administration, generation, registration, certification, distribution, installation, storage, deregistration, archiving, revocation, derivation and destruction of keys in accordance with a security policy.

Správa sítě **Network management**

Proces plánování, návrhu, implementace, provozu, sledování a údržby sítě.

Process of planning, designing, implementing, operating, monitoring and maintaining a network.

Správce aktiva (provozovatel informačního sytému) **Assets Manager (information system operator)**

Jedinec (entita), který zabezpečuje zpracování informací nebo poskytování služeb a vystupuje vůči ostatním fyzickým a právnickým osobám v informačním systému jako nositel práv a povinností spojených s provozováním systému.

Individual (entity) who enables information processing or service providing and acts towards other natural and legal persons in the information system as the bearer of rights and obligations connected to operating the system.

Správce informačního systému veřejné správy **Operator of the information system of public administration.**

Subjekt, který podle zákona určuje účel a prostředky zpracování informací a za informační systém odpovídá.

Subject who by law determines the objective and means for information processing and is responsible for the information system.

Správce kryptografie **Crypto officer**

Role zastávaná osobou, případně procesem zastupujícím určitou osobu, která přistupuje ke kryptografickému prostředku za účelem provádění kryptografických inicializačních, či řídicích funkcí daného kryptografického prostředku.

Role taken by an individual or a process (i.e. subject) acting on behalf of an individual that accesses a cryptographic module in order to perform cryptographic initialisation or management functions of a cryptographic module.

Správce osobních údajů **Controller (of personal data)**

Fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který sám nebo společně s jinými určuje účely a prostředky zpracování osobních údajů; jsou-li účely a prostředky tohoto zpracování určeny právem Unie či členského státu, může toto právo určit dotčeného správce nebo zvláštní kritéria pro jeho určení.

A natural or legal person, public authority, agency or another body, which alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

Správce osobně identifikovantelných informací (údajů) PII **Controller of personally identifiable information (data) PII**

Fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který sám nebo společně s jinými určuje účely a prostředky zpracování osobních údajů; jsou-li účely a prostředky tohoto zpracování určeny právem Unie či členského státu, může toto právo určit dotčeného správce nebo zvláštní kritéria pro jeho určení.

A natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

Správce systému **System administrator**

Osoba zodpovědná za řízení a údržbu počítačového systému.

Person responsible for the management and maintenance of a computer system.

Správce zabezpečení účtů **Security account manager**

Správce zabezpečení účtů v operačním systému Windows, např. databáze, ve které se uchovávají hesla uživatelů (hesla v operačním systému Windows NT se nacházejí např. v adresáři c:\winnt\repair a c:\winnt\config).

Administrator for securing the accounts in the Windows operating system, e.g. a database, where user passwords are kept (passwords in Windows NT operating system may be kept, for example, in the directory c:\\winnt\repair and c:\\winnt\config).

Spyware **Spyware**

Program skrytě monitorující chování oprávněného uživatele počítače nebo systému. Svá zjištění tyto programy průběžně (např. při každém spuštění) zasílají subjektu, který program vytvořil, respektive distribuoval. Takové programy jsou často na cílový počítač nainstalovány spolu s jiným programem (utilita, počítačová hra), s jehož funkcí však nesouvisí.

The programme, which secretly monitors the behaviour of an authorised computer or system user. The findings are sent by these programmes continuously (e.g. at every startup) to the subject which created the programme or distributed it. Such programmes are frequently installed on the target computer together with another programme (utility, computer game). However, they bear no relation to it.

SQL **Structured query language (SQL)**

Standardizovaný dotazovací jazyk používaný pro práci s daty v relačních databázích.

Standard query language used to work with data in relational databases.

SQL injection **SQL injection**

Injekční technika, která zneužívá bezpečnostní chyby vyskytující se v databázové vrstvě aplikace. Tato chyba zabezpečení se projevuje infiltrací neoprávněných znaků do SQL příkazu oprávněného uživatele nebo převzetím uživatelova přístupu k vykonání SQL příkazu.

Injection technique, which abuses security errors occurring in the database layer of an application. This security error manifests itself by infiltrating unauthorised characters into an SQL command of an authorised user, or by taking over user access, to execute the SQL command.

Stanovení kontextu **Establishing the context**

Vymezení vnějších a vnitřních parametrů, které mají být zohledněny při managementu rizik a nastavení rozsahu platnosti a kritérií rizik pro politiku managementu rizik.

Establishing the limits of external and internal parameters to be taken into account during risk management and setting of the risk validity ranges and risk criteria for the risk management policy.

Statistické řízení procesů **Statistical Process Control (SPC)**

Řízení kvality produktu nebo procesu s pomocí statistických technik.

The use of statistical techniques to control the quality of a product or process.

Stav kybernetického nebezpečí **State of cyber danger**

Stavem kybernetického nebezpečí se rozumí stav, ve kterém je ve velkém rozsahu ohrožena bezpečnost informací v informačních systémech nebo bezpečnost služeb nebo sítí elektronických komunikací.

Under cyber danger, we understand such a state when there is a large measure of danger to information security in information systems or security of services or electronic communications.

Strana zúčastněná na (ochraně) soukromí **Privacy (protection) stakeholder**

Fyzická nebo právnická osoba, veřejná autorita, vládní organizace nebo jakýkoli jiný orgán, který může ovlivnit, být ovlivněn nebo být vnímán jako ovlivněný rozhodnutím nebo činností vztahující se ke zpracování osobně identifikovatelných informací (PII).

A natural or legal person, public authority, agency or any other body that can affect, be affected by or perceive themselves to be affected by a decision or activity related to personally identifiable information (PII) processing.

Strategie bezpečnosti informací společnosti **Corporate information security policy**

Dokument, který popisuje pokyny vedení a podporu bezpečnosti informací v souladu s obchodními požadavky a příslušnými zákony a předpisy.

Document that describes management direction and support for information security in accordance with business requirements and relevant laws and regulations.

Structure text (strukturovaný text) **Structure text**

Programovací jazyk z rodiny IEC 61113-3 pro PLC. Je nejvíce podobný klasickým programovacím jazykům. Jedná se o klasickou reprezentaci syntaktický poskládaných příkazů.

IEC 61113-3 PLC programming language. It is most similar to traditional programming languages. This is a classical representation of syntactic composite commands.

Středisko distribuce klíčů **Key distribution centre (KDC)**

Entita pověřená generováním nebo získáváním a distribuováním klíčů dalším entitám.

An entity entrusted to generate or acquire and distribute keys to other entities.

Středisko generování klíčů **Key Generation Center (KGC)**

Organizační jednotka, která zabezpečuje generování kryptografických klíčů a jejich plnění do nosičů pro nezávislou distribuci do kryptografických prostředků.

Organisation body that enables the generation of cryptographic keys and their loading into tokens for an independent distribution into cryptographic devices.

Středisko správy klíčů **Security Management Centre (SMC)**

Organizační jednotka, která zabezpečuje správu kryptografických klíčů a konfiguraci kryptografických prostředků v síti. Středisko generuje kryptografické klíče pro kryptografické prostředky v síti, zabezpečuje jejich elektronickou distribuci a realizuje politiku komunikace kryptografických prostředků v síti.

Organisation body that ensures the management of cryptographic keys and the configuration of cryptographic devices in a network. The centre generates cryptographic keys for the cryptographic devices in a network, provides for their electronic distribution and implements strategy for communication of cryptographic devices in the network.

Střední doba mezi poruchami **Mean Time Between Failures**

Předpokládaná doba mezi dvěma po sobě jdoucími poruchami určitého systému nebo jeho části.

Expected time between consecutive failures in a system or its component.

Střední doba opravy **Mean Time To Repair**

Očekávaná nebo vypozorovaná doba, za kterou jsou rozbitý systém nebo jeho komponenta znovu uvedeny do provozu.

Expected or observed duration to return a malfunctioning system or component to normal operations.

Stuxnet **Stuxnet**

Počítačový červ, který je vytvořen, aby útočil na průmyslové řidicí systémy typu **SCADA**, jenž je využíván k řízení velkých průmyslových podniků, například továren, elektráren, produktovodů a dokonce armádních zařízení.

Computer worm created to attack industrial control systems of the SCADA type used to control large industrial enterprises, for example, factories, power generating plants, product lines and even military objects.

Subjekt **Subject**

V počítačové bezpečnosti aktivní entita, která může přistupovat k objektům.

In computer security, an active entity which can access objects.

Subjekt kritické infrastruktury **Subject of critical infrastructure**

Provozovatel prvku kritické infrastruktury; jde-li o provozovatele prvku evropské kritické infrastruktury, považuje se tento za subjekt evropské kritické infrastruktury.

The operator of an element of critical infrastructure; if it is an operator of an element of the European critical infrastructure, the operator is considered to be a subject of the European critical infrastructure.

Subjekt osobně identifikovantelných informací (údajů) PII **PII Principal**

Fyzická osoba, které se osobně identifikovatelné informace týkají (viz též subjekt údajů).

A natural person to whom the personally identifiable information (PII) relates (see also data subject).

Světelná závora **Photo Eye**

Senzor citlivý na světlo, který převádí světelný signál na signál elektrický a který produkuje binární signál závislý na přerušení paprsku světla.

A light-sensitive sensor that converts a light signal into an electrical signal, producing a binary signal based on an interruption of a light beam.

Symetrický algoritmus **Symmetric Algorithm**

Šifrovací algoritmus, který používá k šifrování i dešifrování dat stejný kryptografický klíč. Tento klíč musí mít k dispozici pouze odesilatel a příjemce šifrovaných dat, proto se tento klíč nazývá „tajný klíč“.

Encryption algorithm which uses the same cryptographic key for both encryption and decryption. This key must be available only to the sender and the recipient, and this is why this key is denoted as a „secret key“.

Symetrická kryptografie **Symmetric Cryptography / Cryptographic technique**

Kryptografická technika, která používá stejný tajný klíč jak pro odesilatele, tak pro příjemce. Poznámka: bez znalosti tajného klíče je výpočetně neproveditelné vypočítat transformace jak odesilatele, tak příjemce.

A cryptographic technique that uses the same secret key for both the originator's and the recipient's transformation. Note: Without knowledge of the secret key, it is computationally infeasible to compute either the originator's or the recipient's transformation.

SYN-cookies **SYN-cookies**

Prvek obrany proti útoku zaplavením pakety protokolu **TCP** s příznakem **SYN**. Více **SYN Flood**.

*Element of defence against a flooding by packets in the **TCP** protocol with the attribute **SYN**. See **SYN-Flood**.*

SYN-flood **SYN-flood**

Kybernetický útok (typu Denial of Service) na server zaplavením pakety protokolu TCP. Útočník zasílá záplavu TCP/SYN paketů s padělanou hlavičkou odesílatele. Každý takový paket server přijme jako normální žádost o připojení. Server tedy odešle paket SYN-ACK a čeká na paket ACK. Ten ale nikdy nedorazí, protože hlavička odesílatele byla zfalšována. Takto polootevřená žádost nějakou dobu blokuje jiné, legitimní žádosti o připojení. Více **DoS**, **DDoS**, **SYN-cookie**.

Cyber attack (Denial of Service type) on a server by flooding with packets in the TCP protocol. The attacker sends a flood of TCP/SYN packets with a forged heading of the sender. The server accepts every such packet as a normal request

for a connection. The server then sends out the SYN-ACK packet and waits for the ACK packet. This however never arrives as the heading of the sender was forged. Such a semi-open request blocks out, for some time, other legitimate requests for a connection. See DoS, DDoS, SYN-cookie.

Systém detekce průniku **Intrusion detection system (IDS)**

Technický systém, který se používá pro zjištění, že byl učiněn pokus o průnik nebo takový čin nastal, a je-li to možné, pro reakci na průnik do informačních systémů a sítí.

A technical system that is used to identify that an intrusion has been attempted, is occurring, or has occurred and possibly responds to intrusions in information systems and networks.

Systémy detekce a prevence průniku (IDPS) **Intrusion Detection and Prevention Systems (IDPS)**

Systémy, které se používají pro zjištění, že byl učiněn pokus o průnik nebo takový čin nastal, a pro aktivní reakci na průnik do informačních systémů a sítí.

Systems that are used to identify that an intrusion has been attempted, is occurring, or has occurred and actively respond to intrusions in information systems and networks.

Systém doménových jmen **Domain name system (DNS)**

Distribuovaný hierarchický jmenný systém používaný v síti Internet. Překládá názvy domén na číselné **IP** adresy a zpět, obsahuje informace o tom, které stroje poskytují příslušnou službu (např. přijímají elektronickou poštu či zobrazují obsah webových prezentací).

*Distributed hierarchical name system used on the Internet network. It translates domain names into numerical **IP** addresses and back, contains information about which machines provide the relevant service (e.g. accepts electronic mail or show the content of web pages).*

Systém odolný vůči selhání **Fault Tolerant System**

Systém, který má zabudované mechanismy, které zajišťují správnou funkci systému i při selhání určitého hardware anebo software.

A system with the built-in mechanisms to provide the correct execution of its function even in the presence of a hardware or software fault.

Systém prevence průniku — **Intrusion prevention system (IPS)**

Varianta systémů detekce průniku, které jsou zvláště určeny pro možnost aktivní reakce.

A variant on intrusion detection systems that are specifically designed to provide an active response capability.

Systém řízeného přístupu — **Controlled access system (CAS)**

Prostředky pro automatizaci fyzického řízení přístupu (např. použití odznaků vybavených magnetickými proužky, inteligentních karet, biometrických snímačů).

Means for automating of the physical control of access (e.g. use of badges equipped with magnetic strips, smart cards, biometric sensors).

Systém řízení — **Management system**

Soubor vzájemně propojených nebo vzájemně na sebe působících prvků organizace k ustavení politik strategií, cílů a procesů k dosažení těchto cíl.

Set of interrelated or interacting elements of an organisation to establish policies and objectives and processes to achieve those objectives.

Systém řízení identit — **Identity Management System (IdMS)**

Systém, který spravuje a řídí informace o identitě entit v rámci celého životního cyklu informací v určité doméně.

System controlling entity identity information throughout the information lifecycle in one domain.

Systém řízení bezpečnosti informací (SŘBI) — **Information security management system (ISMS)**

Část systému řízení, založená na přístupu k bezpečnostním rizikům, k ustavení, implementování, provozování, monitorování, přezkoumávání, spravování a zlepšování bezpečnosti informací.

Part of the management system, based on the attitude towards security risks, definition, implementation, operation, monitoring, re-analysing, administration and improvement of information security.

Systém řízení kontinuity organizace **Business continuity management system (BCMS)**

Část celkového systému řízení organizace, která ustanovuje, zavádí, provozuje, monitoruje, přezkoumává, udržuje a zlepšuje kontinuitu organizace.

Part of the overall management system that establishes, implements, operates, monitors, reviews, maintains and improves business continuity.

Šifrovací algoritmus **Encryption algorithm**

Proces, který transformuje otevřený text na šifrovaný text.

Process which transforms plaintext into ciphertext.

Šifrovací systém **Encryption system**

Kryptografická technika používaná k ochraně důvěrnosti dat, která se skládá ze tří složek: šifrovacího algoritmu, dešifrovacího algoritmu a metody generování klíčů.

Cryptographic technique used to protect the confidentiality of data, and which consists of three component processes: an encryption algorithm, a decryption algorithm, and a method for generating keys.

Šifrování **Encryption, Ciphering**

Kryptografická transformace dat (zvaných „prostý text“) do podoby (zvané „šifrovaný text“), který skrývá význam původních dat, aby se zabránilo jejich úniku či zneužití. Je-li tato transformace vratná, pak se obrácený proces, kterým se šifrovaný text převede na prostý text, nazývá dešifrování.

Cryptographic transformation of data (called “plaintext”) into a form (called “ciphertext”) that conceals the data’s original meaning to prevent it from being leaked or used. If the transformation is reversible, the corresponding reversal process is called decryption and restores the encrypted data to plaintext.

Šifrování veřejným klíčem **Public key encryption**

Šifrování prováděné asymetrickým algoritmem.

Encryption performed using an asymmetric algorithm.

Škodlivý obsah **Malicious contents**

Aplikace, dokumenty, soubory, data nebo jiné zdroje, do kterých jsou zabudovány nebo ukryty škodlivé funce či schopnosti.

Applications, documents, files, data or other resources that have malicious features or capabilities embedded or hidden.

Škodlivý software **Malware – malicious software**

Software vytvořený s nekalým úmyslem, který obsahuje funkce nebo nástroje, které mohou přímo nebo nepřímo způsobit škodu uživateli anebo počítačovému systému. Mezi škodlivý software patří počítačové viry, trojské koně, červy, špionážní software, atd.

Software designed with malicious intent containing features or capabilities that can potentially cause harm directly or indirectly to the user and the user's computer system. Malware includes viruses, trojans, worms, spyware etc.

Špatně utvořený dotaz **Malformed query**

(1) Chybný dotaz, který může vyvolat nestandardní nebo neočekávané chování systému.
(2) Způsob útoku.

(1) Erroneous query, which may result in triggering a nonstandard or unexpected behaviour of a system.
(2) Mode of an attack.

Tajná vrátka / Přístup ke službám **Maintenance hook**

Zadní vrátka v softwaru, která umožňují snadné udržování a přidání dalších charakteristik a která mohou umožnit vstup do programu v neobvyklých místech nebo bez obvyklých kontrol.

Loophole in software which enables easy maintenance and addition of other characteristics and which can enable an access to a programme in unusual locations or without the usual checks.

Tajný (proprietární) algoritmus **Secret (proprietary) algorithm**

Algoritmus, který je utajován. Jeho autorem a garantem může být státní instituce a může být určen pro použití výhradně v orgánech státu. Vlastníkem proprietárního algoritmu ale může být i soukromá společnost, která jej vyvinula a využívá ho ve své produkci. Bezpečnost těchto algoritmů může být posouzena státní institucí nebo nezávislou laboratoří a bývá obvykle doložena certifikátem. I tyto algoritmy mohou vycházet ze standardů. Potenciální útočník nemá informace o algoritmu pro cílený útok.

An algorithm which is kept secret. Its author and guarantor can be a state institution, and it may be targeted for use exclusively for state bodies. However, the owner of the proprietary algorithm can be a private company which developed it and uses it in its products. The security of these algorithms may be evaluated by a state institution or an independent laboratory and is usually attested to by a certificate. Even these algorithms can be based on standards. A potential enemy has no information about the algorithm for a targeted attack.

Tajný klíč **Secret key**

Kryptografický klíč používaný v symetrické kryptografii. Je používán k šifrování i dešifrování dat. Jedná se o (sdílené) tajemství, které musí sdílet každý, kdo je oprávněn šifrovat i dešifrovat data. Z tohoto důvodu musí být klíč utajován – odtud tajný klíč.

An encryption key used in symmetric cryptography. It is used both to encrypt and decrypt data. It is a (shared) secret to be shared by any party authorised to encrypt and decrypt data. This is the reason why the key must be kept secret – hence secret key.

Technická opatření **Technical Measures**

Bezpečnostní opatření nebo protiopatření informačního systému, která jsou primárně zaváděna a spouštěná informačním systémem prostřednictvím mechanismů integrovaných do jeho hardwarových, softwarových nebo firmwarových komponent.

The security measures or countermeasures for an information system that are primarily implemented and executed by the information system through mechanisms contained in the hardware, software, or firmware components of the system.

Technické prostředky (vybavení) **Hardware**

Fyzické součásti systému (zařízení) nebo jejich část (např. počítač, tiskárna, periferní zařízení).

Physical components of a system (equipment) or their parts (e.g. a computer, printer, peripheral devices).

Techniky zlepšující (ochranu) soukromí **Privacy enhancing technology (PET)**

Opatření týkající se (ochrany) soukromí, skládající se z opatření, produktů nebo služeb informačních a komunikačních technologií, které chrání soukromí eliminací nebo omezením osobně identifikovatelných informací (PII) nebo zabráněním zbytečného a/nebo nezamýšleného zpracování PII, a to vše bez ztráty funkčnosti systému ICT.

Measures of privacy protection, consisting of information and communication technology (ICT) measures, products, or services that protect privacy by eliminating or reducing personally identifiable information (PII) or by preventing unnecessary and undesired processing of PII, all without losing the functionality of the ICT system.

Telefonní phishing **Phone phishing**

Phishingová technika, která využívá falešného hlasového automatu (Interactive Voice Response) s podobnou strukturou jako má originální bankovní automat ("Pro změnu hesla stiskněte 1, pro spojení s bankovním poradcem stiskněte 2"). Oběť je většinou vyzvána emailem k zavolání do banky za účelem ověření informace. Zde je pak požadováno přihlášení za pomoci PIN nebo hesla. Některé automaty následně přenesou oběť do kontaktu s útočníkem vystupujícím v roli telefonního bankovního poradce, což mu umožňuje další možnosti otázek.

Phishing technique, which uses a false voice automaton (Interactive Voice Response) with a structure similar to the original banking automaton ("For a change of password press 1, for connection to a bank advisor press 2"). The victim is usually asked in an email to call the bank for information verification. Here, sign-on is requested using a PIN or a password. Some automata subsequently transfer the victim to contact with the attacker playing the role of a telephone bank advisor, which allows for other possibilities for questions.

TEMPEST **TEMPEST**

Kódové označení americké Národní bezpečnostní agentury pro zabezpečení elektronických komunikačních zařízení před kompromitujícím vyzařováním, které by v případě zachycení a analýzy mohlo odhalit přenášené, přijímané, manipulované nebo jinak zpracovávané informace.

Codename by the US National Security Agency to secure electronic communications equipment from compromising emanations, which, if intercepted and analysed, may disclose the information transmitted, received, handled, or otherwise processed.

Teplotní sensor, čidlo **Temperature Sensor**

Čidlo, které snímá teplotu okolního prostředí a vysílá elektrický signál v závislosti na teplotě.

A sensor that reads the temperature of the environment and issues an electrical signal related to its temperature.

TERENA **TERENA**

Trans-European Research and Education Networking Association, evropská mezinárodní organizace podporující aktivity v oblasti internetu, infrastruktur a služeb v rámci akademické komunity.

Trans-European Research and Education Networking Association, a European international organisation supporting activities in the area of internet, infrastructures and services in the academic community.

TF-CSIRT **TF-CSIRT**

Mezinárodní fórum umožňující spolupráci týmů **CSIRT** na evropské úrovni. Dělí se na dvě skupiny – uzavřenou, která je přístupná pouze akreditovaným týmům, a otevřenou, která je přístupná všem zájemcům o práci týmů **CSIRT**. TF-CSIRT je jednou z aktivit mezinárodní organizace **TERENA**. Pracovní skupina TF-CSIRT se schází obvykle několikrát ročně.

*International forum enabling the cooperation of **CSIRT** teams on a European level. It is divided into two groups – a closed one, which is open only to accredited teams, and an open one, which is accessible to all parties interested in the **CSIRT** teams' work. TF-CSIRT is one of the activities of the **TERENA** international organisation. Working group TF-CSIRT meets usually several times per year.*

Tlakový senzor **Pressure Sensor**

Určitý snímač, který zasílá elektrický signál na základě tlaku, kterým na něj působí okolní prostředí. Tlakové senzory mohou měřit rovněž míru změny tlaku za účelem měření hladiny a průtoku.

A certain sensor that sends an electrical signal related to the pressure acting on it by its surrounding medium. Pressure sensors can also use differential pressure to obtain level and flow measurements.

Topologie **Topology**

Topologie představuje kvalitativní geometrii popisující vzájemné uspořádání jednotlivých prvků. (např. komunikačních uzlů).

Topology is a qualitative geometry describing positions of individual elements (for example: communication nodes).

TOR (anonymní síť) **TOR (anonymity network)**

Volný software pro anonymní komunikaci, honě používaný pro přístup k DarkNetu. Název je acronym odvozený z původního názvu softwarového projektu, The Onion Router.

A free software for enabling anonymous communication, oftenly used to access DarkNet. The name is an acronym derived from the original software project name The Onion Router.

Torrent **Torrent**

Soubor s koncovkou .torrent, který obsahuje informace o jednom nebo více souborech ke stažení. Více ***BitTorrent***.

A file with the extension .torrent, which contains information about one or more files to be downloaded. See ***BitTorrent****.*

Továrna **Plant**

Viz **Závod**

See ***Plant***

Transmission control protocol **Transmission control protocol (TCP)**

Základní protokol ze sady protokolů Internetu, který představuje transportní vrstvu. Použitím TCP mohou aplikace na počítačích propojených do sítě vytvořit mezi sebou spojení, přes které mohou přenášet data. Protokol garantuje spolehlivé doručování a doručování ve správném pořadí. TCP také rozlišuje data pro vícenásobné, současně běžící aplikace (například webový server a emailový server)

běžící na stejném počítači. TCP podporuje mnoho na internetu populárních aplikačních protokolů a aplikací, včetně **WWW**, emailu a **SSH**.

*A basic protocol from the protocol set of the **Internet**; more precisely it represents the transport layer. Using the TCP, applications on interconnected computers can link up and transmit data over the links. The protocol guarantees a reliable delivery as well as delivery in the right order. TCP also differentiates data for multiple concurrently running applications (e.g. a web server and email server) running on the same computer. TCP is supported by many of the application protocols and applications popular on the Internet, including **WWW**, email and **SSH**.*

Transport layer security **Transport layer security (TLS)**

Kryptografický protokol, který poskytuje komunikační bezpečnost pro Internet. Používá se asymetrické šifrování pro výměnu klíčů, symetrické šifrování pro důvěrnost a kody pro ověřování celistvosti zpráv. Široce se používá několik verzí těchto protokolů v aplikacích jako prohlížení na webu, elektronická pošta, faxování přes internet, instantní zprávy and voice-over-IP (**VoIP**).

*A cryptographic protocol that provides communication security over the Internet. They use asymmetric cryptography for authentication of key exchange, symmetric encryption for confidentiality and message authentication codes for message integrity. Several versions of the protocols are in widespread use in applications such as web browsing, electronic mail, Internet faxing, instant messaging and voice-over-IP (**VoIP**).*

Trojský kůň **Trojan horse, trojan**

Program, který plní na první pohled nějakou užitečnou funkci, ale ve skutečnosti má ještě nějakou skrytou škodlivou funkci. Trojský kůň se sám nereplikuje, šíří se díky viditelně užitné funkci, kterou poskytuje.

A programme, which performs a useful function on the surface, but in reality, also has some hidden harmful function. The trojan horse does not replicate itself; it is distributed thanks to the visible utility it provides.

Trusted introducer **Trusted introducer**

Úřad, který sjednocuje evropské bezpečnostní týmy typu **CERT** / **CSIRT**. Zároveň také napomáhá vzniku **CERT** / **CSIRT** týmů a provádí jejich akreditace a certifikace. Je provozován organizací **TERENA**. Více **TERENA**.

The authority uniting European security teams of the type CERT/CSIRT. At the same time, it also helps in creating the CERT/CSIRT teams and provides for their

*accreditation and certification. It is operated by the TERENA organisation. See **TERENA.***

Třetí strana **Third party**

Osoba nebo organizace nezávislá jak na osobě nebo organizaci, která poskytuje předmět posuzování shody (produkt, služba), tak i na odběrateli tohoto předmětu.

Person or organisation independent both of the person or the organisation which submits the object to be judged for compliance (product, service) and also independent of the purchaser of the object.

Typ přístupu **Access type**

V počítačové bezpečnosti typ operace, specifikované přístupovým právem.

In computer security, type of an operation specified by an access right.

Tým reakce na incidenty **Incident response team (IRT)**

Skupina patřičně vyškolených, schopných a důvěryhodných pracovníků, která řeší incidenty v průběhu jejich životního cyklu. CERT (Computer Emergency Response Team) a CSIRT (Computer Security Incident Response Team) jsou obecně používané názvy pro IRT.

A team of appropriately skilled, able and trusted members of the organisation that handles incidents during their lifecycle. CERT (Computer Emergency Response Team) and CSIRT (Computer Security Incident Response Team) are commonly used terms for IRT.

Tým vyšetřovatelů **Investigative team**

Všechny osoby, které se přímo podílejí na vedení vyšetřování.

All persons directly involved in the conduct of the investigation.

Účelnost **Efficiency**

Vztah mezi dosaženými výsledky a tím, jak správně byly zdroje využity.

Relation between the achieved results and how well have the sources been used.

Údaje **Data**

Z pohledu **ICT** reprezentace informací formalizovaným způsobem vhodným pro komunikaci, výklad a zpracování.

*From the **ICT** point of view, this is a representation of information in a formalised way suitable for communication, explanation and processing.*

Údaje o zdravotním stavu **Data concerning health**

Osobní údaje týkající se tělesného nebo duševního zdraví fyzické osoby, včetně údajů o poskytnutí zdravotních služeb, které vypovídají o jejím zdravotním stavu.

Personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status.

Údaje pro ověření hesla **Password verification data**

Údaje, které slouží k ověření toho, že určitá entita zná určité heslo.

Data that is used to verify an entity's knowledge of a specific password.

Událost **Event**

Výskyt nebo změna určité množiny okolností.

Occurrence or change of a particular set of circumstances.

Událost bezpečnosti informací **Information security event**

Zjištěný výskyt stavu systému, služby nebo sítě označující možné porušení politiky bezpečnosti informací nebo selhání opatření nebo předem neznámá situace, která může být pro bezpečnost závažná.

Identified occurrence of a system, service or network state indicating a possible breach of information security policy or a failure of controls, or a previously unknown situation that may be security relevant.

Událost hrozby **Threat Event**

Událost nebo situace, která má potenciál způsobit nežádoucí následky nebo dopady.

An event or situation that has the potential for causing undesirable consequences or impacts.

Údržba **Maintenance**

(1) Jakákoliv činnost, která buď zabraňuje poruše, nebo selhání zařízení, nebo obnovuje jeho provozní schopnosti.
(2) Jakákoliv změna aplikace po jejím dodání (např. oprava chyb, rozšíření funkcí, zvýšení výkonu či zlepšení funkce aplikace).

(1) Any act that either prevents a failure or malfunction of equipment or restores its operating capability.
(2) Any change in an application after its delivery (e.g. error correction, added functionality, enhanced performance or improvement of the application's functionality).

Úmyslné oklamání, podvržení **Spoofing**

Činnost s cílem podvést (oklamat) uživatele nebo provozovatele zpravidla pomocí předstírání falešné identity.

Activity with the objective of deceiving (misleading) a user or operator usually by sporting a false identity.

Uniform resource locator **Uniform resource locator (URL)**

Zdrojový identifikátor, který popisuje umístění konkrétního zdroje, včetně protokolu, sloužící k načítání tohoto zdroje. Nejznámějším příkladem URL je např. *http://www.nejakadomena.nekde*.

Source identifier describing the location of a concrete source, including a protocol, serving to link to this source. The best known such an example is http://www.somedomain.somewhere.

Universální unikátní identifikátor **Universal unique identifier (UUID)**

Standard pro identifikátory používaná při tvorbě softwaru, standardizovaný organizací Open Software Foundation (**OSF**) jako součást Distributed Computing Environment (**DCE**).

*An identifier standard used in software construction, standardised by the Open Software Foundation (**OSF**) as part of the Distributed Computing Environment (**DCE**).*

Upřednostněné činnosti **Prioritised activities**

Činnosti, kterým musí být bezprostředně po incidentu dána přednost, aby byly zmírněny dopady.

Activities that must be prioritised in the immediate aftermath of an incident to mitigate impacts

URL trojan **URL trojan**

Přesměrovává infikované počítače připojené přes vytáčené připojení k Internetu na dražší tarify. Více hesla **Dialer** a **Trojan Horse**.

*It redirects infected computers connected via the dial-in Internet connection to more expensive rates. See **Dialer** and **Trojan Horse**.*

Úroveň přístupu **Access level**

Úroveň autorizace požadovaná pro přístup k chráněným zdrojům.

Level of authorisation required to access protected sources.

Úroveň rizika **Level of risk / risk level**

Velikost rizika vyjádřená jako kombinace následků a jejich pravděpodobnost.

The magnitude of the risk expressed in terms of the combination of consequences and their likelihood.

Úřad pro přidělování čísel na Internetu **Internet assigned numbers authority (IANA)**

Autorita, která dohlíží na přidělování **IP adres**, správu kořenových zón **DNS** (přidělování **TLD** domén a vznik generických domén) a správu a vývoj internetových protokolů. V současné době je **IANA** jedním z oddělení organizace **ICANN**.

*Authority oversseing **IP address** assignment, administration of **DNS** zones (assignment of **TLD** domains and the creation of generic domains) and the administration and development of internet protocols. At present, **IANA** is one of the departments of the **ICANN** organization.*

User datagram protocol **User datagram protocol (UDP)**

Internetový síťový protokol pro nespojovou komunikaci (RFC 768).

An Internet networking protocol for unconnected communications (RFC 768).

Ustálený stav **Steady State**

Stav, kdy určitá vlastnost, např. hodnota, rychlost, periodicita nebo amplituda, vykazuje pouze zanedbatelnou změnu po libovolně dlouhou dobu.

A state when a specific property, such as value, speed, periodicity, or amplitude, exhibits only negligible change over an arbitrarily long period.

Útočník **Attacker**

Osoba úmyslně využívající zranitelnosti v technických nebo netechnických bezpečnostních opatřeních s cílem zcizit, nebo ohrozit informační systémy a sítě, nebo narušit dostupnost informačních systémů a síťových zdrojů legitimním uživatelům

A person deliberately exploiting vulnerabilities in technical and non-technical security controls in order to steal or compromise information systems and networks, or to compromise availability to legitimate users of the information systems.

Útočný potenciál **Attack potential**

Míra útočného úsilí, které je určitý útočník schopen vyvinout na určitý cíl vyjádřená v závislosti na schopnostech, zdrojích a motivaci útočníka.

Measure of the attack effort to be expended in attacking a target, expressed in terms of an attacker's expertise, resources and motivation.

Útok **Attack**

Pokus o zničení, vystavení hrozbě, změnu, vyřazení z činnosti, zcizení aktiva nebo získání neoprávněného přístupu k aktivu nebo uskutečnění neoprávněného použití aktiva.

Attempting to destroy, compromise, alter, disable, steal or gain unauthorised access to an asset or to make unauthorised use of an asset.

Útok hrubou silou **Brute force attack**

Metoda k zjišťování hesel, kdy útočící program zkouší jako možné heslo všechny existující kombinace znaků, dokud nezjistí skutečné heslo. Tento způsob je časově

velmi náročný. Jeho úspěšnost je závislá na délce hesla, složitosti hesla a na výpočetním výkonu použitého počítače.

Method to find passwords when the attacking programme tries all existing character combinations for a possible password. This method is very time-consuming. Its success depends on password length and the computing power of the computer used.

Útok na počítačovou síť **Computer network attack (CNA)**

Činnost realizovaná za účelem narušit, blokovat, znehodnotit nebo zničit informace uložené v počítači anebo na počítačové síti, či počítač anebo počítačovou síť samotnou. Útok na počítačové síti je určitým druhem kybernetického útoku.

Activity done to corrupt, block, degrade or destroy information stored in a computer or on a computer network, or the computer or computer network as such. The attack on a computer network is a certain sort of cyber attack.

Útok postranním kanálem **Side-channel attack**

Útok provedený na základě na znalosti fyzické implementace kryptografického systému, spíše než na základě hrubé síly, nebo teoretických slabin použitého kryptografického algoritmu. K útoku postranním kanálem lze využít například informace o časování, spotřebě energie nebo elektromagnetickém vyzařování.

An attack based on information gained from the physical implementation of a cryptosystem, rather than on the brute force or theoretical weaknesses in the underlying algorithm. A side-channel attack may use, for example, timing information, power consumption, or electromagnetic emissions.

Uzavřené bezpečnostní prostředí **Closed-security environment**

Prostředí, ve kterém je věnována zvláštní pozornost (formou autorizací, bezpečnostních prověření, řízení konfigurace atd.) ochraně dat a zdrojů před náhodnými nebo úmyslnými činy.

Environment where special attention (by a form of authorisations, security checks, configuration control, etc.) is given to protection of data and sources from accidental or intentional actions.

Uživatel **User**

Každá fyzická nebo právnická osoba, která využívá službu informační společnosti, zejména za účelem vyhledávání či zpřístupňování informací.

Any natural or legal person using a service of the information society in order to look for, or make access to, information.

Uživatelský profil **User profile**

Popis uživatele, typicky používaný pro řízení přístupu. Může zahrnovat data jako ID uživatele, jméno uživatele, heslo, přístupová práva a další atributy.

Description of a user typically used for access control. It may include data such as user ID, user name, password, access rights and other attributes.

V reálném čase **Real-Time**

Ve vztahu k výkonu: výpočet určitých výsledků v průběhu skutečného času, ve kterém běží související fyzický proces, díky tomu tyto výsledky lze využít k řízení daného procesu.

Pertaining to the performance: computation of certain results during the actual time that the related physical process is running, so that the results could be used to control the physical process.

Vada / skulina **Flaw / loophole**

Provozní nefunkčnost, vynechání, nebo přehlédnutí, která umožňuje, aby byly ochranné mechanizmy obejity nebo vyřazeny z činnosti.

Operational dysfunction, omission, or oversight making it possible to bypass protective mechanisms or put them out of action.

Validace dat **Data validation**

Proces používaný k určení, zda data jsou přesná, úplná nebo splňují specifikovaná kritéria. Validace dat může obsahovat kontroly formátu, kontroly úplnosti, kontrolní klíčové testy, logické a limitní kontroly.

The process used to determine if data are accurate, complete, or satisfy specified criteria. Data validation may contain checks of format, checks for completeness, control key tests, logical and limit checks.

Validace identity **Identity validation**

Vykonání testů umožňujících systému na základě zpracování dat rozpoznat a ověřit entity.

Execution of tests enabling a system to recognise and validate entities on the basis of data processing.

Varování **Alert**

"Okamžité" upozornění, že informační systém a síť mohou být pod útokem nebo v ohrožení kvůli nehodě, selhání nebo lidské chybě.

"Instant" indication that an information system and network may be under attack, or in danger because of accident, failure or human error.

Vedoucí pro ochranu osobních údajů **Chief privacy officer (CPO)**

Vyšší vedoucí pracovník, který je v organizaci odpovědný za ochranu osobních údajů.

Senior management individual who is accountable for the protection of personally identifiable information in an organization.

Vedoucí týmu vyšetřovatelů **Investigative lead**

Osoba vedoucí vyšetřování na strategické úrovni.

Person leading the investigation at a strategic level.

Vektor útoku **Attack vector**

Cesta nebo nástroje, pomocí nichž útočník může získat přístup do počítače nebo síťového serveru aby mohl dosáhnout svých nekalých záměrů.

A path or means by which an attacker can gain access to a computer or network server to deliver a malicious outcome.

Velikonoční vajíčko **Easter egg**

Skrytá a oficiálně nedokumentovaná funkce nebo vlastnost počítačového programu, DVD nebo CD. Většinou se jedná pouze o neškodné hříčky a vtípky, grafické symboly, animace, titulky se jmény tvůrců apod. Tato skrytá funkce se nevyvolává obvyklým způsobem (menu, tlačítko apod.), ale netradiční kombinací běžných uživatelských činností, stiskem myši na nějakém neobvyklém místě, zvláštní posloupností stisku konkrétních kláves apod. Často bývají vajíčka skryta v obrazovce „O programu" („About"), kde se dají zobrazit např. po poklepání na různé části tohoto panelu s podržením klávesy ALT apod.

Hidden and officially undocumented function or property of a computer programme, DVD or CD. Mostly these are puns and jokes doing no harm, graphics symbols, animations, subtitles with authors' names and similar. This hidden

function is not activated in the usual way (menu, key, etc.) but by an unorthodox combination of the usual user activities, pushing a mouse key on an unusual place, a special sequence of keys, and so on. Often, eggs are hidden on the screen under "About" where these can be displayed by tapping on various parts of this panel while holding the key ALT and similar.

Ventil **Valve**

Mechanické zařízení regulující průtok tekutin (plynů, kapalin, zkapalněných tuhých látek, kalů atd.) v potrubí. Může přerušit průtok, regulovat jeho objem nebo ho přesměrovat do jiné větve systému. Pojem ventil v české strojařské terminologii zahrnuje také kohouty, šoupátka a klapky.

A mechanical device regulating the flow of fluids (gases, fluidised solids, slurry, etc.) in piping. It may interrupt the flow, regulate its volume and direct it to another branch of the system. In the Czech mechanical engineering terminology, the vent also includes taps, slide valves and flap valves.

Veřejná IP adresa **Public IP address**

IP adresa, která je směrovatelná v **Internetu**. Takováto IP adresa je tedy dostupná z celé sítě **Internetu**, pokud tomu nebrání například konfigurace **firewallu** či routeru.

*The IP address that is routable on the **Internet**. Such an address is then accessible from the whole **Internet** network unless prohibited, for example, by **firewall** or router configuration.*

Veřejná komunikační síť **Public telecommunication network**

Síť elektronických komunikací, která slouží zcela nebo převážně k poskytování veřejně dostupných služeb elektronických komunikací, a která podporuje přenos informací mezi koncovými body sítě, nebo síť elektronických komunikací, jejímž prostřednictvím je poskytovaná služba šíření rozhlasového a televizního vysílání.

A network of electronic communications serving, wholly or predominantly to provide publicly available services of electronic communications, and which supports information transfer among the endpoints of the network, or a network of electronic communications through which radio and television broadcast are provided as a service.

Veřejná telefonní síť **Public telephone network**

Síť elektronických komunikací, která slouží k poskytování veřejně dostupných telefonních služeb a která umožňuje mezi koncovými body sítě přenos mluvené řeči, jakož i jiných forem komunikace, jako je faksimilní a datový přenos.

A network of electronic communications to provide publicly available telephone services, and which allows for the transmission of voiced speech as well as other forms of communications, such as facsimiles and data transmissions, among the endpoints of the networks.

Veřejně dostupná služba elektronických komunikací — **Publicly available electronic communications service**

Služba elektronických komunikací, z jejíhož využívání není nikdo předem vyloučen.

Service of electronic communications from whose use no one may be a priori excluded.

Veřejně známý kryptografický algoritmus — **Published cryptographic algorithm**

Algoritmus, který byl publikován, je veřejně dostupný a je založený na otevřených zdrojích. Zpravidla se jedná o kryptografický standard, který je možno využívat bez omezení. Bezpečnost systému je závislá na kryptografickém klíči, který není známý (Kerckhoffův princip). Jedná se nejen o symetrické a asymetrické šifrovací algoritmy ale i další funkce používané v kryptografii. Tyto algoritmy a funkce jsou veřejností neustále testovány na různé typy útoků, a pokud jim odolávají, jsou považovány za bezpečné. Současně má ale potenciální útočník veškeré informace k cílenému útoku (kromě kryptografického klíče). Nové typy útoků a zvyšování výpočetní kapacity počítačů vede ke zvyšování velikosti kryptografických klíčů a přijímání nových standardů pro zachování bezpečnosti těchto algoritmů.

An algorithm, which has been published, is publicly available and based on open sources. Usually, it is a cryptographic standard to be used without any limitations. System security is based on a cryptographic key which not known (Kerckhoff's principle). It applies to symmetric and asymmetric encryption algorithms as well as other functions used in cryptography. These algorithms and functions keep being tested by the public against all sorts of attacks and if they withstand these, are considered secure. At the same time, a potential attacker has all the information for a targeted attack (except the cryptographic key). New types of attacks and an increase in computing power lead to an increase in the length of cryptographic keys and the adoption of new standards to keep these standards secure.

Veřejný informační systém **Public information system**

Informační systém poskytující služby veřejnosti, který má vazby na informační systémy veřejné správy.

Information system providing services to the public and having relations to information system of the public administration.

Veřejný klíč **Public key**

Klíč v asymetrické kryptografii, který může být zveřejněn. Veřejný klíč tvoří pár se soukromým klíčem.

A key of an entity's asymmetric key pair, which can be made public. A public key is paired with a private key.

Více faktorová autentizace **Multi-factor authentication**

Ověřování pomocí dvou nebo více faktorů autentizace.

Authentication using two or more of the authentication factors.

Virtuální aktivum **Virtual asset**

Zastoupení aktiva v kyberprostoru. Poznámka: V tomto kontextu lze měnu definovat buď jako prostředek směny, nebo jako majetek, který má hodnotu v určitém prostředí, například ve videohře nebo v simulaci finančního obchodování.

Representation of an asset in the Cyberspace. Note: In this context, currency can be defined as either a medium of exchange or a property that has value in a specific environment, such as a video game or a financial trading simulation exercise.

Virtuální lokální síť **Virtual local area network (VLAN)**

Logicky nezávislá síť v rámci jednoho nebo více zařízení. Virtuální sítě lze definovat jako domény všesměrového vysílání (Více **LAN**) s cílem učinit logickou organizaci sítě nezávislou na fyzické vrstvě.

*Logically independent network in the framework of one or more devices. Virtual networks can be defined as the domains of all-directional broadcast (See **LAN**) with the objective of making the logical network organisation independent of the physical network.*

Virtuální měna **Virtual currency**

Virtuální peněžní aktiva.

Monetary virtual assets.

Virtuální privátní síť **Virtual private network (VPN)**

Privátní počítačová síť, která dovolí připojit vzdálené uživatele do cílené ***LAN*** přes ***Internet***. Bezpečnost se řeší pomocí šifrovaného tunelu mezi dvěma body (nebo jedním a několika). Při navazování spojení je totožnost obou stran ověřována pomocí digitálních certifikátů.

A private computer network allowing for the connection of remote users to the target LAN via the Internet. Security is tackled using an encrypted tunnel between two points (or among one and several points). The identity of both parties is verified using digital certificates when making the connection.

Virtuální stroj **Virtual machine (VM)**

Softwarově definovaný kompletní prováděcí zásobník sestávající z virtualizovaného hardwaru, operačního systému (hostujícího OS) a aplikací.

Software-defined complete execution stack consisting of virtualized hardware, operating system (guest OS), and applications.

Virus **Virus**

Typ malware, který se šíří z počítače na počítač tím, že se připojí k jiným aplikacím. Následně může působit nežádoucí a nebezpečnou činnost. Má v sobě obvykle zabudován mechanismus dalšího šíření či mutací.

Type of malware spreading from one computer to another by attaching itself to other applications. Consequently, it may cause unwanted and dangerous activity. Usually, it has a built-in mechanism for further distribution or mutations.

Vlastník aktiva **Asset owner**

Jedinec, nebo entita, který má vedením organizace přidělenou odpovědnost za výrobu, vývoj, údržbu, použití a bezpečnost aktiva.

An individual or entity whom the organisation management has assigned the responsibility for production, development, maintenance, use and security of an asset.

Vlastník aplikace **Application owner**

Organizační role odpovědná za správu, využívání a ochranu aplikace a jejích dat. Poznámka: Vlastník aplikace činí veškerá rozhodnutí týkající se zabezpečení aplikace.

Organizational role responsible for the management, utilization and protection of the application and its data. Note: The application owner makes all decisions pertaining to the application's security.

Vlastník rizika **Risk owner**

Osoba nebo entita s odpovědností a oprávněním řídit riziko.

Person or entity with the accountability and authority to manage a risk.

Vnější kontext **External context**

Vnější prostředí, ve kterém se organizace snaží dosáhnout svých cílů.

The external environment in which an organisation seeks to achieve its objectives.

Vnitřní kontext **Internal context**

Vnitřní prostředí, ve kterém se organizace snaží dosáhnout svých cílů.

the internal environment in which an organisation seeks to achieve its objectives.

Vnitřní, interní skupina **Internal group**

Část organizace poskytovatele služeb, která uzavřela dokumentovanou dohodu s poskytovatelem služeb o svém podílu na návrhu, přechodu, dodávce a zlepšování služby nebo služeb.

Part of an organisation of a service provider, which has concluded a documented contract with the service provider about its share in the design, handover, delivery and improvement of a service or services.

Vrcholové vedení **Top management**

Osoba nebo skupina osob, která na nejvyšší úrovni vede a řídí organizaci.

A person or a group of persons who lead the organisation at the highest level.

Vstup přes autorizovaného uživatele **Piggyback entry**

Neautorizovaný přístup k systému prostřednictvím legitimního spojení autorizovaného uživatele.

Unauthorised access to the system using a legitimate link of an authorised user.

Vstup / výstup (I/O) **Input/Output (I/O)**

Zařízení, které slouží ke komunikaci s počítačem anebo údaje obsažené v komunikaci.

Equipment that is used to communicate with a computer as well as the data involved in the communications.

Vstupně-výstupní (I/O) server **Input/output (I/O) server**

Řídicí prvek určený ke sběru, dočasnému uložení a zpřístupnění procesních informací z řídicích prvků jako jsou PLC, RTU či IED. I/O server může běžet na řídicím serveru nebo na samostatném počítači. I/O servery jsou často využívány pro komunikaci s řídicími prvky třetích stran, například HMI nebo řídicí server.

A control component responsible for collecting, buffering and providing access to process information from control subcomponents such as PLCs, RTUs and IEDs. An I/O server can reside on the control server or a separate computer. I/O servers are often used for interfacing third-party control components, such as an HMI or a control server.

Vybavení pro zpracování informací **Information processing facilities**

Jakýkoliv systém, služba nebo infrastruktura pro zpracování informací anebo fyzické místo, kde se nacházejí.

Any information processing system, service or infrastructure, or the location where they reside.

Výbor pro řízení kybernetické bezpečnosti **Cyber security management committee**

Definovaná bezpečnostní role v souladu se zákonem o kybernetické bezpečnosti, představující organizovanou skupinu tvořenou osobami, které jsou pověřeny celkovým řízením a rozvojem systémů spadajících pod zákon o kybernetické

bezpečnosti, anebo se významně podílejí na řízení a koordinaci činností spojených s kybernetickou bezpečností těchto systémů.

A defined security role in accordance with the Cyber Security Act, representing an organised group consisting of persons who are entrusted with the overall management and development of systems covered by the Cyber Security Act, or are significantly involved in the management and coordination of activities related to the cyber security of these systems.

Vycpávka (Padding) **Padding**

Přidání dalších bitů do datového řetězce. Například u blokové šifry je poslední blok doplněn těmito bity na požadovanou velikost bloku.

Appending extra bits to a data string. For example, in a block cipher, the last block is filled up with these bits to the required size of the block.

Vyčistit **Sanitize**

Proces vymazání informací z určitého media takovým způsobem, že je není možné s danou mírou úsilí obnovit.

A process to remove information from media such that data recovery is not possible at a given level of effort.

Vyčištění **Clearing**

Cílené přepsání nebo vymazání klasifikovaných dat na datovém mediu, které má speciální bezpečnostní klasifikaci a bezpečnostní kategorii, takže dané medium může být opakovaně použito pro zápis ve stejné bezpečnostní klasifikaci a bezpečnostní kategorii.

the targeted overwriting or erasure of classified data on a data medium which has a special security classification and security category so that the given medium could be repeatedly used for a record in the same security classification and security category.

Vydavatel autorizačních údajů **Credential issuer**

Subjekt odpovědný za poskytování pověření zadavateli v určité doméně.
Poznámka 1 k položce: Pověření poskytované vydavatelem pověření může mít fyzickou podobu, např. členskou (čipovou) kartu.
Poznámka 2 k položce: Vydání pověření pro zadavatele lze zaznamenat jako atribut zadavatele, např. zaznamenáním jedinečného čísla vydaného tokenu.

Poznámka 3 k položce: Pověření poskytnuté vydavatelem může být uživatelské jméno a heslo. Pověření ve formě čipové karty nebo podobného bezpečnostního zařízení může být nakonfigurováno tak, aby ověřovalo heslo off-line.

Entity responsible for provisioning of a credential to a principal in a specific domain
Note 1 to entry: A credential provisioned by a credential issuer can have a physical form, e.g. a membership (smart) card.
Note 2 to entry: The issuance of a credential for a principal can be recorded as an attribute for the principal, e.g. by recording the unique number of the token issued.

Note 3 to entry: A credential provisioned by an issuer can be a username and password. A credential in the form of a smart card or similar security device, can be configured to validate a password off-line.

Vydání, vydaná verze **Release**

Soubor jedné nebo více nových či změněných konfiguračních položek, které jsou nasazovány do provozního prostředí jako výsledek jedné nebo více změn.

The aggregate of one or more new or changed configuration items which are put into the operational environment as the result of one or more changes.

Vyhnutí se riziku **Risk avoidance**

Rozhodnutí nedopustit zapojení se do rizikových situací, nebo je vyloučit.

Decision not to allow an involvement into risk situations, or to exclude these.

Výchozí stav konfigurace **Configuration baseline**

Konfigurační informace formálně se vztahující k určitému času během života služby nebo prvku služby.

Configuration information formally related to a certain time in the lifetime of a service, or element of the service.

Výkonné vedení **Executive management**

Osoba nebo skupina osob, na které orgán řízení a správy svěřil odpovědnost za uskutečnění strategií a politik k dosažení cílů organizace. Výkonné vedení je někdy nazýváno vrcholovým vedením a může zahrnovat generálního ředitele, finančního ředitele, informačního ředitele a podobné role.

A person or group of people who have delegated responsibility from the governing body for the implementation of strategies and policies to accomplish the purpose of the organisation. Executive management is sometimes called top management and can include Chief Executive Officer, Chief Financial Officer, Chief Information Officer, and similar roles.

Výkonnost **Performance**

Měřitelný výsledek.

Measurable result.

Výpadek proudu (rozsáhlý), blackout **Outage (large), Blackout**

Rozsáhlý výpadek elektrického proudu.

Widespread electrical power outage.

Výrobní informační systém **Manufacturing Execution System (MES)**

Systém, který využívá počítačové sítě k automatizaci řízení výroby a k automatizaci procesů. Stažením receptur a pracovních plánů a zpětným nahráním výstupů výroby MES vyplňuje mezeru mezi řídicí a provozní úrovní nebo mezi výrobními a řídicími systémy.

A system that uses network computing to automate production control and process automation. By downloading recipes and work schedules and uploading production results, an MES bridges the gap between control and operational level or between production and control systems.

Výrobní řídicí jednotka **Process Controller**

Typ počítačového systému, zpravidla montovaný do rozvaděče, který zpracovává vstupy ze senzorů, aplikuje na ně řídicí algoritmy a posílá výstupy do akčních členů.

A type of computer system, typically rack-mounted, that processes sensor inputs, applies on them control algorithms, and issues actuator outputs.

Vystavení hrozbám **Exposure**

Možnost, že konkrétní útok využije specifickou zranitelnost systému zpracování dat.

The possibility that a concrete attack would use a specific vulnerability of a data processing system.

Výstupní promněnná **Manipulated Variable**

Hodnota, nebo podmínka, kterou řídicí prvek vysílá do akčního členu, aby ovlivnil hodnotu řízené proměnné.

The value or condition that the control sendsto initiate a change in the value of the regulated variable.

Vyšetřování incidentu bezpečnosti informací **Information security investigation**

Získávání, zkoumání, analýza a interpretace stop a důkazů s cílem vysvětlit podstatu incidentu informační bezpečnosti.

Acquisition, examinations, analysis and interpretation of traces and proofs to aid understanding the nature of an information security incident.

Vytěžování počítačové sítě **Computer network exploitation (CNE)**

Zneužití informací uložených na počítači nebo v počítačové síti.

Abuse of information stored on the computer or computer network.

Využití návnady **Baiting**

Způsob útoku, kdy útočník nechá infikované CD, flashdisk nebo jiné paměťové médium na místě, kde jej oběť s velkou pravděpodobností nalezne, např. ve výtahu, na parkovišti. Poté již nechá pracovat zvědavost, se kterou oběť dříve či později vloží toto médium do svého počítače. Tím dojde k instalaci viru, za pomoci kterého získá útočník přístup k počítači nebo celé firemní počítačové síti.

Mode of attack when the attacker leaves an infected CD, flash disc or another storage medium where the victim can find it with a high probability, e.g. in a lift, on the car park. This leaves curiosity to play out and sooner or later the victim inserts the medium into the computer. This results in virus installation with which the attacker gets access to the computer or the whole companywide computer network.

Vývojový digram **Flow chart**

Grafický programovací jazyk vycházející z vývojových diagramů, jejichž funcionalitu reprezentují. Je součást normy IEC 61113-3.

A graphic programming language based on flowcharts whose functionality they represent. It is part of IEC 61113-3.

Významná síť **Important network**

Síť elektronických komunikací definovaná zákonem o kybernetické bezpečnosti, zajišťující přímé zahraniční propojení do veřejných komunikačních sítí nebo zajišťující přímé připojení ke kritické informační infrastruktuře.

A network of electronic communications as defined by the law on cyber security and enabling direct link into foreign communication networks or enabling direct connection to critical information infrastructure.

Významný informační system **Important information system**

Komplex informačních systémů podle zákona o kybernetické bezpečnosti, které spravují orgány veřejné moci, které nejsou kritickou informační infrastrukturou a u kterých by mohlo porušení bezpečnosti informací omezit nebo výrazně ohrozit výkon působnosti orgánu veřejné moci.

Complex of information systems according to the law on cyber security, managed by the public administration bodies, which themselves are not a part of the critical infrastructure, and where any infringement of information security would limit or seriously endanger the function of a public administration body.

Vzdálená diagnostika **Remote Diagnostics**

Diagnostika prováděná jednotlivci komunikujími z vnějšku bezpečnostního perimetru informačního systému.

Diagnostic activities conducted by individuals communicating externally to an information system security perimeter.

Vzdálená termínálová jednotka **Remote Terminal Unit (RTU)**

(1) Počítač s bezdrátovým rozhraním, který se používá tam, kde není možné optické či metalické připojení. Zpravidla se používá pro komunikaci se vzdáleným výrobním vybavením.
(2) Specifická řídicí jednotka, která se využívá v rámci DCS a SCADA systémů pro podporu vzdálených stanic. RTU je výrobní zařízení často vybavené síťovým rozhraním, které může být bezdrátové, metalické nebo optické a umožňuje

komunikaci s dohledovou a řídicí jednotkou. Někdy tuto roli plní PLC s komunikačním rozhraním v takovém případě se o PLC mluví jako o RTU.

(1) A computer with wireless interfacing used in remote situations where communications via wire or optics are unavailable. Usually used to communicate with remote field equipment.
(2) A special purpose data acquisition and control unit designed to support DCS and SCADA remote stations. RTUs are field devices often equipped with network capabilities, which can include wired and wireless radio interfaces to communicate to the supervisory controller. Sometimes PLCs are implemented as field devices to serve as RTUs; in this case, the PLC is often referred to as an RTU.

Vzdálená údržba **Remote Maintenance**

Údržba prováděná jednotlivci komunikujícími z vnějšku bezpečnostního perimetru informačního systému.

Maintenance activities conducted by individuals communicating external to an information system security perimeter.

Vzdálený přístup **Remote access**

Proces využití síťových zdrojů z jiné sítě nebo z koncového zařízení, které není stále připojené – fyzicky nebo logicky – do sítě, do které přistupuje.

A process of accessing network resources from another network, or from a terminal device, which is not permanently connected, physically or logically, to the network it is accessing.

Vzdálený přístupový bod **Remote Access Point**

Určitá zařízení, oblasti a místa řídicí sítě pro vzdálenou konfiguraci řídicího systému a vzdálený přístup k údajům o výrobě. Např. využití mobilního zařízení k přístupu k datům prostřednictvím WLAN, nebo využití laptopu a modemu ke vzdálenému přístupu k ICS systému.

Certain devices, areas and locations of a control network for remotely configuring control systems and accessing process data. E.g. using a mobile device to access data over a WLAN, or using a laptop and modem connection to remotely access an ICS system.

Vzdálený uživatel **Remote User**

Uživatel nacházející se na jiném místě, než na kterém se nachází síťové zdroje, které právě využívá.

User at a site other than the one at which the network resources being used are located.

Wardriving **Wardriving**

Vyhledávání nezabezpečených bezdrátových Wi-Fi sítí osobou jedoucí v dopravním prostředku, pomocí notebooku, PDA nebo smartphonem.

Searching for insecure wireless Wi-Fi networks by a person sitting in a means of transport, using a notebook, PDA or smartphone.

Warez **Warez**

Slangové označení autorská díla, se kterými je nakládáno v rozporu s autorským právem. Podle druhu bývá někdy warez rozdělován na gamez (počítačové hry), appz (aplikace), crackz (cracky) a také moviez (filmy). Nejčastějším způsobem šíření warezu je dnes hlavně **Internet**.

A term from the computer slang denoting copyright-protected creations, which are treated in violation of the copyright. Warez is sometimes split into gamez (computer games), appz (applications), crackz (cracks) and also moviez (films). Today, the most frequent way of distribution is mainly the Internet.

Webový vandalizmus **Web vandalism**

Útok, který pozmění (zohyzdí) webové stránky nebo způsobí odmítnutí služby (denial-of-service attacks).

The attack which alters (defaces) web pages or causes a service denial (denial-of-service attacks).

White hat **White hat**

Etický hacker, který je často zaměstnáván jako expert počítačové bezpečnosti, programátor nebo správce sítí. Specializuje se na penetrační testy a jiné testovací metodiky k zajištění IT bezpečnosti v organizaci.

An ethical hacker who is often employed as an expert in computer security, programmer or network administrator. He or she specialises in penetration tests and other testing methodologies to ensure IT security in an organisation.

Whitelist, bílá listina **Whitelist**

Určitý seznam jednotlivých entit, například hostů či aplikací, o kterých je známo, že jsou neškodné a jsou schválené k používání uvnitř určité organizace anebo informačního systému.

A list of discrete entities, such as hosts or applications that are known to be benign and are approved for use within an organisation or information system.

Whois **Whois**

Internetová služba, která slouží pro zjišťování kontaktních údajů majitelů internetových domén a IP adres.

Internet service to find contact data of the owners of internet domains and IP addresses.

WiFi **WiFi**

Bezdrátová technologie pro šíření dat („vzduchem“), vhodná pro tvorbu sítových infrastruktur tam, kde je výstavba klasické kabelové sítě nemožná, obtížná nebo nerentabilní (kulturní památky, sportoviště, veletrhy). Pro přenos dat postačí vhodně umístěné navazující přístupové body, lemující cestu od vysílače k příjemci.

Wireless technology for data distribution ("by air"), suitable for the creation of network infrastructures in places where the building of a classical cable network is impossible, difficult or not cost-effective (cultural monuments, sports facilities, fairgrounds). Suitably located successive points of access along the route from the transmitter to the recipient are sufficient for data transmission.

WiMax **WiMax**

Telekomunikační technologie, která poskytuje bezdrátový přenos dat pomocí nejrůznějších přenosových režimů, od point-to-multipoint spojení pro přenos a plně mobilní internetový přístup.

Telecommunication technology providing wireless data transmission using various transmission modes, from point-to-multipoint to completely mobile internet access for the transmission.

Wireshark **Wireshark**

Dříve **Ethereal.** Protokolový analyzer a paketový sniffer, který umožňuje odposlouchávání všech protokolů, které počítač přijímá / odesílá přes síťové rozhraní. Wireshark dokáže celý paket dekódovat a zobrazit tak, jak jej počítač odeslal. Jeho výhodou je, že je šířen pod svobodnou licencí **GNU / GPL**.

*Formerly **Ethereal**. Protocol analyser and packet sniffler, which enables eavesdropping of all protocols which the computer receives and sends via an interface. Wireshark can decode the whole packet and show it in a way as sent out by the computer. Its advantage is that it is distributed under a free licence **GNU/GPL**.*

World wide web **World wide web (WWW)**

Graficky orientovaná služba **Internetu** – systém vzájemně propojených hypertextových stránek využívajících formátovaný text, grafiku, animace a zvuky.

*Graphically-oriented service of the **Internet** – a system of interconnected hypertext pages using formatted text, graphics, animation and sounds.*

X.509 **X.509**

Standard pro systémy založené na veřejném klíči (**PKI**) pro jednoduché podepisování. X.509 specifikuje např. formát certifikátu, seznamy odvolaných certifikátů, parametry certifikátů a metody kontroly platností certifikátů.

*The standard for systems based on the public key (**PKI**) for simple signatures. X.509 specifies, for example, the format of a certificate, lists of cancelled certificates, parameters of certificates and methods for checking the validity of certificates.*

Zadní vrátka **Backdoor / trapdoor**

Skrytý softwarový nebo hardwarový mechanizmus obvykle vytvořený pro testování a odstraňování chyb, který může být použít k obejití počítačové bezpečnosti. Metoda v počítačovém systému nebo v algoritmu, která útočníkovi umožňuje obejít běžnou autentizaci uživatele při vstupu do programu nebo systému a zároveň mu umožňuje zachovat tento přístup skrytý před běžnou kontrolou. Pro vniknutí do operačního systému mohou obejít ***firewall*** například tím, že se vydávají za webový prohlížeč. Tento kód může mít formu samostatně instalovaného programu nebo se jedná o modifikaci stávajícího systému. Samotný vstup do systému pak mívá formu zadání fiktivního uživatelského jména a hesla, které napadený systém bez kontroly přijme a přidělí uživateli administrátorská práva.

*Hidden software or hardware mechanism usually created for testing and error removal, which can be used to bypass computer security. A method in a computer system or in an algorithm, which allows the attacker to bypass the normal user authentication at the access to a programme or system and simultaneously allows to have this access hidden from normal checks. A **firewall** can be bypassed, to penetrate the operating system, for example, by pretending to be a web browser.*

This code can assume the form of an independently installed programme, or it could be a modification of an existing system. The access to the system as such tends to have the form of a fictitious user name and password, which the attacked system accepts without checking and assigns to the user administrative rights.

Zahlcení pingy **Ping flood**

Jednoduchý ***DoS*** útok, kdy útočník zaplaví oběť s požadavky „ICMP Echo Request“ (ping). Útok je úspěšný, pokud útočník má větší šířku pásma, než oběť, nebo může kooperovat s dalšími útočníky současně. Více ICMP flood.

*Simple **DoS** attack when the attacker floods the victim with requests "ICMP Echo Request" (ping). The attack is successful provided the attacker has a wider bandwidth than the victim, or, the attacker can cooperate with other attacker simultaneously. See **ICMP flood**.*

Zahlcení TCP SYN **TCP SYN flood**

Typ útoku **DDoS**, zasílá záplavu **TCP/SYN** paketů s padělanou hlavičkou odesílatele. Každý takový paket je serverem přijat jako normální žádost o připojení. Server tedy odešle **TCP/SYN-ACK** packet a čeká na **TCP/ACK**. Ten ale nikdy nedorazí, protože hlavička odesílatele byla zfalšována. Takto polootevřená žádost nějakou dobu blokuje jiné, legitimní žádosti o připojení.

*Type of a **DDoS** attack, it sends a flood of **TCP/SYN** packets with a forged heading of the sender. Each such packet is accepted by the server as a normal request for a connection. Server then sends out a **TCP/SYN-ACK** packet and waits for **TCP/ACK**. This however never arrives as the user heading was forged. Thus a half-open request blocks, for some time, other legitimate requests for a connection.*

Zahlcení UDP **UDP flood**

Typ **DoS** útoku pomocí User datagram protocol (**UDP**). Útočník pošle nespecifikované množství UDP paketů na náhodný port systému oběti. Přijímací systém oběti není schopen určit, která aplikace si daný paket vyžádala, což vygeneruje ICMP paket nedoručitelnosti **UDP** paketu. Jestliže na přijímací port oběti přijde více UDP paketů, může dojít ke zkolabování systému.

*A type of an attack using the User datagram protocol (**UDP**). The attacker sends out an unspecified number of packets to a random port of the system of the victim. Receiving system of the victim is unable to determine which application requested such a packet, which generates an ICMP packet of undeliverabilty of the **UDP** packet. If more **UDP** packets arrive in the receiving port of the victim, the system may collapse.*

Zainteresovaná strana **Interested party**

Osoba nebo organizace, která může ovlivnit, může být ovlivněna nebo se může cítit být ovlivněna rozhodnutím nebo činností.

Person or organisation that can influence, be influenced by, or influenced by a decision or activity.

Zajišťovat pomocí vnějších zdrojů, (outsourcovat) **Outsource**

Učinit dohodu, že externí organizace bude vykonávat část funkce nebo procesu organizace.

Make an arrangement where an external organisation performs part of an organisation's function or process

Zákazník **Customer**

Organizace nebo část organizace, která přijímá službu nebo služby.

An organisation or its part receiving a service or services.

Základní prvky řízení **Baseline controls**

Minimální soubor ochranných opatření ustavených pro určitý systém nebo organizaci.

Minimal set of protective measures set for a certain system or organisation.

Základní vstupně-výstupní systém **Basic input output system (BIOS)**

Programové vybavení, které se používá při startu počítače pro inicializaci a konfiguraci připojených hardwarových zařízení a následnému spuštění operačního systému.

Software used during the startup of a computer for initialisation and configuration of connected hardware devices and subsequent start of the operating system.

Zálohovací procedura **Backup procedure**

Postup k zajištění rekonstrukce dat v případě selhání nebo havárie.

Procedure to enable data reconstruction in case of a failure or contingency.

Záložní soubor **Backup file**

Datový soubor, vytvořený za účelem pozdější možné rekonstrukce dat. Kopie dat uložená na jiném nosiči (nebo i místě). Záložní data jsou využívána v případě ztráty, poškození nebo jiné potřeby práce s daty uloženými v minulosti.

Data file created with the objective of possible future data reconstruction. Copies of data stored on another carrier (or even in a different place). Backup data are used in case of a loss, corruption or any other need to work with data stored in the past.

Záplata **Patch**

Aktualizace, která odstraňuje bezpečnostní problém nebo nestabilní chování aplikace, rozšiřuje její možnosti či zvyšuje její výkon.

Update which removes a security problem or unstable behaviour of an application, expands its possibilities and enhances its performance.

Zaplavení, zahlcení **Flooding**

Náhodné nebo záměrné vložení velkého objemu dat, jehož výsledkem je odmítnutí služby.

Accidental or intentional insertion of a large volume of data resulting in a service denial.

Zaručení, zajištění **Assurance**

Důvod pro oprávněné přesvědčení, že určitý požadavek bude nebo byl splněn.

Grounds for justified confidence that a claim has been or will be achieved.

Záruka totožnosti **Identity assurance**

Míra zaručení výsledku ověření totožnosti. Záruka totožnosti vyjadřuje úroveň důvěry v provedení, integritu a použitelnost informací o totožnosti včetně důvěry v údržbu informací o totožnosti.

Level of assurance in the result of identification. Identity assurance expresses the level of confidence in provenance, integrity and applicability of identity information including confidence in identity information maintenance.

Zařízení pro uchování důkazů **Evidence preservation facility**

Bezpečné prostředí nebo místo, kde jsou uloženy získané důkazy. Zařízení pro uchování důkazů by nemělo být vystaveno magnetickému poli, prachu, vibracím, vlhkosti ani jiným vlivům prostředí (jako jsou extrémní teploty a vzdušná vlhkost), které by mohli poškodit potenciální elektronické důkazy v něm uložené.

Secure environment or a location where acquired evidence is stored. An evidence preservation facility should not be exposed to magnetic fields, dust, vibration, moisture or any other environmental elements (such as extreme temperature or air humidity) that may damage the potential digital evidence within the facility.

Zásady ochrany soukromí **Privacy protection principles**

Soubor zásad určujících ochranu soukromí osobně identifikovatelných informací (PII) při jejich zpracování v systémech informačních a komunikačních technologií.

Set of principles governing the privacy protection of personally identifiable information (PII) when processed in information and communication technology systems.

Zašifrovaný klíč **Encrypted key**

Kryptografický klíč, který byl zašifrován schválenou bezpečnostní funkcí pomocí klíče k šifrování klíčů.

A cryptographic key that was encrypted using an approved security function with a key encryption key.

Zašifrovaný text, šifrovaný text **Encrypted text, Ciphertext**

Prostý text, který byl transformován za účelem ukrytí jeho informačního obsahu.

Plain text, which was transformed to hide its information content.

Zatížení klíče **Key loading**

Objem dat v bitech, který může být zašifrován jedním kryptografickým klíčem bez ohrožení bezpečnosti zašifrování.

A volume of data in bits which can be encrypted by one cryptographic key without compromising the security of encryption.

Závazná podniková pravidla (ochrany osobních údajů) **Binding corporate rules (of personal data protection)**

Koncepce ochrany osobních údajů, kterou dodržuje správce nebo zpracovatel usazený na území členského státu při jednorázových nebo souborných předáních osobních údajů správci nebo zpracovateli v jedné nebo více třetích zemích v rámci skupiny podniků nebo uskupení podniků vykonávajících společnou hospodářskou činnost.

Personal data protection policies which are adhered to by a controller or processor established on the territory of an (EU) member state for transfers or a set of transfers of personal data to a controller or processor in one or more third countries within a group of enterprises, or group of enterprises engaged in a joint economic activity.

Závislost **Dependency**

Takový vztah mezi komponenty, že je-li požadavek na závisející součást zahrnut do PP, ST balíčku, musí být odpovídající požadavek na součást, na které závisí, být rovněž zahrnut do PP, ST balíčku.

A relationship between components such that if a requirement based on the depending component is included in a PP, ST or package, a requirement based on the component that is depended upon must normally also be included in the PP, ST or package

Závod **Plant**

Soubor fyzických prvků nezbytných k realizaci určitého výrobního procesu, včetně množství statických dílů, které nejsou řízeny ICS. Nicméně činnost ICS může ovlivnit účelnost, výkonnost a trvanlivost součástí závodu.

The set of physical elements necessary to implement a particular production process, including many of the static components not controlled by the ICS. However, the operation of the ICS may impact the adequacy, strength, and durability of the plant's components.

Záznam auditních logů **Audit logging records**

Zaznamenávání údajů o bezpečnostnostních událostech týkajících se bezpečnosti informací za účelem jejich pozdějšího přezkoumání, analýzy a průběžného dohledu.

Recording of data on security events related toinformation security for the purpose of later re-examination, analysis and ongoing monitoring.

Zbytková data **Residual data**

Data zanechaná v datovém médiu po vymazání souboru nebo části souboru. Nemusí se však jednat pouze o data, která zbyla po mazání souborů na disku, nežádoucí zbytková data může zanechat na lokálním počítači například i práce pomocí vzdáleného připojení (***VPN***). Může se jednat například o nasbíraná (do cache) data aplikace.

*Data left behind in a data medium after the erasure of a file or part of it. It need not be, however, only data left after the erasure of disc files; unwanted residual data can be left on the local computer, for example, even by work using a remote connection (**VPN**). It could be data collected (into a cache), for example, of an application.*

Zbytkové riziko **Residual risk**

Riziko zbývající po zvládnutí (ošetření) rizika.

Risk remaining after risk management (treatment).

Zdroj hrozby **Threat Source**

Úmysl a postup cílený na úmyslné využití zranitelnosti, nebo situace či metoda, která může neúmyslně spustit zranitelnost.

The intent and method targeted at the intentional exploitation of a vulnerability or a situation or method that may accidentally trigger a vulnerability.

Zdroj rizika **Risk source**

Prvek, který sám nebo v kombinaci s jinými prvky má vnitřní potenciální schopnost způsobit riziko.

Element, which either alone or in combination with other elements, has the internal capability to cause a risk.

Zkreslení webových stránek **Defacement**

Průnik do webového serveru protivníka a nahrazení jeho internetových stránek obsahem, který vytvořil útočník. Zkreslení není skrytí, naopak, usiluje o medializaci a jeho psychologická síla spočívá jednak ve vyvolání pocitu ohrožení a nedůvěry ve vlastní informační systémy napadené strany, jednak v prezentaci ideologie či postojů útočníka.

Breaking into the web server of an adversary and replacing its internet pages by the content created by the attacker. Corruption is not hidden, quite the reverse, it

aims at medialization, and its psychological power rests on the one hand in creating a feeling of threat and mistrust in own information systems of the infected party, on the other hand in presenting the ideology or points of view of the attacker.

Zlovolná logika **Malicious logic**

Program, implementovaný v hardwaru, firmwaru nebo softwaru, jehož účelem je vykonat nějakou neautorizovanou nebo škodlivou akci (např. logická bomba, trojský kůň, virus, červ apod.).

Programme implemented in hardware, firmware or software whose purpose is to perform some unauthorised or harmful action (e.g. a logical bomb, Trojan horse, virus, worm, etc.).

Znalostní báze **Knowledge base**

Databáze obsahující inferenční pravidla a informace o zkušenostech a odborných znalostech v určité oblasti.

Database containing reference rules and information about the experience and professional knowledge in a certain area.

Znalostní testování **White box testing**

Testování, které zahrnuje zkoumání detailů implementace.

Testing which includes inspection of the implementation details.

Známá chyba **Known error**

Problém, který má určenu primární příčinu nebo je pomocí náhradního řešení stanovena metoda pro snížení či odstranění dopadů problému na službu.

Problem whose primary cause is known, or for which a method is established, to decrease or remove the impact of the problems on a service, using a substitute solution.

Zneužití **Exploit**

Popsaný způsob jak narušit bezpečnost informačního systému pomocí využití jeho známé zranitelnosti.

Defined way to breach the security of information systems through vulnerability.

Zneužití počítače **Computer abuse**

Záměrná nebo z nedbalosti plynoucí neautorizovaná činnost, která ovlivňuje počítačovou bezpečnost systému zpracování dat nebo je s ní spojena.

Unauthorised activity caused by intent or negligence which impacts computer security of a data processing system, or is related to it.

Zodolnění, hardening **Hardening**

Proces zabezpečení určitého systému zmenšením počtu využitelných zranitelností. Zodolnění zpravidla zahrnuje odstranění software, uživatelských účtů a služeb, které nejsou nezbytně nutné.

A process of securing a system by reducing its number of usable vulnerabilities. Hardening typically includes the removal of software, user accounts and services that are not essentially necessary.

Zodolněný operační systém **Hardened operating system**

Operační systém, který je záměrně nakonfigurován, nebo vyroben tak, aby bylo minimalizováno riziko narušení nebo útoku. Může jít o obecný OS (např. Linux), nebo o řešení vyvinuté na míru.

An operating system that is intentionally configured or designed to minimise the potential for compromise or attack. This may be a general OS, such as Linux or a bespoke solution.

Zombie **Zombie**

Infikovaný počítač, který je součástí sítě botnetů.

Infected computer, which is part of botnet networks.

Zpracování osobních údajů **Processing of personal data**

Jakákoliv operace nebo soubor operací s osobními údaji nebo soubory osobních údajů, který je prováděn pomocí či bez pomoci automatizovaných postupů, jako je shromáždění, zaznamenání, uspořádání, strukturování, uložení, přizpůsobení nebo pozměnění, vyhledání, nahlédnutí, použití, zpřístupnění přenosem, šíření nebo jakékoliv jiné zpřístupnění, seřazení či zkombinování, omezení, výmaz nebo zničení.

Any operation or set of operations on personal data or sets of personal data, whether or not performed by automated means, such as collection, recording,

organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Zpracování osobně identifikovatelných údajů **Processing of PII**

Operace nebo sada operací prováděná s osobně identifikovatelnými informacemi.

An operation or set of operations performed upon personally identifiable information (PII).

Zpracovatel osobních údajů **Processor of Personal Data**

Fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který zpracovává osobní údaje pro správce.

A natural or legal person, public administration body or another subject that processes personal data for the controller.

Zpracovatel PII **PII processor**

Strana zúčastněná na (ochraně) soukromí, která zpracovaná osobně identifikovatelné informace (PII) jménem a v souladu s instrukcemi správce PII.

Privacy stakeholder that processes personally identifiable information (PII) on behalf of and by the instructions of a PII controller.

Způsobilost **Proficiency**

Schopnost vyšetřovacího týmu dosáhnout stejně dobrých výsledků jako jiný investigativní tým na shodném zdroji potenciálních elektronických důkazů.

The ability of an investigative team to achieve results equivalent to those of a different investigative team given the same sources of potential digital evidence.

Zranitelnost **Vulnerability**

Slabé místo aktiva nebo opatření, které může být využito jednou nebo více hrozbami.

Weakness of an asset or control that can be exploited by one o more threats.

Zranitelnost CVE **CVE vulnerability**

Zranitelnost uvedená v seznamu **CVE** (Běžné chyby zabezpečení a ohrožení).

*Vulnerability listed in **CVE** (Common Vulnerabilities and Exposures).*

Ztráta **Loss**

Snížení hodnoty aktiva.

Reduction in the value of an asset.

Zveřejnění **Disclosure**

Viz **Prozrazení**.

*See **Disclosure**.*

Zvládání bezpečnostních incidentů **Security incident management**

Činnosti detekce, hlášení a posuzování bezpečnostních incidentů, odezvy na bezpečnostní incidenty, zacházení a poučení se z bezpečnostních incidentů.

Actions of detecting, reporting, assessing, responding to, dealing with, and learning from information security incidents.

Zvládání rizika, ošetření rizika **Risk treatment**

Proces vedoucí k modifikaci (změně) rizika.

Process to modify (change) risk.

Žádost o službu **Service request**

Žádost o informace, radu, přístup ke službě nebo o předem dohodnutou změnu.

Request for information, advice, access to service, or for a previously agreed change.

Žádost o změnu **Request for change**

Návrh na provedení změny služby, prvku služby nebo systému řízení služeb.

Proposal to make a change of a service, element of a service or a system of service control.

Životní cyklus **Life cycle**

Posloupnost vývojových stádií systému, produktu, služby nebo jiné entity vyvořené člověkem od jejího návrhu až po ukončení životnosti.

Evolution of a system, product, service, project or other human-made entity from conception through retirement.

Poznámky:

Anglicko – český slovník / English – Czech Glossary

Aborted connection **Předčasně ukončené spojení**

Connection terminated earlier, or in another way, than prescribed. It can often provide unauthorised access to unauthorised persons.

Acceptance criteria **Akceptační kritéria**

Criteria to be applied when performing the acceptance procedures (e.g. successful document review, or successful testing in the case of software, firmware or hardware).

Acceptance statement **Akceptační prohlášení**

Formal management declaration to assume responsibility for risk ownership, risk treatment and residual risk.

Access control **Řízení přístupu**

Means to ensure that access to assets is authorised and restricted based on business and security requirements.

Access control certificate **Certifikát řízení přístupu**

Security certificate containg information on access control.

Access control information (ACI) **Informace řízení přístupu**

Any information used for the purpose of access control including context information.

Access control list (ACL) **Seznam pro řízení přístupu**

List of permissions to grant access to an object (e.g. a disc file); it determines, who or what has the right to access the object and which operations it can do with it. In the security model using the ACL system, it searches ACL before performing any operation and looks up the corresponding record and by it makes a decision if the operation may be executed.

Access control policy **Politika řízení přístupu**

Set of principles and rules, which define conditions to provide access to a certain object.

Access level **Úroveň přístupu**

Level of authorisation required to access protected sources.

Access period **Období přístupu**

Time period during which access to a certain object is allowed.

Access permission **Povolení přístupu**

All access rights of a subject related to a certain object.

Access point / Wireless access point **Přístupový bod, Bezdrátový přístupový bod**

A device or piece of equipment that allows wireless devices to connect to a wired or optical network. The connection uses a wireless local area network (WLAN) or related standard.

Access right **Přístupové právo**

Permission for a subject to access a concrete object for a specific type of operation.

Access type **Typ přístupu**

In computer security, type of an operation specified by an access right.

Accountability **Odpovědnost**

A property that ensures that the actions of an entity can be traced uniquely back to the entity. The accountability follows from the obligation to perform activities and tasks given by current and past activities.

Accreditation **Akreditace**

The official management decision of a competent representative of an organisation, to authorise the operation of the information system and the explicit acceptance of risks (including the strategic, economic or reputational ones) which ensue to the organisation from the agreed security measures.

Accredited user **Autorizovaný uživatel**

User having certain right or permission to work in the information system and with the applications in accordance with defined access guidelines.

Active cyber defence **Aktivní kybernetická obrana**

(1) A set of measures to detect, analyse, identify and mitigate threats in and from the cyberspace, in real time, combined with the capability and resources to take proactive or attack action against threat agents in those agents˘ home networks. (2) Proactive measures to detect or obtain information about a cyber intrusion, cyber attack or an imminent cyber operation, or to find the source of an operation,

which includes launching a preemptive, preventive or counter-operation against the source.

Active threat **Aktivní hrozba**

Any threat of an intentional change in the state of a data processing system or computer network. Threat, which would result in messages modification, the inclusion of false messages, false representation, or service denial.

Actuator **Akční člen, aktuátor**

A device for moving or controlling a mechanism or system. It is operated by a source of energy, typically electric current, hydraulic fluid pressure, or pneumatic pressure, and converts that energy into motion. An actuator is a mechanism by which a control system acts upon an environment. The control system can be simple (a fixed mechanical or electronic system), software-based (e.g. a printer driver, robot control system), or a human or another agent.

Address resolution protocol (ARP) **Protokol ARP**

*Protocol defined in the document RFC 826 enables the translation of network addresses (**IP**) to hardware (**MAC**) addresses. ARP does not use authentication. Hence it cannot be misused for attacks, e.g. of the MITM type.*

Address space **Adresový (adresní) prostor**

*A continuous range of IP addresses. Address space is made up of a set of unique identifiers (**IP addresses**). In the **Internet** environment, **IANA** organisation is the administrator of the address range.*

Administrative / procedural security **Administrativní / procedurální bezpečnost**

Administrative measures to ensure computer security. These measures can be operational procedures or procedures related to responsibility, procedures for examining security incidents and revision of audit records.

Administrator **Administrátor**

The person responsible for the management of a part of a system (e.g. information system) for which he/she usually has the highest access privileges (supervisor rights).

Advanced persistent threat (APT) **Pokročilá a trvalá hrozba**

Typical purpose of APT is a long-term and persistent infiltration into, and abuse of, the target system using advanced and adaptive techniques (unlike usual single attacks).

Adverse actions **Nežádoucí jednání**

Actions performed by a threat agent on an asset.

Adware **Adware**

Advertising application which shows the user unsolicited advertising. Often it acquires information about behaviour. Note: the application may be installed without user knowledge or consent or may be pushed to the user under licencing conditions of other software.

Aggregation **Agregace**

Controlled loss or limitation of information or equipment, usually by aggregation, merge, or statistical methods.

Agreement **Dohoda**

Mutual acknowledgement of terms and conditions under which a working relationship is conducted.

Alarm **Alarm**

A device or function that signals the existence of an abnormal condition by making audible or visible signals. (2) In process control, an alarm means an event / condition that is dangerous for the process. These states are stored in the alarm system. The alarm must be confirmed (reset) after the occurrence. Otherwise, it still remains active in the Alarm System.

Alarm system **Alarm system**

System for alarms registering, saving and viewing.

Alert **Varování**

"Instant" indication that an information system and network may be under attack, or in danger because of accident, failure or human error.

Algorithm **Algoritmus**

Unambiguously defined mathematical process for the execution of a set of computational rules that, if followed, will give a prescribed result.

Anonymisation **Anonymizace**

The process by which personally identifiable information (PII) is irreversibly altered in a way that a PII principal can no longer be identified directly or indirectly, either by the PII controller alone or in collaboration with any other party.

Anonymity **Anonymita**

The specific characteristic of information that prevents to identify the subject concerned.

Anonymized data **Anonymizované údaje**

Data produced as the output of a personally identifiable information anonymisation process.

Anonymous login **Anonymní přihlášení**

Login into network and access to its resources without authentication of the party.

Antispam **Antispamový filtr**

Sophisticated software comparing each email with a number of defined rules and if the email satisfies a rule, counts in the weight of the rule. The weights can vary in value, positive and negative. When the total of weights exceeds a certain value, it is labelled as spam.

Anti-stealth technique **Anti-stealth technika**

*Ability of an **antivirus programme** to detect even stealth-viruses (sub-stealth-viruses) which are active in memory, for example by using direct disc reading bypassing the operating system.*

Antivirus **Antivir**

*See **Antivirus programme**.*

Antivirus programme **Antivirový program**

Single-purpose or multipurpose programme doing one or more of the following functions: searching for computer viruses (by a single or several different techniques, often with a possibility of their selection or setting mode for search – scanning, heuristic analysis, methods of checksums, monitoring of suspicious activities), healing of infected files, backup and recovery of system sectors on the disc, storing control information on files on disc, providing information on viruses, etc.

Application **Aplikace**

IT solution, including application software, application data and procedures, designed to support selected organisational processes or functions.

Application owner **Vlastník aplikace / Garant aplikace**

Organizational role responsible for the management, utilization and protection of the application and its data. Note: The application owner makes all decisions pertaining to the application's security.

Application Security Control (ASC) **Opatření aplikační bezpečnosti**

A data structure containing a precise enumeration and description of security activities and the associated verification measurement to be performed at a specific point in an application's life cycle.

Application Server **Aplikační server**

Software specialised for operating shared applications.

Application service provider **Poskytovatel aplikačních služeb**

Operator who provides a hosted software solution that provides application services which includes web based or client-server delivery models. Example: Online game operators, office application providers and online storage providers.

Application services **Aplikační služby**

Software whose functions are delivered to subscribers using an on-line model, which has a web or client-server application.

Assessor **Hodnotitel**

Person who leads and conducts a privacy impact assessment. Note: The assessor may be supported by one or more other internal and/or external experts as part of their team.

Asset **Aktivum**

Anything that has value to an individual, company or public administration.

Asset guarantor **Garant aktiva**

Security role defined in accordance with the law on cyber security and representing a natural person commissioned to develop, utilise and secure an asset. It is a role similar to that of the asset owner in a number of standards ISO/IEC 27 000.

Asset owner **Vlastník aktiva**

An individual or entity whom the organisation management has assigned the responsibility for production, development, maintenance, use and security of an asset.

Assets Manager (information system operator) **Správce aktiva (provozovatel informačního sytému)**

Individual (entity) who enables information processing or service providing and acts towards other natural and legal persons in the information system as the bearer of rights and obligations connected to operating the system.

Assets value **Hodnota majetku**

Objective expression of a generally perceived value or a subjective evaluation of the importance (criticality) of an asset, or a combination of both approaches.

Assurance **Zaručení, zajištění**

Grounds for justified confidence that a claim has been or will be achieved.

Asymmetric Algorithm **Asymetrický algoritmus**

*Encryption algorithm to implement **Asymmetric cryptography**.*

Asymmetric cryptography **Asymetrická kryptografie**

A group of cryptographic methods (sometimes known as public-key cryptography) where different keys are used for encrypting and decrypting – more precisely a pair of mathematically bound keys. The pair is made up of a public key and a private key. The first key is used as the encryption key, the second one as the decryption key. In addition to making the content of communication secret, asymmetric communication is also used for the electronic (digital) signature that gives the possibility to verify the author of data.

Attack **Útok**

Attempting to destroy, compromise, alter, disable, steal or gain unauthorised access to an asset or to make unauthorised use of an asset.

Attack potential **Útočný potenciál**

Measure of the attack effort to be expended in attacking a target, expressed in terms of an attacker's expertise, resources and motivation.

Attack surface **Attack surface**

Code within a computer system that can be run by unauthorized users.

Attack vector **Vektor útoku**

A path or means by which an attacker can gain access to a computer or network server to deliver a malicious outcome.

Attacker **Útočník**

A person deliberately exploiting vulnerabilities in technical and non-technical security controls in order to steal or compromise information systems and networks, or to compromise availability to legitimate users of the information systems.

Audit **Audit**

Systematic, independent and documented process for obtaining audit evidence and evaluating it objectively to determine the extent to which the audit criteria are fulfilled.

Audit event **Auditovaná událost**

Event detected by the system and resulting in triggering and recording the audit.

Audit logging **Auditní logování**

Recording of data on information security events for the purpose of review and analysis, and ongoing monitoring.

Audit logging records **Záznam auditních logů**

Recording of data on security events related toinformation security for the purpose of later re-examination, analysis and ongoing monitoring.

Audit scope **Předmět auditu**

Extent and boundaries of an audit.

Audit trail, audit log **Auditní záznam**

A chronological record of those system activities, which suffice for restoring, backtracking and evaluation of the sequence of states in the environment as well as activities related to operations and procedures from their inception to the final result.

Authentication **Ověření totožnosti**

Poskytnutí záruky, že udávaná charakteristika určité entity je správná.

Authentication exchange **Autentizační výměna**

Mechanism whose objective is to find out the identity of an entity (subject) by way of information exchange.

Authentication factor **Autentizační faktor**

A piece of information and/or process used to authenticate or verify the identity of an entity. Authentication factors are divided into four categories: 1) something an entity has (e.g., device signature, passport, hardware device containing a credential, private key); 2) something an entity knows (e.g., password, PIN); 3) something an entity is (e.g., biometric characteristic); or 4) something an entity typically does (e.g., behaviour pattern).

Authentication information **Informace o autentizaci**

Information used to establish validity of proclaimed identity of a given entity.

Authentication protocol **Autentizační protokol**

Defined sequence of messages between an entity and a verifier that enables the verifier to perform authentication of an entity.

Authenticity **Autentičnost**

Property that a certain entity is identical with what it claims to be.

Authorization **Autorizace**

Granting rights including granting access on the basis of access rights. Process of rights granting to a subject to perform defined activities in the information system.

Automated security incident measurement (ASIM) **Automatické monitorování výskytu bezpečnostního incidentu**

Automatic monitoring of network operations with the detection of non-authorised activities and undesirable events.

Availability **Dostupnost**

Property of being accessible and usable upon demand by an authorised entity.

Backdoor / trapdoor **Zadní vrátka**

*Hidden software or hardware mechanism usually created for testing and error removal, which can be used to bypass computer security. A method in a computer system or in an algorithm, which allows the attacker to bypass the normal user authentication at the access to a programme or system and simultaneously allows to have this access hidden from normal checks. A **firewall** can be bypassed, to penetrate the operating system, for example, by pretending to be a web browser. This code can assume the form of an independently installed programme, or it could be a modification of an existing system. The access to the system as such tends to have the form of a fictitious user name and password, which the attacked system accepts without checking and assigns to the user administrative rights.*

Backup file **Záložní soubor**

Data file created with the objective of possible future data reconstruction. Copies of data stored on another carrier (or even in a different place). Backup data are used in case of a loss, corruption or any other need to work with data stored in the past.

Backup procedure **Zálohovací procedura**

Procedure to enable data reconstruction in case of a failure or contingency.

Baiting **Využití návnady**

Mode of attack when the attacker leaves an infected CD, flash disc or another storage medium where the victim can find it with a high probability, e.g. in a lift, on the car park. This leaves curiosity to play out and sooner or later the victim inserts the medium into the computer. This results in virus installation with which the attacker gets access to the computer or the whole companywide computer network.

Baseline controls **Základní prvky řízení**

Minimal set of protective measures set for a certain system or organisation.

Basic input output system (BIOS) **Základní vstupně-výstupní systém**

Software used during the startup of a computer for initialisation and configuration of connected hardware devices and subsequent start of the operating system.

Batch Processing **Dávkové zpracování**

Running one or more programmes using scripts.

Batch viruses **Dávkové viry**

Computer viruses created using batch files. An interesting possibility for some operating systems (e.g. UNIX), exist however even for MS-DOS. They are not too widespread and are more of a rarity.

Best practice **Příklad dobré praxe, osvědčený způsob**

Well-tested method or procedure, which in the given area offers the most effective solution, which has been repeatedly proven as right and leads towards optimum results.

Binding corporate rules (of personal data protection) **Závazná podniková pravidla (ochrany osobních údajů)**

Personal data protection policies which are adhered to by a controller or processor established on the territory of an (EU) member state for transfers or a set of transfers of personal data to a controller or processor in one or more third countries within a group of enterprises, or group of enterprises engaged in a joint economic activity.

Biometric data **Biometrické údaje**

Personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or fingerprints.

Biometric system **Biometrický systém**

System for the purpose of the automated recognition of individuals based on their behavioural and physiological characteristics.

Biometrics **Biometrie**

Automatic recognition of a specific individual based on their behavioural or biological characteristics.

BitTorrent **BitTorrent**

*Tool for peer-to-peer (**P2P**) distribution of files, which spreads out the load of data transfers among all clients downloading data.*

Black box testing **Slepé testování**

Examining a process using known inputs and comparing the results against predicted outputs, which reflect the requirements for the process.

Black hat **Black hat**

*See **Cracker**.*

Blacklist **Černá listina**

A list of specific entities, such as hosts or applications that are known to be malign and are thus denied, rejected, or disregarded.

Blended attack **Kombinovaný útok**

Attack that seeks to maximize the severity of damage and speed of contagion by combining multiple attacking methods.

Block Cipher **Bloková šifra**

Symmetric encryption system with the property that the encryption algorithm operates on a block of plaintext, i.e. a string of bits of a defined length, to yield a block of ciphertext.

Bluetooth **Bluetooth**

Wireless technology standard for data transfer over short distances.

Bot **Bot (Robot)**

Within the framework of cyber criminality: programmes which take over computers in the network and use them for criminal activities – for example, distributed attacks (DDoS) and mass distribution of unsolicited commercial emails. Individual bots are the basis for large groups of robots known as botnets. Computer wholly or partially taken over by a bot is known as "zombie".

Bot Herder / Bot Wrangler **Původce botnetu**

(1) A cracker who controls a large number of compromised machines (robots, bots, zombies).
(2) The topmost computer in the botnet hierarchy controlling compromised computers of the given botnet.

Botnet **Síť botů**

Software for the remote control of bots, which run on infected computers. The software ensures that the cracker can access the computing power of many machines simultaneously. It allows for illegal activities on a large scale-in particular DDoS attacks and spam distribution.

Breach **Porušení, prolomení**

A breach or an abuse of information security or a breach of a security policy.

Breach of Data Protection **Porušení ochrany údajů**

A breach of security, intentional or unintentional that leads to the destruction, loss, alteration, unauthorised disclosure of, or access to, protected data during transmission or procession.

Bring Your Own Device (BYOD) **BYOD**

Refers to workers bringing their own mobile devices, such as smartphones, laptops and PDAs, into the workplace for use and connectivity.

Broadcast **Plošné visílání**

Transmission to all devices in a network without any acknowledgment by the receivers.

Brute force attack **Útok hrubou silou**

Method to find passwords when the attacking programme tries all existing character combinations for a possible password. This method is very time-consuming. Its success depends on password length and the computing power of the computer used.

BSD licence **BSD licence**

A family of permissive free software licenses, imposing minimal restrictions on the redistribution of covered software

Buffer Overflow **Přetečení zásobníku**

A condition at an interface under which more input can be placed into a buffer or data holding area than the capacity allocated, overwriting other information.

Adversaries exploit such conditions to crash a system or to insert a specially crafted code that allows them to gain control of the system.

Bug **Chyba**

A programming error, which causes a security problem in software. The attacker can utilise the bug to control the computer, make a running service dysfunctional or running improperly, to modify data and similar.

Building automation **Automatizace budov**

Central ventilation, temperature, humidity, lighting and other building control system. The reason is efficient energy management and simplification of maintenance. The building management system is a typical example of a DCS (Distributed Control System).

Business continuity **Kontinuita činností organizace**

Capability of the organisation to continue delivery of products or services at acceptable predefined levels following disruptive incident.

Business continuity management (BCM) **Řízení kontinuity organizace**

A holistic management process that identifies potential threats to an organisation and the impacts to business operations those threats, if realised, might cause, and which provides a framework for building organisational resilience with the capability of an effective response that safeguards the interests of its key stakeholders, reputation, brand and value-creating activities.

Business continuity management system (BCMS) **Systém řízení kontinuity organizace**

Part of the overall management system that establishes, implements, operates, monitors, reviews, maintains and improves business continuity.

Business continuity plan (BCP) **Plán kontinuity činností**

Documented procedures that guide organisations to respond, recover, resume, and restore to a pre-defined level of operation following disruption.

Business impact analysis (BIA) **Analýza dopadů na činnosti organizace**

Process of analysing operational functions and the effect that a disruption might have upon them.

Certificate **Certifikát**

Entity's data rendered unforgeable with the private or secret key of a certification authority. Note: Unforgeable means impossible to copy or imitate unlawfully.

Certification **Certifikace**

(1) Third-party attestation related to products, processes, systems or persons. (2) Proces for verification of the competence of communication and information systems for handling classified information, approval of such competence and issuance of a certificate.

Certification authority (CA) **Certifikační autorita**

In computer security, a third party which issues digital certificates and uses its authority to confirm the authenticity of data, which exist in the freely accessible part of the certificate.

Certification body **Certifikační orgán**

Third party which assesses and certifies a system, for example system for the control of computer security for a client organization, with regard to international standards and other documentation needed for a certified system.

Certification document **Certifikační dokument**

Document stating that any system of control, for example system for the control of information security, meets the required standard, and other documentation needed for a certified system.

Chain letter **Řetězový dopis**

Letter sent out to many recipients and containing information which each recipient has to pass on to many other addressees. It is a frequently used method of pressure ("If you do not send this letter to 25 other people, something terrible happens to you in 10 days").

Chain of custody **Řetězec péče (o důkazy)**

Demonstrable possession, movement, handling, and location of material (especially evidence) from one point in time until another.

Chat **Chat**

Way of direct (online) communication of several persons using the Internet.

Chief privacy officer (CPO) **Vedoucí pro ochranu osobních údajů**

Senior management individual who is accountable for the protection of personally identifiable information in an organization.

Clearing **Vyčištění**

the targeted overwriting or erasure of classified data on a data medium which has a special security classification and security category so that the given medium could be repeatedly used for a record in the same security classification and security category.

Closed-security environment **Uzavřené bezpečnostní prostředí**

Environment where special attention (by a form of authorisations, security checks, configuration control, etc.) is given to protection of data and sources from accidental or intentional actions.

Cloud computing **Cloud computing**

Mode of utilisation of computing technology whereby scalable and flexible IT functions are accessible to users as a service. The advantage of clouds: easy software upgrade, unsophisticated client stations and software, cheap access to a mighty computing power without hardware investments, guaranteed availability. Disadvantages: confidential data are available also to the cloud provider.

Common Criteria **Společná kriteria**

The Common Criteria for Information Technology Security Evaluation (abbreviated as Common Criteria or CC) is an international standard (ISO/IEC 15408) for computer security certification. It is currently in version 3.1 revision 4. Common Criteria is a framework in which computer system users can specify their security functional and assurance requirements (SFRs and SARs respectively) through the use of Protection Profiles (PPs), vendors can then implement and/or make claims about the security attributes of their products, and testing laboratories can evaluate the products to determine if they actually meet the claims. In other words, Common Criteria assures that the process of specification, implementation and evaluation of a computer security product has been conducted in a rigorous and standard and repeatable manner at a level that is commensurate with the target environment for use.

Communication security (COMSEC) **Bezpečnost komunikací**

Use of such security measures in communications which prohibit unauthorised persons from obtaining information which could be gained from access to communication traffic and its evaluation, or which ensure the authenticity of the communication process. Computer security as applied to data communications – data transfer.

Communication system **Komunikační systém**

System, which provides for the transfer of information among end users. It includes end communication devices, transfer environment, system administration, handling by personnel and operational conditions and procedures. It may also include means of cryptographic protection.

Competence **Odborná způsobilost**

Ability to apply knowledge and skills to achieve intended results.

Completely automated public Turing test to tell computers from humans apart (CAPTCHA) **CAPTCHA**

Turing test used on the web to automatically differentiate real users from robots, for example, when entering comments, at registration, etc. The test usually consists of an image with a deformed text and the task for the user is to rewrite the pictured text into the entry field. It is assumed that the human brain can properly recognise even corrupted text, but an internet robot using OCR technology cannot do. The disadvantage of the image CAPTCHA is its unavailability for users with visual impairment; hence usually there is the option of having the letters from the image read aloud.

Compromising **Kompromitace**

Compromise of information security, which may result in programme or data modification, their destruction, or their availabilty to unauthorised entities.

Computer abuse **Zneužití počítače**

Unauthorised activity caused by intent or negligence which impacts computer security of a data processing system, or is related to it.

Computer crime / Cyber crime **Počítačová kriminalita / Kybernetická kriminalita**

Crime committed using a data processing system or computer network or directly related to them.

Computer emergency response team (CERT) **Skupina pro reakci na kybernetické hrozby**

*CERT is another name for **CSIRT**; unlike **CSIRT**, CERT is a registered trademark. See **CSIRT**.*

Computer fraud **Počítačový podvod**

Fraud committed using a data processing system or computer network or directly related to them.

Computer incident response capability (CIRC) **Schopnost reagovat na počítačové hrozby**

A cyber defence capability, which ensures fast and effective reaction to risks and vulnerabilities in systems; provides methodology for reporting and managing incidents; provides support and help to the operational and security managements of systems. It is part of the emergency (crisis) planning for system recovery.

Computer network **Počítačová síť**

A collection of computers together with a communication infrastructure (communication lines, hardware, software and configuration data) through which they (computers) can send and share data with each other.

Computer network attack (CNA) **Útok na počítačovou síť**

Activity done to corrupt, block, degrade or destroy information stored in a computer or on a computer network, or the computer or computer network as such. The attack on a computer network is a certain sort of cyber attack.

Computer network exploitation (CNE) **Vytěžování počítačové sítě**

Abuse of information stored on the computer or computer network.

Computer security (COMPUSEC) **Počítačová bezpečnost**

Branch of informatics dealing with securing of information in computers (discovering and lowering risks connected to the use of the computer). Computer security includes:
(1) enabling protection against unauthorised manipulation with the devices of a computer system,
(2) protection against unauthorised data manipulation,
(3) protection of information against pilferage (illegal creation of data copies),
(4) secure communication and data transfer (cryptography),
(5) secure data storage,
(6) availability, integrity and authenticity of data.
It is also the introduction of security properties of hardware, firmware and software into the computer system so that it is protected against unauthorised disclosure, amendments, changes or erasure of facts or to prevent these, or against access denial — protection of data and sources against accidental or harmful activities.

Computer security audit **Audit počítačové bezpečnosti**

Independent verification of measures of implementation and their efficiency with the view of attaining computer security.

Computer security incident response team (CSIRT) **Skupina pro reakci na kybernetické bezpečnostní incidenty**

A team of experts to support the handling of cyber security incidents. CSIRT provides its clients with the necessary services for solutions to incidents and helps them in recovering the system after a disruption. To minimise incident risks and minimise their number, CSIRT offices also provide preventive and educational services. For clients, they provide information on detected weaknesses of used hardware and software instruments and about possible attacks, which make use of these weaknesses so that the clients may quickly address these weaknesses

Computer system audit **Audit počítačového systému**

Analysis of procedures used in data processing in order to evaluate their efficiency and correctness, and to recommend improvements.

Computer virus **Počítačový virus**

A computer programme, which replicates itself by attaching its copies to other programmes. It may contain a part which activates it when certain conditions are met (e.g. time) in the host device. It is distributed using the Internet (electronic mail, downloading programmes from unreliable sources), using mobile storage media and others. This is done to obtain various types of data, for identity theft, for putting the computer out of operation, etc.

Computer, personal computer (PC) **Osobní počítač**

In accordance with the wording of CSN 36 9001 this is "a data processing machine executing independent sequences of various arithmetic and logical operations." In other words: a machine characterised by processing data according to a previously created programme stored in its memory.

Confidential information **Důvěrná informace**

Information that should not be made available or disclosed to unauthorized individuals, entities or processes.

Confidentiality **Důvěrnost**

Property that information is not made available or disclosed to unauthorised individuals, entities or processes.

Configuration (of a system or device) **Konfigurace (systému nebo zařízení)**

Step in system design; for example, selecting functional units, assigning their locations, and defining their interconnections.

Configuration baseline **Výchozí stav konfigurace**

Configuration information formally related to a certain time in the lifetime of a service, or element of the service.

Configuration Control **Řízení konfigurace**

Process for controlling modifications to hardware, firmware, software, and documentation to ensure the information system is protected against improper modifications before, during, and after system implementation.

Configuration item (CI) **Konfigurační položka**

Element, which must be controlled in order to deliver a service or services.

Configuration management database (CMDB) **Konfigurační databáze**

Data warehouse used for records of configuration items' attributes and relations among configuration items during their whole life cycle.

Conformity **Shoda**

Fulfilment of a requirement.

Consent of the data subject **Souhlas subjektu údajů**

Any freely given, specific, informed and unambiguous indication of the data subject's will by which they, by a statement or by a clear affirmative action, signify agreement to the processing of their data.

Consequence **Následek**

Outcome of an event affecting objectives.

Contamination **Kontaminace**

Input of data with a certain security classification or security category into a wrong security category.

Contingency plan **Havarijní plán**

Plan for backup procedures, response to an unforeseen event and recovery after a contingency.

Contingency procedure **Havarijní postup**

Procedure, which is an alternative to the normal procedure in case of an occurrence of an unusual but assumed situation.

Continual improvement **Neustálé zlepšování**

Recurring activity to enhance performance.

Continuous Process **Průběžný proces**

A process that operates on the basis of a continuous flow, as opposed to batch, intermittent, or sequenced operations.

Control **Opatření**

A measure that is modifying risk, including all policies, strategies, procedures, directives, usual procedures (practices) or organisational structures, which may be of an administrative, technological, management or legal character.

Control **Řídící prvek**

The part of the ICS used to perform the monitoring, control and regulation of the physical process. This includes all control servers, field devices, actuators, sensors, and their supporting communication systems.

Control Algorithm **Řídicí algoritmus**

A mathematical representation of a control action.

Control Centre **Řídicí středisko**

An equipment structure or group of structures from which a process is measured, controlled, and monitored.

Control Loop **Řídicí smyčka**

A control loop consists of sensors for measurement, controller hardware such as PLCs, actuators such as control valves, breakers, switches and motors, and the communication of variables. Controlled variables are transmitted to the controller from the sensors. The controller interprets the signals and generates corresponding manipulated variables, based on set points, which it transmits to the actuators. Process changes from disturbances result in new sensor signals, identifying the state of the process, to again be transmitted to the controller.

Control Network **Řídicí síť**

A network that connects the supervisory control level to lower-level control modules and typically connects equipment that controls physical processes and that is time or safety critical. The control network can be subdivided into zones, and there can be multiple separate control networks within one enterprise and site.

Control objective **Cíle opatření**

Statement describing what is to be achieved as a result of implementing controls.

Control Objectives for Information and Related Technology (COBIT) **COBIT**

Control Objectives for Information and Related Technology (COBIT) is a framework created by ISACA for information technology (IT) management and IT governance. It is a supporting toolset that allows managers to bridge the gap between control requirements, technical issues and business risks.

Control Server **Řídicí server**

A controller that also acts as a server that hosts the control software that communicates with lower-level control devices, such as Remote Terminal Units (RTUs) and Programmable Logic Controllers (PLCs), over an ICS network. In a SCADA system, this is often called a SCADA server, MTU, or supervisory controller.

Control System **Řídicí systém**

A system in which deliberate guidance or manipulation is used to achieve a prescribed value for a variable. Control systems include SCADA, DCS, PLCs and other types of industrial measurement and control systems.

Controlled access system (CAS) **Systém řízeného přístupu**

Means for automating of the physical control of access (e.g. use of badges equipped with magnetic strips, smart cards, biometric sensors).

Controlled Variable **Řízená proměnná**

The variable that the control system attempts to keep at the set point value. The set point may be constant or variable.

Controller **Řídicí jednotka**

A device or programme that automatically regulates a controlled variable.

Controller (of personal data) **Správce osobních údajů**

A natural or legal person, public authority, agency or another body, which alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

Controller of personally identifiable information (data) PII **Správce osobně identifikovantelných informací (údajů) PII**

A natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

Cookie / HTTP cookie **Cookie / HTTP cookie**

Data exchanged between an HTTP server and a browser to store state information on the client side and retrieve it later for HTTP server use. A cookie is at present mostly used for the recognition of a user who visited the application before, or for storing user setting of the web application. Nowadays, discussions are underway about cookies in connection to watching the movements and habits of users by some webs.

Copy protection **Ochrana před kopírováním**

Use of a special technique for the detection or prevention of unauthorised copying of data, software and firmware.

Core network **Páteřní síť**

The central part of a telecommunication network that provides various services to customers who are connected by the access network.

Corporate information security policy **Strategie bezpečnosti informací společnosti**

Document that describes management direction and support for information security in accordance with business requirements and relevant laws and regulations.

Correction **Náprava**

Action to eliminate a detected nonconformity.

Corrective action **Nápravné opatření**

Action to eliminate the cause of a noncompliance and prevent recurrence.

Countermeasure **Protiopatření**

Activity, equipment, procedure, technology intended to minimise vulnerability.

Covert Channel **Skrytý kanál**

A transmission channel that could be used for data transfer in a way impairing security policy.

Crack **Crack**

Unauthorised infringement of programme or system security protection, its integrity or system of its registration/activation.

Cracker **Prolamovač**

An individual trying to obtain an unauthorised access to a computer system. These individuals are often harmful and possess means for breaking into a system.

CRAMM **CRAMM**

CRAMM (CCTA Risk Analysis and Management Method) is a risk management methodology, currently on its fifth version, CRAMM Version 5.0. CRAMM comprises three stages, each supported by objective questionnaires and guidelines. The first two stages identify and analyse the risks to the system. The third stage recommends how these risks should be managed.

Creative commons (CC) **Creative commons**

A non-profit organisation headquartered in Mountain View, California, United States devoted to expanding the range of creative works available for others to

build upon legally and to share. The organisation has released several copyrights – licenses known as Creative Commons licenses free of charge to the public

Credential issuer **Vydavatel autorizačních údajů**

Entity responsible for provisioning of a credential to a principal in a specific domain.
Note 1 to entry: A credential provisioned by a credential issuer can have a physical form, e.g. a membership (smart) card.
Note 2 to entry: The issuance of a credential for a principal can be recorded as an attribute for the principal, e.g. by recording the unique number of the token issued.
Note 3 to entry: A credential provisioned by an issuer can be a username and password. A credential in the form of a smart card or similar security device, can be configured to validate a password off-line.

Credential service provider (CSP) **Poskytovatel služby autorizačních údajů**

Trusted entity related to a particular domain responsible for management of credentials issued in that domain.

Credentials **Autorizační údaje**

Data transferred in order to establish proclaimed identity of a given entity, credentials.

Crisis **Krize**

A situation where the equilibrium among the basic components of the system on the one hand, and approach of the environment on the other hand, is disrupted seriously.

Crisis / Emergency situation **Krizová situace**

The emergency as per the law on an integrated emergency system, compromise of the critical infrastructure, or any other danger when a state of hazard, state of emergency, or threat to the state is announced (henceforth only "emergency").

Crisis management **Krizové řízení**

Collection of management activities of the bodies of crisis management aimed at the analysis and evaluation of security risks and planning, organisation, implementation and verification of activities conducted in connection with preparation for crises and their solution or protection of critical infrastructure.

Crisis measure **Krizové opatření**

Organisational or technical measure to solve a crisis situation and remedy its consequences, including measures interfering with the rights and obligations of people.

Crisis plan **Krizový plán**

Aggregate planning document elaborated by entities set forth by law and which contains a set of measures and procedures to solve crises.

Crisis planning **Krizové plánování**

The activity of the relevant bodies of crisis management aimed at minimising (prevention of) the origin of crises. Searching for the most suitable ways of anti-crisis intervention, optimisation of methods and forms to handle these unwanted phenomena (that is, reduction of the impacts of crises) and establishing the most rational and economical ways of recovery for the affected systems and their return into the normal daily state.

Crisis preparedness **Krizová připravenost**

Preparation of measures to solve own crisis situations and partially participate in solving crisis situations in the neighbourhood.

Crisis state **Krizový stav**

The legislative measure announced by the Parliament of the Czech Republic (threat to the state, and the state of war), by the Government of the Czech Republic (state of emergency) or governor of the region/mayor (state of danger), to solve a crisis.

Critical asset **Kritické aktivum**

Asset which can have a direct impact on production or generation, transmission, storage and distribution of electric power, gas, oil and heat.

Critical communication infrastructure (of the state) **Kritická komunikační infrastruktura (státu)**

The complex of communication systems, services or networks (meeting the defined criteria across and inside the branches of cyber security) whose dysfunctionality would result in a serious impact on state security, provision of the basic daily needs of the population, public health or the economy of the state.

Critical information infrastructure **Kritická informační infrastruktura**

The complex of information and communication systems (meeting the defined criteria across and inside the branches of cyber security) whose dysfunctionality would result in a serious impact on state security, provision of the basic daily needs of the population, public health or the economy of state.

Critical infrastructure **Kritická infrastruktura**

Systems and services whose dysfunctionality or wrong functionality would result in a serious impact on state security, its economy, public administration and in the end on the provision of the basic daily needs of the population.

Critical infrastructure protection **Ochrana kritické infrastruktury**

Measures aimed at lowering the risk of corruption of an element of the critical infrastructure.

Cross-section criteria **Průřezová kritéria**

A set of viewpoints to assess how serious is the corruption of an element in the critical infrastructure with bounds that include the scope of life losses, impact on the health of people, extraordinary serious economic impact or impact on the public due to an extensive limitation of providing the necessary services or any other serious intervention into the daily life.

Cross-site scripting (XSS) **Cross-site scripting**

The attack on web applications consisting in an attempt to find a security error in the application and using this for the insertion of own code. The inserted code usually tries to get personal data of users, the content of the database or to bypass the security elements of an application.

Cryptanalytic attack **Kryptografický útok**

Attack against a cipher that makes use of properties of the cipher.

Crypto Ignition Key (CIK) **Kryptografický iniciační klíč**

Physical (usually electronic) token to store keys, intended for the storing, transport and protection of cryptographic keys and initialising data. It contains part of key material without which the encryption device cannot encrypt and decrypt data. A cryptographic device without the inserted CIK does not contain open cryptographic keys nor other secret data.

Crypto officer **Správce kryptografie**

Role taken by an individual or a process (i.e. subject) acting on behalf of an individual that accesses a cryptographic module in order to perform cryptographic initialisation or management functions of a cryptographic module.

Cryptographic algorithm **Kryptografický algoritmus**

A well-defined computational procedure that takes variable inputs, which may include cryptographic keys, and produces an output. It is usually used for data encryption or decryption.

Cryptographic device **Kryptografický prostředek**

Cryptographic device (encryptor) is a hardware and software device using mathematical methods and procedures together with cryptographic algorithms and cryptographic keys, in order to transform (encrypt and decrypt) data. The

encryption function is the dominant one for this device. The encryption/decryption function can be implemented also by a cryptographic (HW and SW) module which may be part of another device.

Cryptographic key **Kryptografický klíč**

Sequence of symbols that controls the operation of a cryptographic transformation. The cryptographic key can contain, in addition to a random sequence of data, other data to ensure the integrity, time of validity, name and number of key.

Cryptographic protocol **Kryptografický protokol**

Protocol which performs a security-related function using cryptography.

Cryptography **Kryptografie**

Science of cryptography – a discipline covering the principles, means and methods to transform data in order to conceal their semantic content, to prevent an unauthorised use or prevent unrecognised modification.

Customer **Zákazník**

An organisation or its part receiving a service or services.

CVE vulnerability **Zranitelnost CVE**

*Vulnerability listed in **CVE** (Common Vulnerabilities and Exposures).*

Cyber attack **Kybernetický útok**

Attack on IT infrastructure having the objective of causing damage and obtaining sensitive or strategically important information. It is used most often in the context of either politically or militarily motivated attacks.

Cyber counterattack **Kybernetický protiútok**

Attack on IT infrastructure as a response to a previous cyber attack. It is used most often in the context of either politically or militarily motivated attacks.

Cyber crime **Kybernetická kriminalita**

A criminal activity where services or applications in the cyberspace are used for or are the target of a crime, or where the cyberspace is the source, tool, target, or place of a crime.

Cyber defence **Kybernetická obrana**

Defence against a cyber attack and mitigation of its consequences. Also, resistance of the subject towards an attack and a capability to defend itself effectively.

Cyber espionage **Kybernetická špionáž**

Obtaining strategically sensitive or strategically important information from individuals or organisations by using or targetting IT means. It is used most often in the context of obtaining political, economic or military supremacy.

Cyber harassment **Počítačové obtěžování**

Internet harassment (even an individual case) usually of an obscene or vulgar character. It is often part of cyberstalking. See also ***Cyberstalking****.*

Cyber operations **Kybernetická operace**

The employment of cyber capabilities or cyberspace with the primary purpose of achieving objective.

Cyber protection **Kybernetická ochrana**

The condition of being protected against physical, social, spiritual, financial, political, emotional, occupational, psychological, educational or other types or consequences of failure, damage, error, accidents, harm or any other event in the cyberspace which could be considered non-desirable.

Cyber security **Kybernetická bezpečnost**

(1) Collection of legal, organisational, technological and educational means aimed at protecting cyberspace.
(2) Preservation of confidentiality, integrity and availability of information in the cyberspace.

Cyber Security Designer **Architekt kybernetické bezpečnosti**

Defined security role by the law on cyber security and representing the individual who provides for the design and implementation of security measures, having the expertise for such an activity and who can prove such a capability in practice.

Cyber security management committee **Výbor pro řízení kybernetické bezpečnosti**

A defined security role in accordance with the Cyber Security Act, representing an organised group consisting of persons who are entrusted with the overall management and development of systems covered by the Cyber Security Act, or are significantly involved in the management and coordination of activities related to the cyber security of these systems.

Cyber strategy **Kybernetická strategie**

The general approach to the development and use of capabilities to operate in cyberspace, integrated and coordinated with other areas of operation, to achieve or support the set objectives by using identified means, methods and instruments in a certain timetable.

Cyber terrorism **Kyberterorismus**

Criminal activity done using or targeting primarily IT means with the objective of creating fear or inadequate response. It is used most often in the context of attacks having an extremist, nationalistic or politically motivated character.

Cyber threat **Kybernetická hrozba**

Potential cause of an unwanted cybersecurity incident, which can result in harm to a system, people, society, organization, or other entities in cyberspace.

Cyber war, Cyber warfare **Kybernetická válka**

Use of computers and the Internet to wage a war in cyberspace. System of extensive, often politically or strategically motivated, related and mutually provoked organized cyber attacks and counterattacks.

Cyberbullying **Počítačová / Kybernetická šikana**

Type of bullying using electronic means such as mobile phones, emails, pagers, internet, blogs and similar for sending harassing, offending or attacking emails and text messages, the creation of pages and blogs defaming selected individuals or groups of people.

Cybergrooming (Child grooming) **Kybergrooming (Child grooming)**

The behaviour of users of internet communication instruments (chat, ICQ, et al.) who try to get the trust of a child to either abuse the child (especially sexually) or misuse the child for illegal activity.

Cyber-incident **Kybernetický incident**

Cyber-event that involves a loss of information security or impacts business operations.

Cyber-insurance **Kybernetické pojištění**

Insurance that covers or reduces financial loss to the insured caused by a cyber-incident.

Cybernetics **Kybernetika**

The science dealing with general principles of information management and transmission in machines, living organisms and communities. It uses mainly the apparatus of mathematics in its specifications. It is based on the knowledge that some processes in the living organisms are described by the same equations as analogue processes in technological devices.

Cyber-risk **Kybernetické riziko**

Risk caused by a cyber-threat.

Cyberspace **Kybernetický prostor**

Digital environment enabling the origin, processing and exchange of information, made up of information systems and the services and networks of electronic communications.

Cybersquatting **Doménové pirátství**

Registration of the domain name related to the name or trademark of another company, with the purpose of subsequent offering the domain to this company at a high financial amount.

Cyberstalking **Kyberstalking**

Various kinds of stalking and harassment using electronic media (especially using emails and social networks), the objective being for example to instil a feeling of fear in the victim. The culprit obtains information about the victim most often from web pages, forums, or other mass communication tools. Often such activity is merely an intermediate step to a criminal act which may include a substantial limitation of human rights of the victim, or misuse the behaviour of the victim to steal, defraud, blackmail, etc.

Cycle Time, period time **Doba cyklu, čas cyklu**

Time, usually in seconds, in which the control unit completes one control loop (reading sensor data to memory, evaluation of control algorithms, the output of control signals to actuators, process regulation, the input of new signals from sensors).

Czech cyberspace **Český kyberprostor**

Cyberspace under the jurisdiction of the Czech Republic.

DarkWeb **DarkWeb**

An overlay network that uses the Internet but requires specific software (e.g. TOR browser, Freenet, I2P anonymous network, etc.), configurations, or authorization.

Data **Údaje**

*From the **ICT** point of view, this is a representation of information in a formalised way suitable for communication, explanation and processing.*

Data authentication **Autentizace dat / Ověření totožnosti dat**

Process used to verify data integrity (verification that received and sent data are identical, verification that programme is not infected by a virus, for example).

Data breach **Narušení dat**

Compromise of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to protected data transmitted, stored or otherwise processed.

Data centre **Datové centrum**

A data center is a facility used to house computer systems and associated components, such as telecommunications and storage systems. It generally includes redundant or backup power supplies, redundant data communications connections, environmental controls (e.g., air conditioning, fire suppression) and various security devices.

Data concerning health **Údaje o zdravotním stavu**

Personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status.

Data corruption **Poškození dat**

Accidental or intentional corruption of data integrity.

Data diode **Datová dioda**

Data diode is a device to provide for automatic unidirectional communication in critical systems. Data diode allows transfer of data from a system with lower security to a system with higher security.

Data Encryption Standard (DES) **DES**

*Data Encryption Standard is a symmetric block enciphering algorithm. It is a publicly available standard with key length of 56 bits. See also **3DES** for more.*

Data Historian **Historian**

A centralized database with the support of data analysis using statistical procedures to analyse processes.

Data integrity **Integrita dat**

Assurance that data were not changed. In the figurative sense denotes also the validity, consistency and accuracy of data, e.g. databases or file systems. It tends to be implemented by checksums, hash functions, self-correcting codes, redundancy, journalling, etc. In cryptography and information security in general, integrity means data validity.

Data protection **Ochrana dat**

Administrative, technological, procedural, staffing or physical measures implemented in order to protect data against an unauthorised access or against corruption of data integrity.

Data reconstruction **Rekonstrukce dat**

Method of data reconstruction by analysing the original sources.

Data restoration/ Data recovery **Obnova dat**

The act of re-creation, or reacquisition, of data lost, or whose integrity was compromised. Methods include copying from an archive, restoration of data from source data, or repeated establishment of data from alternative sources.

Data security **Bezpečnost dat**

Computer security applied to data. Includes for example control of access, definition of policies and processes and ensuring data integrity.

Data validation **Validace dat**

The process used to determine if data are accurate, complete, or satisfy specified criteria. Data validation may contain checks of format, checks for completeness, control key tests, logical and limit checks.

Database **Databáze**

Set of data arranged by a notional structure, which describes properties of these data and relations among corresponding entities, serves one or more application areas.

Dataset **Množina dat, sada dat**

Collection of data.

DC Servo Driver **Ovladač DC Serva**

A driver that works specifically for direct-current servo motors. It transmits commands to the motor and receives feedback from the servo motor resolver or encoder.

Decryption, deciphering **Dešifrování, rozšifrování**

Reverse process to encryption.

Deep packet inspection (DPI) **Podrobná inspekce paketů**

A form of computer network packet filtering that examines the data part (and possibly also the header) of a packet as it passes an inspection point, searching for protocol non-compliance, viruses, spam, intrusions, or defined criteria to

decide whether the packet may pass or if it needs to be routed to a different destination, or, for collecting statistical information.

Defacement **Zkreslení webových stránek**

Breaking into the web server of an adversary and replacing its internet pages by the content created by the attacker. Corruption is not hidden, quite the reverse, it aims at medialization, and its psychological power rests on the one hand in creating a feeling of threat and mistrust in own information systems of the infected party, on the other hand in presenting the ideology or points of view of the attacker.

Defence infrastructure **Obranná infrastruktura**

Set of objects, buildings, ground plots and equipment including necessary services, production and non-production systems needed to ensure their operation, regardless of the form of ownership and the way of utilisation; whose destruction, damage or limitation of activity would, under situation of threat to the state or a state of war, put in danger fulfilment of tasks: (1) of Armed Forces of the Czech Republic (CZE) during the implementation of the Plan of defence of CZE as well as operational plans including plans for mobilisation, (2) of experts during implementation of their partial plans of defence and other elements of security system of CZE, (3) of allied armed forces during the implementation of their operational plans, (4) of protection of population.

Demilitarized zone (DMZ) **Demilitarizovaná zóna**

Perimeter network (also known as a screened sub-net) inserted as a "neutral zone" between networks. DMZ concentrates services provided to someone in the neighbourhood or the whole internet. These external (public) services are usually the easiest target of an internet attack; a successful attacker however only gets to DMZ, not straight into the internal network of the organisation.

Denial of service (DoS) **Odmítnutí služby**

Denial of service is the technique of attack by many coordinated attackers on the internet services or pages resulting in flooding by requests and breakdown or unfunctionality or unavailability of the system for other users.

Dependency **Závislost**

A relationship between components such that if a requirement based on the depending component is included in a PP, ST or package, a requirement based on the component that is depended upon must normally also be included in the PP, ST or package

Diagnostic information **Diagnostická informace**

Information concerning known failure modes and their characteristics. Such information can be used in troubleshooting and failure analysis to help pinpoint the cause of a failure and help define suitable corrective measures.

Dialler **Dialer**

The harmful programme which connects the computer or smartphone of the user to the Internet by a commuted line using a very expensive service provider (usually of the attacker).

Dictionary attack **Slovníkový útok**

Attack on a system that employs a search of a given list of passwords. This is a relatively fast method, depending on the size of the dictionary and whether the victim uses a password that may be detected using the dictionary.

Digest **Otisk**

Result of a hash operation.

Digital device **Digitální zařízení**

Electronic equipment used to process or store digital data.

Digital evidence **Digitální důkaz**

Information or data, stored or transmitted in binary form which has been determined, through the process of analysis, to be relevant to the investigation. Note: This should not be confused with legal digital evidence or potential digital evidence.

Digital signature **Digitální podpis**

An electronic signature is inseparably linked cryptographically to the message so that it makes it possible to verify the identity of the author and the message integrity and thus protect the message against forgery by, say, the recipient. A digital signature is often used by asymmetric cryptography (the signature is created using a private key of the author and is verified by the public key of the author).

Directory service **Adresářová služba**

A service to search and retrieve information from a catalogue of well-defined objects, which may contain information about certificates, telephone numbers, access conditions, addresses, etc.

Disaster recovery plan / Contingency plan **Plán obnovy / Havarijní plán**

Plan for backup procedures, response to an unforeseen event and recovery after a disaster.

Disclosure **Odhalení / Prozrazení**

In IT context it is usually used for the expression of the fact that data, information or mechanisms were disclosed which should be hidden on the basis of policies and technical measures.

Discrete Processing **Diskrétní (nespojité) zpracování**

A type of procesings where a specified quantity of material moves as an independent unit (part of group of parts) among workplaces and each unit maintains its unique identity.

Disruption **Narušení**

An incident, whether anticipated or a random unanticipated or an attack on ICT infrastructure, which disrupts the normal course of operations at a specific location.

Distributed computing environment (DCE) **Distribuované výpočetní prostředí**

A software system developed in the early 1990s by a consortium that included Apollo Computer (later part of Hewlett-Packard), IBM, Digital Equipment Corporation, and others. The DCE supplies a framework and toolkit for developing client/server applications.

Distributed Control System (DCS) **Distribuovaný řídicí systém**

A control system whose control units are placed in several locations and jointly influence a specific process.

Distributed denial of service (DDoS) **Distribuované odmítnutí služby**

Distributed denial of service is the technique of attack by many coordinated attackers on the internet services or pages resulting in flooding by requests or breakdown or unfunctionality or unavailability of the system for other users.

Distributed manufacturing **Distribuovaná výroba**

A geographically separate plant that is accessible through the Internet to a specific enterprise.

Disturbance **Rušení**

An undesired change in an input variable being applied to a system that tends to adversely affect the value of a controlled variable.

Documented information **Dokumentovaná informace**

Information required to be controlled and maintained by an organisation and the medium on which it is contained.

Domain **Doména**

(1) Set of entities operating under a single security policy, e.g. public key certificates created by a single authority or by a set of authorities using the same security policy.
(2) An environment or context that includes a set of system resources and a set of system entities that have the right to access the resources as defined by a common security policy, security model, or security architecture.

Domain name **Doménové jméno**

Name to identify a computer, equipment or service in the network (including the Internet). Example of a domain name: www.afcea.cz.

Domain name registry **Registr doménových jmen**

A database of all domain names registered in a top-level domain or second-level domain extension.

Domain name system (DNS) **Systém doménových jmen**

*Distributed hierarchical name system used on the Internet network. It translates domain names into numerical **IP** addresses and back, contains information about which machines provide the relevant service (e.g. accepts electronic mail or show the content of web pages).*

Domain name system security extensions (DNSSEC) **Bezpečnostní rozšíření systému doménových jmen**

*Set of specifications which enable the security of information provided to **DNS** by a system in IP networks (Internet, for example). DNSSEC uses asymmetric encryption (one key for encryption and the second one for decryption). The owner of the domain, which uses DNSSEC generates both the private and the public key. Using its private key it then electronically signs technical data about the domain, which are then input into **DNS**. Using the public key, which is stored at an authority superior to the domain, it is possible to verify the authenticity of the signature. Some large servers use DNSSEC at present.*

Domain name system server (DNS server) **DNS server / Jmenný server**

Distributed hierarchical name system used in the Internet network. It translates the names of domains to numerical IP addresses and back, contains information about which machines provide the relevant service (e.g. receive emails or show the content of web applications) etc.

Doxingware **Doxingware**

A type of ransomware, which includes methods for collecting file contents and a threat of disclosing these files together with a threat of mediatisation and disclosing the name of the attacked person or organisation.

Easter egg **Velikonoční vajíčko**

Hidden and officially undocumented function or property of a computer programme, DVD or CD. Mostly these are puns and jokes doing no harm, graphics symbols, animations, subtitles with authors' names and similar. This hidden function is not activated in the usual way (menu, key, etc.) but by an unorthodox combination of the usual user activities, pushing a mouse key on an unusual place, a special sequence of keys, and so on. Often, eggs are hidden on the screen under "About" where these can be displayed by tapping on various parts of this panel while holding the key ALT and similar.

Eavesdropping **Odposlech / Nežádoucí odposlech**

Unauthorised catching of information.

Effectiveness, usefulness **Efektivnost, účelnost**

Extent to which planned activities are realized and planned results achieved.

Efficiency **Účelnost**

Relation between the achieved results and how well have the sources been used.

Electromagnetic analysis (EMA) **Elektromagnetická analýza**

Analysis of the electromagnetic field emanated from a cryptographic module as the result of its logic circuit switching, for the purpose of extracting information correlated to security function operation and subsequently the values of secret parameters such as cryptographic keys.

Electromagnetic compromising emanations (EME) **Elektromagnetické kompromitující vyzařování**

Intelligence-bearing signal, which, if intercepted and analysed, potentially discloses the information that is transmitted, received, handled, or otherwise processed by any information-processing equipment.

Electromagnetic valve **Elektromagnetický ventil**

A valve actuated by an electromagnetic coil, typically with only two states: open and closed.

Electronic archive **Elektronický archiv**

Long-term repository of electronically stored information. Electronic archives can be accessed online or offline. Backup systems (e.g. tape, virtual tape, etc.) are not considered to be electronic archives, but rather data protection systems (i.e. mechanisms for disaster recovery and business continuity).

Electronic attack **Elektronický útok**

Use of electromagnetic energy for the purposes of an attack. Includes weapons with directed energy, high-power microwave and electromagnetic pulses and RF equipment.

Electronic communication service **Služba elektronických komunikací**

Service usually provided for a fee, which consists wholly or predominantly of signal transmission over electronic communication networks, including telecommunication services and transmission services in networks used for radio and television broadcast and networks for cable television, excluding services which provide content using the networks and services of electronic communications or have editing supervision of the content transmitted over the networks and provided services of electronic communications; it does not include services of the information society which do not rest wholly or predominantly on the transmission of signals over networks of electronic communications.

Electronic defence **Elektronická obrana**

Use of electromagnetic energy to provide protection and to secure useful utilisation of the electromagnetic spectrum (includes protection of forces, spaces, etc.).

Electronic evidence **Elektronický důkaz**

Information or data, stored or transmitted in binary form that may be relied on as evidence.

Electronic mail (email) **Elektronická pošta**

Text, voice or picture message sent using public network of electronic communications, which can be stored in the network or enduser terminal until collected by the user.

Electronic means **Elektronické prostředky**

Primarily a network of electronic communications, electronic communication equipment, terminals, automatic call and communication systems, telecommunication and electronic mail.

Electronic signature **Elektronický podpis**

A signature made in an electronic form that has the same legal effect as a handwritten signature, if legal conditions are met (e.g. eIDAS in EU, NIST-DSS in the USA or ZertES in Switzerland). Unlike the ***Digital signature,*** *which is based on cryptography, the electronic signature is a legal concept.*

Electronic storage medium **Elektronické paměťové médium**

A device, on which data files may be recorded and transferred among computers.

Electronic warfare **Elektronický boj**

*Military activity using electromagnetic energy in support of offensive and defensive actions in order to achieve offensive and defensive supremacy. This means engaging in fighting in the environment using electromagnetic radiation. It is a separate discipline but as one of the elements, it supports cyber security within **NNEC**.*

Electronically Stored Information (ESI) **Elektronicky uložená informace**

Data or information of any kind and from any source, whose temporal existence is evidenced by being stored in, or on, any electronic medium. ESI includes traditional e-mail, memos, letters, spreadsheets, databases, office documents, presentations, and other electronic formats commonly found on a computer. ESI also includes operating systems, applications, and file-associated metadata (such as timestamps, revision history, file type, etc.).

Element of the critical infrastructure **Prvek kritické infrastruktury**

Building, equipment, device or public infrastructure, in particular, determined using the cross-criteria and sector criteria; if the element in the critical infrastructure is a part of the critical European infrastructure, it is considered to be an element of the critical European infrastructure.

Elliptic curve **Eliptická křivka**

Cubic curve E without a singular point. Note: The set of points E together with an appropriately defined operation for a field that includes all coefficients of the equation describing E is called the definition field of E. The form of a cubic curve equation used to define an elliptic curve varies depending on the field.

Emulation **Emulace**

Use of a data processing system to emulate another data processing system; emulating system receives the same data, runs the same programmes and exhibits the same results as the emulated system.

Encrypted key **Zašifrovaný klíč**

A cryptographic key that was encrypted using an approved security function with a key encryption key.

Encrypted text, Ciphertext **Zašifrovaný text, šifrovaný text**

Plain text, which was transformed to hide its information content.

Encryption algorithm **Šifrovací algoritmus**

Process which transforms plaintext into ciphertext.

Encryption system **Šifrovací systém**

Cryptographic technique used to protect the confidentiality of data, and which consists of three component processes: an encryption algorithm, a decryption algorithm, and a method for generating keys.

Encryption, Ciphering **Šifrování**

Cryptographic transformation of data (called "plaintext") into a form (called "ciphertext") that conceals the data's original meaning to prevent it from being leaked or used. If the transformation is reversible, the corresponding reversal process is called decryption and restores the encrypted data to plaintext.

Endpoint device **Koncové zařízení**

*Network connected **ICT** hardware device like desktop computers, laptops, smart phones, tablets, thin clients, printers or other specialized hardware including smart meters and **IoT** devices.*

Energy-independent storage **Energeticky nezávislé úložiště**

Storage that retains its contents even after power is removed.

Enterprise Resource Planning (ERP) System **Podnikový informační systém**

A system that integrates enterprise-wide information including human resources, financials, manufacturing and logistics as well as connects the organisation to its customers and suppliers.

Entity **Entita**

A specific person, group, device or process.

Entity / identity Authentication **Autentizace / Ověření totožnosti entity / identity**

A verification that an entity is the one claimed.

Entrapment **Léčka**

Intentional placement of obvious defects into a data processing system in order to detect penetration attempts, or to deceive an adversary who should use the defect.

Establishing the context **Stanovení kontextu**

Establishing the limits of external and internal parameters to be taken into account during risk management and setting of the risk validity ranges and risk criteria for the risk management policy.

European critical infrastructure **Evropská kritická infrastruktura**

Critical infrastructure in the territory of the Czech Republic whose infringement would result in a serious impact also on another member of the European Union.

European union agency for cybersecurity (ENISA) **Agentura Evropské unie pro kybernetickou bezpečnost**

Agency founded in 2004 by the European Union as a cooperative centre in the area of network and information security. Its role is to create an information platform for the exchange of information, knowledge and "best practices" and thus help EU, its member states, the private sector and the public in the prevention and solutions of security problems.
ENISA changed its statute by regulation of the European Parliament (EU) 2019/881 of the European Parliament and of the EU Council of 17 April 2019 (Cybersecurity Act) on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013.

Event **Událost**

Occurrence or change of a particular set of circumstances.

Evidence **Důkaz**

Information which is used, either by itself or in conjunction with other information, to establish proof about an event or action. Note: Evidence does not necessarily prove the truth or existence of something, but can contribute to the establishment of such a proof.

Evidence preservation facility **Zařízení pro uchování důkazů**

Secure environment or a location where acquired evidence is stored. An evidence preservation facility should not be exposed to magnetic fields, dust, vibration, moisture or any other environmental elements (such as extreme temperature or air humidity) that may damage the potential digital evidence within the facility.

Executive management **Výkonné vedení**

A person or group of people who have delegated responsibility from the governing body for the implementation of strategies and policies to accomplish the purpose of the organisation. Executive management is sometimes called top management and can include Chief Executive Officer, Chief Financial Officer, Chief Information Officer, and similar roles.

Exercise, skill training **Cvičení, procvičování**

Process of training to assess, verify and improve performance.

Exploit **Zneužití**

Defined way to breach the security of information systems through vulnerability.

Exposure **Vystavení hrozbám**

The possibility that a concrete attack would use a specific vulnerability of a data processing system.

External context **Vnější kontext**

The external environment in which an organisation seeks to achieve its objectives.

Extranet **Extranet**

Extension of an organisation's Intranet, especially over the public network infrastructure, enabling resource sharing between the organisation and other organisations and individuals that it deals with by providing limited access to its Intranet.

Failover **Failover**

Automatic switch to a backup system or process at the instant of failure of the previous one in order to achieve a very short time of outage and increase in reliability.

Failure access **Chybný přístup**

Unauthorised and usually unintentional access to data in a data processing system, which is the result of hardware or software failure.

False negative **Falešné ticho, chybné zamítnutí**

IDPS system reports no alert when there is an attack.

False positive **Falešný poplach, chybné přijetí**

IDPS system reports an alert when there is no attack.

Fault Tolerant System **Systém odolný vůči selhání**

A system with the built-in mechanisms to provide the correct execution of its function even in the presence of a hardware or software fault.

Federated identity **Federovaná identita**

Identity for use in multiple domains, and which contains more identities.

Field Device **Provozní zařízení**

Equipment that is connected to the field side on an ICS. Types of field devices include RTUs, PLCs, actuators, sensors, HMIs, and associated communications.

Fieldbus **Provozní datová sběrnice**

A digital, serial, multi-drop, a two-way data bus or communication path or link between low-level industrial field equipment such as sensors, transducers, actuators, local controllers, and even control room devices. Use of fieldbus technologies eliminates the need for point-to-point wiring between the controller and each device. A protocol is used to define messages over the fieldbus network with each message identifying a particular sensor on the network.

File **Soubor**

General named set of data. It can be a document, multimedia data, database or practically any other content, which the user or software may find useful to have permanently available under a concrete name.

File protection **Ochrana souboru**

Implementation of suitable administrative, technological or physical means for the protection against unauthorised access, modification or erasure of a file.

File system **Souborový systém**

Method of organisation and storage of data in the form of files so that access to them would be easy. File systems are stored on a suitable type of electronic memory, which can be located directly in the computer (hard disc) or can be made accessible using a computer network.

File transfer protocol (FTP) **File transfer protocol (FTP)**

An Internet standard (RFC 959) for transferring files between a client and a server.

Firewall **Firewall**

*A security barrier placed between network environments — consisting of a dedicated device or a composite of several components and techniques — through which all traffic from one network environment traverses to another, and vice versa, and only authorised traffic, as defined by the local security policy, is allowed to pass. A **firewall** can be implemented as hardware or software, or a combination of both.*

Firmware **Firmware**

*Programme controlling **hardware**.*

Flaw / loophole **Vada / skulina**

Operational dysfunction, omission, or oversight making it possible to bypass protective mechanisms or put them out of action.

Flooding **Zaplavení, zahlcení**

Accidental or intentional insertion of a large volume of data resulting in a service denial.

Flow chart **Vývojový digram**

A graphic programming language based on flowcharts whose functionality they represent. It is part of IEC 61113-3.

Forensic analysis / investigation **Forenzní analýza / vyšetřování**

Investigation procedures on digital data to obtain proofs about the activities of users (attackers) in the area of information and communication technologies.

Forum for incident response and security teams (FIRST) **FIRST**

*Worldwide organisation uniting about 200 workplaces of the **CSIRT/CERT** type.*

Freeware **Freeware**

Proprietary software usually distributed free (or for a symbolic reward). We speak sometimes about a kind of software licence. Conditions for the free use and distribution are defined in the licence agreement. The author of the freeware usually retains the copyright.

Function Block **Function block (Funkční bloky)**

Graphic programming language. Programming is done by combining functional blocks. This representation is part of IEC 61113-3.

Gateway **Brána**

Device that converts a specific protocol to another protocol.

Generic TLD **Generické TLD**

*See **TLD.***

Generic traffic flood **Obecné zahlcení**

*Form of a **DDoS** attack.*

GNU / GPL **GNU / GPL**

General public licence GNU – licence for free software requesting that related creations be available under the same licence.

GNU privacy guard (GPG) **GPG**

*Free version of **PGP**. See **PGP**.*

Governance of information security **Správa bezpečnosti informací**

The system by which an organisation's information security activities are directed and controlled.

Governing body **Orgán správy a řízení**

Person or group of people who are accountable for the performance and conformance of the organisation.

Grey hat **Grey hat**

*An individual who according to the activity stands between **White hat** and **Black hat** hackers, since the individual abuses security weakness of systems or a product to publicly draw attention to their vulnerability. However, publicising this sensitive information may be an opportunity for persons of the Black hat character to commit criminal acts.*

Guideline **Směrnice**

A (binding) recommendation of what is expected to be done in order to achieve a certain target.

Hack / Hacking **Hack / Hacking**

(1) Intentionally accessing a computer system without the authorisation of the user or the owner.
(2) A fitting, unusual, witty, or fast solution of an issue using a programme or a computer system in a way that its designer did not intend.

Hacker **Hacker**

Person:
(1) who engages in the study and analysis of details of programmable systems most often for an intellectual inquisitiveness and keeps on improving this ability (White hat);
(2) who enjoys programming and who programs well and fast;
*(3) who is an expert for a certain operating system or a programme, e.g. UNIX. The idea of Hacker is often improperly used for persons who abuse their knowledge during breaking into an information system and thus break the law. See **Cracker**.*

Hackers for hire (H4H) **Hackers for hire**

Acronym for hackers who offer their services to other criminal, terrorist or extremist groups (hired hackers).

Hactivism **Hactivismus**

Hacking for a politically or socially motivated purpose.

Hardened operating system **Zodolněný operační systém**

An operating system that is intentionally configured or designed to minimise the potential for compromise or attack. This may be a general OS, such as Linux or a bespoke solution.

Hardening **Zodolnění, hardening**

A process of securing a system by reducing its number of usable vulnerabilities. Hardening typically includes the removal of software, user accounts and services that are not essentially necessary.

Hardware **Technické prostředky (vybavení)**

Physical components of a system (equipment) or their parts (e.g. a computer, printer, peripheral devices).

Hardware (Physical) random number generator **Fyzikální generator náhodných čísel**

A hardware device using the randomness of a physical phenomenon (for example, unpredictability in the behaviour of atomic and subatomic processes, randomness of radioactive material decay or more often the randomness of the white noise of a noise diode) to generate a random sequence of numbers. Such a generator is usually denoted as „true random number generator" (TRNG).

Hardware security module (HSM) **Hardwarový bezpečnostní modul**

Hardware implementation of a secure crypto-processor using an certificate and a private key to provide secure authentication.

Hash function **Hash funkce**

A one-way mathematical transformation of input data (text) into a file (digest, hash). It is computationally practically unrealistic to get the original data back from the hash return. This function is used in applications of data security (eg. authentication, digital signature, integrity check). Security infringement of a hash function is denoted a collision.

Hash message authentication code (HMAC) **Hash autentizační kód zprávy**

*Authentication code of a message based on a hash function (see **Hash function**).*

Help desk **Horká linka**

Online (as a rule, telephone) service offered by an automated information system and through which users can get help for using shared or specialised services of the system.

Hoax **Poplašná zpráva**

It tries to create an impression of trustworthiness by its content. It informs, for example, about the spread of viruses or it inveighs against the social feeling of the addressee. It may contain harmful code or a link to internet pages with harmful content.

Honeypot **Honeypot**

Generic term for a decoy system used to lure the attacker to spend time on information that appears to be very valuable, but actually is fabricated and would not be of interest to a legitimate user.

Host **Host**

A system or computer in a TCP/IP-based network with an assigned network address.

Human-machine interface (HMI) **Rozhraní člověk-stroj**

Software and hardware that allow human operators to monitor the state of a process under control, modify control settings to change the control objective, and manually override automatic control operations in the event of an emergency. It also allows a control engineer or operator to configure set points or control algorithms and parameters in the controller. The HMI displays process status information, historical information, reports and other information to operators, administrators, managers, business partners, and other authorised users. The location, platform, and interface may vary a great deal. For example, an HMI could be a dedicated platform in the control centre, a laptop on a WLAN or a browser on any system connected to the Internet.

Hypertext transfer protocol (HTTP) **Hypertext transfer protocol**

An application protocol for distributed, collaborative, hypermedia information systems. HTTP is the foundation of data communication for the World Wide Web.

Hypertext transfer protocol secure (HTTPS) **Hypertext transfer protocol secure**

*A widely used communications protocol for secure communication over a computer network, with especially wide deployment on the Internet. Technically, it is not a protocol in and of itself; rather, it is the result of simply layering the Hypertext Transfer Protocol (**HTTP**) on top of the **SSL/TLS** protocol, thus adding the security capabilities of **SSL/TLS** to standard HTTP communications.*

Hypervisor **Hypervisor**

Computer software that creates and runs one or more virtual machines.

ICMP flood **ICMP záplava**

An attack using the ICMP protocol. Most often used are ICMP echo (Ping) packets, which serve to establish if the remote (target) equipment is available. Sending out a large number of these ICMP messages (or large ICMP echo packets) may result in clogging the remote system and its slowdown or total unavailability. This is a simply executed attack of the ***DDoS*** *type.*

ICT Disaster Recovery **Obnova po havárii ICT**

The ability of the ICT elements of an organisation to support its critical business functions to an acceptable level within a predetermined period following a disruption.

ICT disaster recovery plan (ICT DRP) **Plán obnovy po havárii ICT**

Clearly defined and documented plan which recovers ICT capabilities when a disruption occurs. Note: It is called ICT continuity plan in some organizations.

ICT readiness for business continuity (IRBC) **Připravenost ICT na zajištění kontinuity provozu**

Capability of an organisation to safeguard its business operations by detection and response to disruption and recovery of ICT services.

Identifiability **Identifikovatelnost**

Condition which results in a personally identifiable information principal being identified, directly or indirectly, on the basis of a given set of personally identifiable information.

Identification **Identifikace**

A process when a certain entity in a given domain is differentiated from the other entities. Submitted or visible attributes of the entity are verified during the identification. Usually, the identification is part of information exchange among the entity, domain services and used resources. Identification may be made repeatedly even though the entity is known in the network.

Identifier / ID **Identifikátor / ID**

Identity information that unambiguously distinguishes one entity from another one in a given domain.

Identity **Identita**

Set of properties, which uniquely define a definite object – a thing, person, and event.

Identity assurance **Záruka totožnosti**

Level of assurance in the result of identification. Identity assurance expresses the level of confidence in provenance, integrity and applicability of identity information including confidence in identity information maintenance.

Identity management (IdM) **Řízení identit**

Processes and policies involved in managing the lifecycle and value, type and optional metadata of attributes in identities known in a particular domain. Note: In general identity management is involved in interactions between parties where identity information is processed. Processes and policies in identity management support the functions of an identity information authority where applicable, in particular to handle the interaction between an entity for which an identity is managed and the identity information authority.

Identity Management System (IdMS) **Systém řízení identit**

System controlling entity identity information throughout the information lifecycle in one domain.

Identity proofing / Initial entity authentication **Prokázání totožnosti**

A form of authentication based on producing an identity card that is the condition for access rights.

Identity register / IMS register **Registr identit**

Repository of identities for different entities.

Identity theft **Krádež totožnosti / krádež identity**

Result of a successful false claim of identity.

Identity token **Identifikační předmět**

Token used to find out and verify (authenticate) the identity.

Identity validation **Validace identity**

Execution of tests enabling a system to recognise and validate entities on the basis of data processing.

Imaging **Pořízení bitového obrazu**

Process of creating a bitwise copy of an electronic storage medium.

Impact **Dopad**

(1) Adverse change in the attained degree of objectives. (2) Consequenses of a certain act or event.

Important information system **Významný informační system**

Complex of information systems according to the law on cyber security, managed by the public administration bodies, which themselves are not a part of the critical infrastructure, and where any infringement of information security would limit or seriously endanger the function of a public administration body.

Important network **Významná síť**

A network of electronic communications as defined by the law on cyber security and enabling direct link into foreign communication networks or enabling direct connection to critical information infrastructure.

Incident **Incident**

(1) (Security incident) A single or a series of unwanted or unexpected information security breaches (whether of criminal nature or not) that have a significant probability of compromising business operations or threatening information security.
(2) (Operational incident) An unplanned interruption to a service, a reduction in the quality of a service or an event that has not yet impacted the service to the customer.

Incident handling **Řešení incidentů**

Actions of detecting, reporting, assessing, responding to, dealing with, and learning from information security incidents.

Incident response **Reakce na incidenty**

Actions taken to mitigate or resolve an information security incident, including those taken to protect and restore the normal operational conditions of an information system and the information stored in it.

Incident response team (IRT) **Tým reakce na incidenty**

A team of appropriately skilled, able and trusted members of the organisation that handles incidents during their lifecycle. CERT (Computer Emergency Response Team) and CSIRT (Computer Security Incident Response Team) are commonly used terms for IRT.

Incinerate **Spalování**

Destruct by burning media completely to ashes.

Industrial computer (IPC) **Průmyslový počítač**

A computer, the cover and inner construction of which are made in the industrial modification. Industrial modification means a mechanically modified structure for its resistance to dust, water, and mechanical damage. The goal is to increase the

life of components that are particularly sensitive to dust, humidity or vibrations and other mechanical stress. Often, the touch screen is a part of the cover.

Industrial Control System (ICS) **Průmyslový řídicí systém**

A control system, including supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and other control system configurations such as Programmable Logic Controllers (PLC) often found in the industrial sectors and critical infrastructures. An ICS consists of combinations of control components (e.g., electrical, mechanical, hydraulic, pneumatic) that act together to achieve an industrial objective (e.g., manufacturing, transportation of matter or energy).

Information **Informace**

Any sign expression, which makes sense for the communicator and receiver.

Information (cyber) society **Informační (kybernetická) společnost**

A society capable of utilising, and indeed utilising, information and communication technologies. The basis is an incessant exchange of knowledge and information and handling them under the assumption of understanding these. This society considers creation, distribution and manipulation of information as the most significant economic and cultural activity.

Information and communication technology (ICT) **Informační a komunikační technologie**

Any technology dealing with processing and transfer of information, in particular computing and communication technology and software.

Information asset **Informační aktivum**

Knowledge and data of value (importance) to an organisation.

Information assurance **Information assurance**

Set of measures to achieve the required level of confidence in the protection of communication, information and other electronic as well non-electronic systems and information stored, processed or transferred in these systems with regard to confidentiality, integrity, availability, undeniability and authenticity.

Information Criminality **Informační kriminalita**

Criminal activity with a determined relation to software, data, more precisely to stored information, more precisely all activities resulting in unauthorised reading, handling, erasing, abusing, changing or other data interpreting.

Information need **Informační potřeba**

Insight necessary to manage objectives, goals, risks and problems.

Information operation (IO) **Informační operace**

Planned, goal-oriented and coordinated activity done in support of political and military objectives of operation, to influence the decision-making process of a possible adversary and its allies by affecting its information, information processes and communication infrastructure and at the same using information and protection for own information and communication infrastructure. IO is exclusively a military activity, which has to coordinate military information activities with the objective of influencing the thinking (will), understanding and capabilities of the adversary or potential adversary. All information activities should be conducted in line with the objectives of the military operation and to support them at the same time.

Information processing facilities **Vybavení pro zpracování informací**

Any information processing system, service or infrastructure, or the location where they reside.

Information security (INFOSEC) **Bezpečnost informací / informačních systémů**

(1) Preservation (protection) of confidentiality, integrity and availability of information.
(2) Implementation of general security measures and procedures for: (a) protection of information against loss or compromise (loss of confidentiality, integrity and reliability), or as the case may be for their detection and adoption of remedial actions.
(b) continuation of information availability and the ability to work with them within the scope of functional rights. Measures INFOSEC cover security of computers, transmission, emissions and encryption security and exposing threats to facts and systems and prevention thereof.

Information security breach **Narušení bezpečnosti informací**

Compromise of security that leads to the undesired destruction, loss, alteration, disclosure of, or access to, protected information transmitted, stored or otherwise processed.

Information security continuity **Kontinuita bezpečnosti informací**

Processes and procedures for ensuring continued information security operations.

Information security event **Událost bezpečnosti informací**

Identified occurrence of a system, service or network state indicating a possible breach of information security policy or a failure of controls, or a previously unknown situation that may be security relevant.

Information security incident management — **Řízení incidentů bezpečnosti informací**

Processes for detecting, reporting, assessing, responding to, dealing with and learning from security incidents.

Information security investigation — **Vyšetřování incidentu bezpečnosti informací**

Acquisition, examinations, analysis and interpretation of traces and proofs to aid understanding the nature of an information security incident.

Information security management (ISM) — **Řízení bezpečnosti informací**

Managing the preservation of confidentiality, integrity and availability of information.

Information security management system (ISMS) — **Systém řízení bezpečnosti informací (SŘBI)**

Part of the management system, based on the attitude towards security risks, definition, implementation, operation, monitoring, re-analysing, administration and improvement of information security.

Information security management system (ISMS) professional — **Odborník na systém řízení bezpečnosti informací (SŘBI)**

Person who establishes, implements, maintains and continuously improves one or more information security management system processes.

Information Security Programme / Plan — **Plán/program bezpečnosti informací**

A formal document that provides an overview of the security requirements for an organisation-wide information security programme and describes the programme management controls and common controls in place or planned for meeting those requirements.

Information security risk — **Riziko bezpečnosti informací**

Aggregate of possibilities that a threat would utilise the vulnerabilty of an asset or group of assets and thus cause damage to an organisation.

Information security threat — **Bezpečnostní hrozba**

A potential cause of an undesired event, which may result in damage to the system and its assets, e.g. destroying, undesired disclosing (compromising), data modification or unavailability of services.

Information society service — **Služba informační společnosti**

Any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services. For this definition: (1) 'at a distance' means that the service is provided without the parties being simultaneously present; (2) 'by electronic means' means that the service is sent initially and received at its destination using electronic equipment for the processing (including digital compression) and storage of data, and entirely transmitted, conveyed and received by wire, by radio, by optical means or by other electromagnetic means; (3) 'at the individual request of a recipient of services' means that the service is provided through the transmission of data on individual request.

Information system **Informační systém**

A functional unit enabling goal-oriented and systematic acquisition, processing, storage and access to information and data. Includes data and information sources, media, hardware, software and utilities, technologies and procedures, related standards and personnel.

Information warfare **Prostředky informační války**

Integrated use of all military capabilities including information security, deception, psychological operations, electronic warfare, and destruction. All forms of reconnaissance, communication and information systems contribute to it. The objective of information warfare is to put obstacles in the flow of information, influence and decrease efficiency or liquidate the system of command and control of the adversary, and at the same time to protect own systems of command and control from similar actions of an adversary.

Informatisation of society **Informatizace společnosti**

Process of promoting new literacy in a society focused on adopting new methods of work with computers, information and information technology.

Infoware **Infoware**

Application for the automatic support of classical battle events, more precisely a set of activities serving to protect, mine out, damage, suppress or destroy information or information sources, with the objective of achieving a significant advantage in a battle or victory over a concrete adversary. The notion of Infoware must not be mistaken with the notion Infowar that is information war.

Infrastructure as a Service (IaaS) **Infrastruktura jako služba**

The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, including operating systems and applications. The consumer does not manage or control the underlying cloud

*infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host **firewalls**).*

Initialisation vector **Inicializační vektor**

Initialisation vector puts the appropriate algorithm always into a different (random) initial state, and thus even with the same secret key generates in each case a different output sequence. It is a uniquely generated data stream, in case of stream cyphers it is a vector, and with block cyphers, it is the „zero block". Initialising vector tends to be transferred openly and allows the same initial setting of cypher devices.

Input/Output (I/O) **Vstup / výstup (I/O)**

Equipment that is used to communicate with a computer as well as the data involved in the communications.

Input/output (I/O) server **Vstupně-výstupní (I/O) server**

A control component responsible for collecting, buffering and providing access to process information from control subcomponents such as PLCs, RTUs and IEDs. An I/O server can reside on the control server or a separate computer. I/O servers are often used for interfacing third-party control components, such as an HMI or a control server.

Insider **Insider**

Dangerous user (employee, intern) who abuses a legal access to the communication and information system of an organisation, in particular in order to perform unauthorised pilferage of sensitive data and information.

Integrity **Integrita**

The property of accuracy and completeness.

Intelligent electronic device (IED) **Inteligentní electronické zařízení**

A "smart" sensor containing the intelligence required to acquire data, communicate to other devices, and perform local processing and control. It could combine an analogue input sensor, analogue output, low-level control capabilities, a communication system, and programme memory in one device. The use of IEDs in SCADA systems for automatic control at the local level.

Interested party **Zainteresovaná strana**

Person or organisation that can influence, be influenced by, or influenced by a decision or activity.

Interface **Rozhraní**

(1) Location and mode of interconnecting systems or their parts. (2) Means of interaction with a component or module.

Internal context **Vnitřní kontext**

the internal environment in which an organisation seeks to achieve its objectives.

Internal group **Vnitřní, interní skupina**

Part of an organisation of a service provider, which has concluded a documented contract with the service provider about its share in the design, handover, delivery and improvement of a service or services.

Internet **Internet**

A global system of interconnected computer networks which use the standard internet protocol (TCP/IP). Internet serves billions of users around the world. It is a network of networks consisting of millions of private, public, academic, commercial and government networks, with a local to global outreach, that are all interconnected by a wide range of electronic, wireless and optical network technologies.

Internet assigned numbers authority (IANA) **Úřad pro přidělování čísel na Internetu**

*Authority oversseing **IP address** assignment, administration of **DNS** zones (assignment of **TLD** domains and the creation of generic domains) and the administration and development of internet protocols. At present, **IANA** is one of the departments of the **ICANN** organization.*

Internet control message protocol (ICMP) **Internet control message protocol**

*This is a service protocol, which is part of the **IP** protocol. Its main mission is to report error messages regarding the availability of services, computers or routers. For these purposes, ping or tracerout instruments are used, for example.*

Internet corporation for assigned names and numbers (ICANN) **Internetová společnost pro přidělování jmen a čísel na internetu**

The non-profit organisation responsible for the administration of domain names assignment as well IP addresses, for the maintenance of operational stability of internet, support of economic competition, achievement of a broad representation of the global internet community, and which develops its mission by bottom-to-top management and consensual processes.

Internet crime **Internetová kriminalita**

Criminal activity where services or applications in the Internet are used for or are the target of a crime, or where the Internet is the source, tool, target, or place of a crime.

Internet gateway **Internetová brána**

Entry point to access the internet.

Internet of things (IoT) **Internet věcí**

A network of physical objects ("things") embedded with sensors, software, and other technologies for the purpose of connecting and exchanging data with other devices and systems over the internet.

Internet protocol (IP) **Internet Protocol**

Protocol by which all equipment in the Internet mutually communicate. Today, the most used is the fourth revision (IPv4); however, step by step there will be a transition to a newer version (IPv6).

Internet relay chat (IRC) **IRC**

A form of live (real-time) communication of text messages (chat) or synchronous conferences. These are systems intended primarily for group communications in discussion forums, so-called channels, but it also enables one-to-one communication via a private message, as well as a chat and data transfer using direct client-to-client. Today, it is not used so much; it has been replaced by newer instruments such as Skype, ICQ or Jabber.

Internet security **Bezpečnost internetu**

Protection of confidentiality, integrity and availability of information in the Internet network.

Internet service provider (ISP) **Poskytovatel služeb internetu**

The organisation that provides Internet services to users and enables its customers access to the Internet.

Internet services **Internetové služby**

Services provided to a user to enable access to the Internet via an assigned IP address, which typically include authentication, authorisation and domain name services.

Interoperability **Interoperabilita**

Capability to act jointly in fulfilling set objectives, or the capability of systems, units or organisations to provide services to other systems, units or organisations and accept these from them and thus use shared services for an effective common activity.

Intranet **Intranet**

„Private" (internal) computer network using the classical Internet technology making it possible for employees of an organisation to communicate effectively and share information.

Intrusion **Průnik**

Unauthorised, illegal access to a network or a network-connected system, i.e., deliberate or accidental unauthorised access to an information system, or unauthorised use of resources within an information system.

Intrusion detection **Detekce průniku**

The formalised process of detecting intrusions, generally characterised by gathering knowledge about abnormal usage patterns using HW and SW means, including the recognition which vulnerability was used, how and when it happened.

Intrusion Detection and Prevention Systems (IDPS) **Systémy detekce a prevence průniku**

Systems that are used to identify that an intrusion has been attempted, is occurring, or has occurred and actively respond to intrusions in information systems and networks.

Intrusion detection system (IDS) **Systém detekce průniku**

A technical system that is used to identify that an intrusion has been attempted, is occurring, or has occurred and possibly responds to intrusions in information systems and networks.

Intrusion prevention **Prevence průniku**

Formal process of actively responding to prevent intrusions.

Intrusion prevention system (IPS) **Systém prevence průniku**

A variant on intrusion detection systems that are specifically designed to provide an active response capability.

Investigative lead **Vedoucí týmu vyšetřovatelů**

Person leading the investigation at a strategic level.

Investigative team **Tým vyšetřovatelů**

All persons directly involved in the conduct of the investigation.

IP address **IP adresa**

Number, which uniquely identifies a network interface, which uses IP (internet protocol) and serves for the differentiation of interfaces connected in the computer network. At present, the most widespread version IPv4 uses a number of 32 bits written in decimal in groups of eight bits (e.g. 123.234.111.222).

IP Masquerade **Maškaráda IP**

A mechanism of hiding, or pretending, another IP address, and thus posing as another identity.

IP masquerading **IP maškaráda**

*The mechanism, which allows connecting to **the Internet** a large number of devices for which no so-called public **IP** addresses are available. These devices are assigned so-called private IP addresses, and access to the Internet is implemented through the mechanism of address translation (NAT, Network Address Translation).*

IP spoofing **Podvržení IP adresy**

*Spoofing of the source IP address on a device (a computer) which triggers connection (with a recipient) in order to hide the real sender. This technique is used particularly in attacks of **DoS** type.*

IPSec **IPSec**

*A security-based extension of the **IP** protocol predicated on authentication and encryption of each **IP** datagram. It is secured at the network layer. IPSec is defined in a number of RFCs issued by IETF, the fundamental ones are 2401 and 2411.*

IS security policy **Bezpečnostní politika informačního systému**

General purpose of management and direction in the control of information system security with the definition of criteria to assess risks.

ISMS project **Projekt ISMS**

Structured activities undertaken by an organisation to implement an ISMS.

IT network **IT síť**

Geographically distributed system formed by interconnected IT systems for information exchange and containing different components of the interconnected systems and their interfaces with data communication networks, which complement them.

IT security policy **Bezpečnostní politika IT**

*Rules, directives and practices deciding how are assets including sensitive information administered, protected and distributed inside the organisation and its **ICT** systems.*

IT system **IT systém**

Set of devices, methods, data, metadata, procedures and sometimes persons that are arranged to fulfil some functions during information processing.

Kerberos **Kerberos**

Kerberos is a computer network authentication protocol which works by „tickets" to allow nodes communicating over a non-secure network to prove their identity to one another in a secure manner. Its designers aimed it primarily at a client-server model, and it provides mutual authentication—both the user and the server verify each other's identity. Kerberos protocol messages are protected against eavesdropping and replay attacks.

Key **Klíč**

Sequence of symbols that controls the operations of a cryptographic transformation (e.g. encryption, decryption, cryptographic check function computation, signature calculation, or signature verification).

Key authentication **Ověření totožnosti klíče**

A process to verify the identity (authentication) of a user, the user not necessarily being human. A user is considered authenticated if the ownership of a key is justified. Process of verification that the public key truly belongs to that person.

Key destruction **Ničení klíčů**

A service for the secure destruction of keys that are no longer needed.

Key distribution centre (KDC) **Středisko distribuce klíčů**

An entity entrusted to generate or acquire and distribute keys to other entities.

Key encryption key (KEK) **Klíč pro šifrování klíčů**

Cryptographic key that is used for the encryption or decryption of other keys.

Key exchange procedure **Postup výměny klíčů**

Procedure to establish a common cryptographic key. The method uses asymmetric cryptography. This method allows establishing a symmetric enciphering key among the communicating parties using an insecure channel, without the need for prior exchange of a secret enciphering key.

Key Generation Center (KGC) **Středisko generování klíčů**

Organisation body that enables the generation of cryptographic keys and their loading into tokens for an independent distribution into cryptographic devices.

Key loading **Zatížení klíče**

A volume of data in bits which can be encrypted by one cryptographic key without compromising the security of encryption.

Key management **Správa klíčů**

Administration, generation, registration, certification, distribution, installation, storage, deregistration, archiving, revocation, derivation and destruction of keys in accordance with a security policy.

Key pair **Pár klíčů**

Pair consisting of a public key and a private key associated with an asymmetric cipher.

Key validity period **Doba platnosti klíče**

The time period during which a cryptographic key may be used to encipher or decipher data. After the expiration of key validity, an extension period may be defined to use the key for data deciphering.

Keylogger (Keystroke logger) **Keylogger (Keystroke logger)**

Software reading when individual keys are pushed; may, however, be regarded as a virus by an antivirus programme, in case of software it may be a certain form of spyware but there are even hardware keyloggers. It is often used for secret monitoring of all PC activities, is invisible for other users and protected by a password. It enables automatic logging of all keystrokes (written text, passwords, etc.), visits to www pages, chats and discussions over ICQ, MSN and similar, running applications, screenshots of computer work, user file handling and other. Logged data could be secretly sent by email.

Knowledge base **Znalostní báze**

Database containing reference rules and information about the experience and professional knowledge in a certain area.

Known error **Známá chyba**

Problem whose primary cause is known, or for which a method is established, to decrease or remove the impact of the problems on a service, using a substitute solution.

Ladder **Ladder (žebřík)**

Type of graphical programming language. It consists of connecting the supply and output bus with logic functions. It is also referred to as the language of contact schemes. This representation is part of IEC 61113-3.

Lamer **Lamer**

Person, usually a complete beginner, who is unfamiliar with the given IT issues.

Leetspeak **Leetspeak**

Language replacing the letters of the Latin alphabet by numerals and printable ASCII characters. It is used quite a lot on the Internet (chat and online games). This computer dialect, usually of the English language, has no fixed grammatical rules and words may be formed by shortening, e.g. by omissions of letters or corruption ("nd" – end, "U" – you, "r" – are).

Legal digital evidence **Legální elektronický důkaz**

Digital evidence, which is accepted in a judicial process.

Level of risk / risk level **Úroveň rizika**

The magnitude of the risk expressed in terms of the combination of consequences and their likelihood.

Licence **Licence**

Permission as well as the document recording that permission.

Life cycle **Životní cyklus**

Evolution of a system, product, service, project or other human-made entity from conception through retirement.

Life cycle model **Model životního cyklu**

A model of a set of processes and activities concerned with the life cycle that may be organised into stages, which also acts as a common reference for communication and understanding.

Likelihood **Pravděpodobnost, možnost výskytu**

The possibility of something happening.

Linkage / Fusion **Spojování / Fúze**

Useful combination of data or information from one data processing system, with data or information from another system, so as to declassify protected information.

Local area network (LAN) **Lokální síť**

The term for small networks, usually within administratively uniform aggregates – companies, buildings, communities, which are formed with the aim to facilitate sharing of means (IS, data, services, equipment) and to enable effective protection against undesirable phenomena.

Local internet registry (LIR) **Lokální internetový registr**

The organisation, usually active in one network, which is assigned a block of IP addresses from RIR. LIR assigns the IP address blocks to its customers connected to the given network. Most LIRs are internet service providers, companies or academic institutions. Related expressions – RIR.

Log **Log**

Shortened expression for Log file.

Log file **Soubor logů**

File containing information on the activities of subjects in the system, access to this file is controlled.

Logical access control **Logické řízení přístupu**

Use of mechanisms related to data or information to enable control of access.

Logical bomb **Logická bomba**

Harmful logic causing damage to a data processing system and being triggered by certain specific system conditions. Programme (a subset of Malware) which is secretly put into applications or into an operating system where, under predetermined conditions, it performs destructive activities. The logical bomb is composed of two basic components: trigger and action. Predetermined specified condition triggering the logic bomb may be, for example, a fixed date (anniversary of a certain event – for example "Virus 17 November"). In this case, the type is a so-called time bomb.

Loss **Ztráta**

Reduction in the value of an asset.

MAC address **MAC adresa**

MAC = Media Access Control. Unique identifier of a network device allotted by the manufacturer.

Machine Controller **Řídicí jednotka stroje**

A control system that electronically synchronises drives within a machine system instead of relying on synchronisation via a mechanical linkage.

Maintenance **Údržba**

(1) Any act that either prevents a failure or malfunction of equipment or restores its operating capability.
(2) Any change in an application after its delivery (e.g. error correction, added functionality, enhanced performance or improvement of the application's functionality).

Maintenance hook **Tajná vrátka / Přístup ke službám**

Loophole in software which enables easy maintenance and addition of other characteristics and which can enable an access to a programme in unusual locations or without the usual checks.

Malformed query **Špatně utvořený dotaz**

(1) Erroneous query, which may result in triggering a nonstandard or unexpected behaviour of a system.
(2) Mode of an attack.

Malicious contents **Škodlivý obsah**

Applications, documents, files, data or other resources that have malicious features or capabilities embedded or hidden.

Malicious logic **Zlovolná logika**

Programme implemented in hardware, firmware or software whose purpose is to perform some unauthorised or harmful action (e.g. a logical bomb, Trojan horse, virus, worm, etc.).

Malware – malicious software **Škodlivý software**

Software designed with malicious intent containing features or capabilities that can potentially cause harm directly or indirectly to the user and the user's computer system. Malware includes viruses, trojans, worms, spyware etc.

Man in the middle (MITM) **Člověk uprostřed**

Attack in which an attacker is able to read, insert, and modify messages between two communicating parties without their awareness.

Management system **Systém řízení**

Set of interrelated or interacting elements of an organisation to establish policies and objectives and processes to achieve those objectives.

Manipulated Variable **Výstupní promněnná**

The value or condition that the control sendsto initiate a change in the value of the regulated variable.

Manipulation detection **Detekce manipulace**

Procedure to ascertain whether data were modified, either by accident or by design.

Manufacturing Execution System (MES) **Výrobní informační systém**

A system that uses network computing to automate production control and process automation. By downloading recipes and work schedules and uploading production results, an MES bridges the gap between control and operational level or between production and control systems.

Master Terminal Unit (MTU) **Master Terminal Unit**

*See **Control Server.***

Maximum acceptable outage (MAO) **Maximální přípustný výpadek**

Time, it would take for adverse impacts, which might arise as a result of not providing a product/service or performing an activity, to become unacceptable (see also a maximum tolerable period of disruption).

Maximum tolerable period of disruption (MTPD) **Maximální přijatelná doba narušení**

Time, it would take for adverse impacts, which might arise as a result of not providing a product/service or performing activities, to become unacceptable (see also maximum acceptable outage).

Mean Time Between Failures **Střední doba mezi poruchami**

Expected time between consecutive failures in a system or its component.

Mean Time To Repair **Střední doba opravy**

Expected or observed duration to return a malfunctioning system or component to normal operations.

Measures to protect privacy **Opatření ochrany soukromí**

Measures that treat privacy risks by reducing their likelihood or their consequences.

Message authentication **Ověření totožnosti zprávy**

Verification that message was sent by the alleged originator to the intended receiver and that this message was not changed in transmission. Verification of the identity of information source-sender of the message. Frequently, digital signature is used.

Message authentication code **Kód autentizace zprávy**

Bit string, which is a function of data (in an encrypted or plain form) and the secret key, and is attached to data in order to authenticate them.

Message authentication code (MAC) **Autentizační kód zprávy**

Code to check the integrity and secure the authentication of a message. It serves to protect against contingent or intended alterations or errors in the data file. The data file is encrypted by a block algorithm using a secret key (in CBC mode), a portion from the last block of this encrypted data is taken out, and this short code is denoted MAC.

Metadata **Metadata**

Metadata are data that provide information about other data.

Minimal disclosure **Minimání odhalení**

Principle of identity management to restrict the transfer of identity information to a third party to the minimum possible level required for a particular purpose.

Minimum business continuity objective (MBCO) **Minimální úroveň chodu organizace**

Minimum level of services and/or products that is acceptable to the organisation to achieve its business objectives during a disruption.

Modem **Modem**

A device used to convert serial digital data from an end device to an analogue signal then transmitted over a telephone network to another end device and decoded there.

Monitoring **Monitorování**

Determining the status of a system, a process or an activity. Note: To determine the status there may be a need to check, supervise or critically observe.

Monitoring means **Monitorovací prostředky**

Tools and means to monitor system operation.

Motion Control Network **Motion Control Network**

A specific network enabling the applications to control the movement of parts of specific industrial settings, including sequencing, speed control, regulation and incremental motion.

Multi-factor authentication **Více faktorová autentizace**

Authentication using two or more of the authentication factors.

National authority **Národní autorita**

State authority responsible for the issues of cyber security (guarantee).

National security council **Bezpečnostní rada státu**

Permanent working body of the government of the Czech Republic (CZE) for the coordination of security of CZE and preparation of proposals to implement them.

NATO computer incident response capability – Technical centre (NCIRT TC) **NATO CIRC – Technické centrum (NCIRC TC)**

NATO CIRC technical support centre – second level. It enables the capability to respond to incidents, monitor incidents, perform system recovery, and provides direct technical support and help to the operational and security management of the operational NATO information systems.

NATO Cooperative cyber defence centre of excellence **NATO CCD COE**

NATO centre for cooperation in cyber security (Filters tee 12, Tallinn 10132, Estonia, http://www.ccdcoe.org).

NATO Cyber defence management authority **NATO CDMA**

NATO authority to manage cyber defence with the aim of providing an umbrella and interconnections for existing capabilities of cyber defence within the Alliance.

Network **Síť**

Set of computer terminals (workstations) and servers which are mutually interconnected in order to exchange data and communicate.

Network address translation (NAT) **Překlad síťových adres**

The mechanism enabling access of several computers from a local network to the Internet under one public IP address. Computers from the local address are assigned so-called private IP addresses. The border element of such a local network provides for the translation of a private IP address to a public one. See also ***Private IP address****.*

Network administration **Administrace sítě**

Day-to-day servicing and management of infrastructure, focused on processes, maintenance and development of networks.

Network Behavior Anomaly Detection (NBAD) **Detekce anomálního chování sítě**

A solution for helping protection against zero-day attacks. NBAD is an integral part of network behaviour analysis, which offers security in addition to that

provided by traditional anti-threat applications such as firewalls, antivirus software and spyware-detection software.

Network integrity **Integrita sítě**

Functionality and operaoperability of interconnected networks of electronic communications, protection of these networks against failures caused by electromagnetic jamming or operational loading.

Network Interface Card (NIC) **Síťová karta**

A circuit board or card that is installed in a computer so that it can be connected to a network.

Network management **Správa sítě**

Process of planning, designing, implementing, operating, monitoring and maintaining a network.

Network of electronic communications **Síť elektronických komunikací**

Transmission systems, or as the case may be, communication and routing equipment and other devices, including elements of the network which are not active, which make for the transmission of signals over wire lines, by radio, optical or other electromagnetic devices, including satellite networks, fixed lines with commuted circuits or packets, and mobile ground networks, networks for the distribution of electrical energy in the extent to transmit signals, networks for radio and television broadcast and networks for cable television, regardless of the type of transmitted information.

Network sniffer **Síťový analyzátor**

Device or software used to capture information flowing in networks.

Nonconformity **Neshoda**

Non-fulfilment of a requirement.

Non-repudiation **Nepopiratelnost**

Ability to prove the occurrence of a claimed event or action and its originating entities.

Normal operation **Běžný provoz**

Operation where the entire set of algorithms, security functions, services or processes are available or configurable.

Object Linking and Embedding (OLE) for Process Control (OPC) **Object Linking and Embedding pro Procesní řízení**

A set of open standards developed to promote interoperability between disparate field devices, automation/control, and business systems.

Objective **Cíl**

Result to be achieved.

One-way function **Jednosměrná funkce**

Function with the property that it is easy to compute the output for a given input but it is mathematically infeasible to find an input for a given output.

One-way hash function **Jednosměrná hash funkce**

A function, which maps strings of bits to fixed-length strings of bits, satisfying the following two properties: for a given input, one and only one output can be derived mathematically; from a given output, it is mathematically infeasible to find a corresponding input.

Online service **Online služba**

A service which is implemented by hardware, software or a combination of these, and provided over a communication network. Online services include, for example, a search engine, online backup services, Internet-hosted email, and software as a service (SaaS).

Open communication system **Otevřený komunikační systém**

It represents (includes) a global computer network including all its functions and supported both by private companies and public institutions.

Open software foundation (OSF) **Open software foundation**

A not-for-profit organization founded in 1988 under the U.S. National Cooperative Research Act of 1984 to create an open standard for an implementation of the UNIX operating system.

Open-security environment (OSE) **Otevřené bezpečnostní prostředí**

Environment where data and source protection against accidental or intentional acts is achieved by using standard operational procedures.

Operating system **Operační systém**

Software which controls programme executions and which can offer various services, e.g. assignment of devices, scheduling, control of input and output and data administration. Examples of operating systems are the MS-DOS system, LINUX, UNIX, Solaris, and others.

Operational controls **Provozní opatření**

It is a process act by which a certain affair does not terminate; only some issues are taken care of to expedite matters. This differentiates it from a decision. It may have the form of a directive, order or other normative acts.

Operational documentation **Provozní dokumentace**

Documentation of the information system of public administration describing the functional and technological features of the information system.

Operational environment **Provozní prostředí**

Set of all software and hardware including the operating system and hardware platform required for the module to operate securely.

Operator of the information system of public administration. **Provozovatel / Správce informačního systému veřejné správy**

Subject performing at least some of the activities related to the information system. The administrator of the information system of public administration can commission other subjects unless prohibited by law.

Organisation **Organizace**

Person or group of people that has its own functions with responsibilities, authorities and relationships to achieve its objectives.

Organisational Measures **Organizační opatření**

Processes that collect and use the information to evaluate the performance of various organisational resources, as human, physical, financial ones, as well as of the organisation as a whole in the light of the organisational strategies and while doing so, they influence the behaviour of information resources during the implementation of organisational strategies.

Outage (large), Blackout **Výpadek proudu (rozsáhlý), blackout**

Widespread electrical power outage.

Outsource **Zajišťovat pomocí vnějších zdrojů, (outsourcovat)**

Make an arrangement where an external organisation performs part of an organisation's function or process

Outsourcing **Outsourcování**

Acquisition of services (with or without products) in support of a business function for performing activities using supplier's resources rather than the acquirer's.

Packet **Paket**

Block of data transferred in computer networks and using the technology of "packet switching". A packet consists of control data and user data. Control data contain information necessary for packet delivery (destination address, source address, checksums, and information on packet priority). User data contain those data items, which should be delivered to the target (destination addressee).

Padding **Vycpávka (Padding)**

Appending extra bits to a data string. For example, in a block cipher, the last block is filled up with these bits to the required size of the block.

Passive threat **Pasivní hrozba**

The threat of making access to data without actually changing the state of the data processing system or the computer network.

Password **Heslo**

String of characters used to authenticate an identity or to verify access authorisation.

Password cracker **Prolamovač hesel**

A programme designed to crack passwords, codes, keys.

Password verification data **Údaje pro ověření hesla**

Data that is used to verify an entity's knowledge of a specific password.

Patch **Záplata**

Update which removes a security problem or unstable behaviour of an application, expands its possibilities and enhances its performance.

Peer to peer (P2P) **Rovný s rovným**

This is a computer network where individual clients communicate directly. This model is primarily used in interchangeable networks. Total transmission capability grows as a rule with the growing number of users in this model. In the classic model client-server this is quite the reverse.

Penetration **Proniknutí / průnik**

Unauthorised access to a computer system, network or service.

Penetration testing **Penetrační testování**

Analysis of functions of a computer system and networks with the objective of finding out weak spots in computer security so that these could be removed.

Performance **Výkonnost**

Measurable result.

Peripheral equipment **Periferní zařízení**

Equipment controlled by a computer and able to communicate with it, e.g. input/output devices and auxiliary memory.

Personal data **Osobní údaje**

Any information relating to an identified or identifiable natural person (i.e. data subject); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Personal data breach **Porušení ochrany osobních údajů**

A breach of protection and security of personal data leading to the accidental or unlawful destruction, loss, alteration, disclosure or publication of personal data transmitted, stored or otherwise processed.

Personal identification number (PIN) **Osobní identifikační číslo / PIN**

Numeric code used to authenticate an identity.

Personally identifiable information (data) (PII) **Osobně identifikovatelné informace (údaje)**

Any information that can be used to identify the PII principal to whom such information relates, or is or might be directly or indirectly linked to a PII principal.

Pharming **Pharming (rhybaření)**

The fraudulent method used on the Internet to obtain sensitive data from the victim of the attack. The principle is an attack on DNS and rewriting the IP address, which results in redirecting the client to a false address of internet banking, email, social network, etc., after inserting the URL into the browser. These pages are as a rule indistinguishable from the real pages of a bank and even experienced users may not recognise this change (unlike the related technique of phishing).

Phishing **Phishing („rybaření“, „rhybaření“, „házení udic“)**

A fraudulent method having the objective of stealing the digital identity of a user, the sign-on names, passwords, bank account numbers and accounts etc. to subsequently misuse these (drawing cash from the account, unauthorised access to data etc.). Creation of a fraudulent message distributed mostly by electronic mail trying to elicit the mentioned data from the user. The messages may be

masqueraded to closely imitate a trustworthy sender. It may be a forged request from a bank whose services the user accesses with a request to send the account number and PIN for a routine check (use of the dialogue window purporting to be a bank window – so-called spoofing). Thus the fraudster tries to convince accessing persons that they are at the right address, whose security they trust (pages of electronic shops etc.). Also, very often credit card numbers and PINS are stolen in this fashion.

Phone phishing **Telefonní phishing**

Phishing technique, which uses a false voice automaton (Interactive Voice Response) with a structure similar to the original banking automaton ("For a change of password press 1, for connection to a bank advisor press 2"). The victim is usually asked in an email to call the bank for information verification. Here, sign-on is requested using a PIN or a password. Some automata subsequently transfer the victim to contact with the attacker playing the role of a telephone bank advisor, which allows for other possibilities for questions.

Photo Eye **Světelná závora**

A light-sensitive sensor that converts a light signal into an electrical signal, producing a binary signal based on an interruption of a light beam.

Phreaker **Phreaker**

Person doing "hacking" on the phone, using various tricks manipulating the services of telephone companies.

Phreaking **Phreaking**

Denotation for tapping into a somebody else's telephone line in distribution panels, public telephone booths or directly in the ground/below ground telephone lines and thanks to these: (1) it is possible to call anywhere free of charge, (2) surf the internet free of charge, and (3) listen to somebody else's telephone conversations. Payment for the call is of course at the cost of the victim (registered user of the line, or the telephone company). Tapping into a mobile network by using various methods or the manufacture of listening devices are also considered phreaking.

Physical access control **Fyzické řízení přístupu**

Use of physical mechanisms to enable control of access (e.g. placing the computer in a locked room). See ***Access Control****.*

Physical asset **Hmotný majetek / Fyzické aktivum**

Asset that has a tangible or material existence. Physical assets usually refer to cash, equipment, inventory and properties owned by the individual or organisation. Software is considered an intangible asset.

Piggyback entry — **Vstup přes autorizovaného uživatele**

Unauthorised access to the system using a legitimate link of an authorised user.

PII Principal — **Subjekt osobně identifikovantelných informací (údajů)**

A natural person to whom the personally identifiable information (PII) relates (see also data subject).

PII processor — **Zpracovatel PII**

Privacy stakeholder that processes personally identifiable information (PII) on behalf of and by the instructions of a PII controller.

Ping — **Ping**

Instrument used in computer networks for testing computer availability over IP networks. Ping measures the time of response and records the volume of lost data (packets).

Ping flood — **Zahlcení pingy**

*Simple **DoS** attack when the attacker floods the victim with requests "ICMP Echo Request" (ping). The attack is successful provided the attacker has a wider bandwidth than the victim, or, the attacker can cooperate with other attacker simultaneously. See **ICMP flood**.*

Ping of death — **Ping smrti**

*Type of an attack on a computer, which includes a dangerous **ICMP** packet sent in error e.g. a packet sent larger than the maximum size of IP packet which collapses the target computer, or, by sending the packet the attacker exceeds the maximum size of **IP** packets which results in the failure of the system.*

Pivoting — **Pivoting**

Use of a system that has been successfully attacked, to attack other systems in the shared network.

Plain text, clear text — **Prostý text, otevřený text**

Information that is not encrypted.

Plant — **Továrna / Závod**

The set of physical elements necessary to implement a particular production process, including many of the static components not controlled by the ICS. However, the operation of the ICS may impact the adequacy, strength, and durability of the plant's components.

Platform as a Service (PaaS) **Platforma jako služba**

The capability provided to the user to deploy onto the cloud infrastructure user-made or acquired applications created by programming languages, libraries, services, and tools supported by the user. The user does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.

Point of contact (PoC) **Kontaktní bod**

Defined organisational role or function serving as the coordinator or focal point of information concerning incident management activities.

Policy **Politika**

The overall intention and direction of an organisation, as formally expressed by its top management.

Port **Port**

It is used for communication using the TCP or UDP protocols. It defines the individual net applications running on one computer. It may take on values in the range 0 – 65535. For example, web pages are usually accessible on port 80, server to send out electronic mail on port 25, FTP server on port 21. These values may be changed, and with some network services, the administrators sometimes set other than normally used port numbers to deceive a potential attacker.

Port Knocking **Klepání na porty**

*Denotes a method in computer networks how to gain access from an untrusted computer into a computer or computer network protected by a **firewall**, without the need to sign on with the computer protected by a **firewall** and change the setting like an administrator. This way creates a semblance that the **firewall** is closed to untrusted computers and yet gives a chance of changing the setting by a special secret sequence. The method bypasses abuse of security errors in programmes serving permanently open ports.*

Port scanner **Port scanner**

Programme to test open ports.

Port Scanning **Skenování portů**

Using a programme to remotely determine which ports on a system are open (e.g., whether the system allows connections through these ports).

Port Trunking / Teaming **Port Trunking / Teaming**

Linked aggregation of several physical ports making up one logical channel.

Portal **Portál**

Information (content regions, pages, applications, and data from external sources) concentrated in one central place, which can be accessed using a web browser.

Potential electronic evidence **Potenciální elektronický důkaz**

Information or data, stored, or transmitted in binary form, for which it has not yet been determined, through the process of analysis, to be relevant to the investigation.

Predisposing Condition **Předpoklad (k něčemu)**

A condition that exists within an organisation, a mission/business process, enterprise architecture, or information system including its environment of operation, which contributes to (increases or decreases) the likelihood that one or more threats, once initiated, will result in undesirable consequences or adverse impact to organisational operations and assets, individuals, other organisations, or the state.

Pressure Regulator **Regulátor tlaku**

A device used to control the pressure of gas or liquid.

Pressure Sensor **Tlakový senzor**

A certain sensor that sends an electrical signal related to the pressure acting on it by its surrounding medium. Pressure sensors can also use differential pressure to obtain level and flow measurements.

Pretexting **Pretexting**

One kind of social engineering. It creates and uses fictitious screenplay with the objective of convincing the victim to perform the required action or to obtain the required information.

Pretty good privacy (PGP) **Dost dobré soukromí**

Mechanism/programme enabling encryption and signature of data. Most typically it is used for encrypting the content of messages (emails) and for providing these messages with an electronic signature.

Prioritised activities **Upřednostněné činnosti**

Activities that must be prioritised in the immediate aftermath of an incident to mitigate impacts

Priority call **Prioritní volání**

A phone call by specific terminals in the event of emergencies, which should be handled with priority by restricting public calls.

Privacy **Soukromí**

Privacy is the capability or right of an individual or group to retain information about themselves. Privacy is also the material or mental space of the subject.

Privacy (protection) stakeholder **Strana zúčastněná na (ochraně) soukromí**

A natural or legal person, public authority, agency or any other body that can affect, be affected by or perceive themselves to be affected by a decision or activity related to personally identifiable information (PII) processing.

Privacy breach **Porušení soukromí / Porušení zabezpečení osobních údajů**

(1) A state where personally identifiable information is processed in violation of one or more relevant privacy safeguarding requirements. (2) A breach of security leading to the accidental or unlawful destruction, loss, alteration, disclosure of, or publication of personal data transmitted or otherwise processed.

Privacy enhancing technology (PET) **Techniky zlepšující (ochranu) soukromí**

Measures of privacy protection, consisting of information and communication technology (ICT) measures, products, or services that protect privacy by eliminating or reducing personally identifiable information (PII) or by preventing unnecessary and undesired processing of PII, all without losing the functionality of the ICT system.

Privacy protection **Ochrana soukromí**

Specific choices made by a personally identifiable information (PII) principal about how their PII should be processed for a particular purpose

Privacy protection policy **Politika ochrany soukromí**

Overall concepts, rules and commitment, as formally expressed by the personally identifiable information (PII) controller related to the processing of PII in a particular setting.

Privacy protection principles **Zásady ochrany soukromí**

Set of principles governing the privacy protection of personally identifiable information (PII) when processed in information and communication technology systems.

Privacy risk **Riziko (ochrany) soukromí**

Effect of uncertainty on (protection of) privacy.

Privacy risk assessment **Posouzení rizik (ochrany) soukromí**

An overall process of risk identification, risk analysis and risk evaluation with regard to the processing of personally identifiable information (PII); see also data protection impact assessment.

Privacy safeguarding requirements **Požadavky na zabezpečení (ochrany) soukromí**

Set of requirements an organisation has to take into account when processing personally identifiable information (PII) with respect to the privacy protection of PII

Private IP address **Privátní IP adresa**

*Groups of **IP** addresses defined under RFC 1918 as reserved for use in internal networks. These IP addresses are not routed from the internet. Here are these ranges: 10.0.0.0 – 10.255.255.255, 172.16.0.0 – 172.31.255.255 and 192.168.0.0 – 192.168.255.255.*

Private key **Soukromý klíč**

A key in asymmetric cryptography, which belongs to a specific entity and should be known only to this entity. It is paired with a public key.

Privilege, Access right / Permission **Oprávnění, přístupové oprávnění**

Authorisation of a subject to access a resource.

Problem **Problém**

Primary cause of one or more incidents.

Procedure **Postup**

Specified method of executing an activity or process.

Process **Proces**

Set of interrelated or interacting activities, which transforms inputs into outputs.

Process Control **Procesní řízení**

A discipline devoted to architecture, mechanisms and algorithms that control the output of a specific process within the required limits. For this purpose, industrial automation tools are used.

Process control system **Řídicí systém výroby**

A system that serves to control and monitor the generation, transmission, storage and distribution of electric power, gas and heat together with the control of supporting processes.

Process Controller **Výrobní řídicí jednotka**

A type of computer system, typically rack-mounted, that processes sensor inputs, applies on them control algorithms, and issues actuator outputs.

Processing of personal data **Zpracování osobních údajů**

Any operation or set of operations on personal data or sets of personal data, whether or not performed by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Processing of PII **Zpracování osobně identifikovatelných údajů**

An operation or set of operations performed upon personally identifiable information (PII).

Processor of Personal Data **Zpracovatel osobních údajů**

A natural or legal person, public administration body or another subject that processes personal data for the controller.

Proficiency **Způsobilost**

The ability of an investigative team to achieve results equivalent to those of a different investigative team given the same sources of potential digital evidence.

Programmable logic controller (PLC) **Programovatelný logický automat**

A small industrial computer originally designed to perform the logic functions executed by electrical hardware (relays, switches and mechanical timer/counters). They have evolved into controllers with the capability of controlling complex processes, and they are used substantially in SCADA and DCS systems. In SCADA environments, PLCs are often used as field devices because they are more economical, versatile, flexible and configurable than special-purpose RTUs. Sometimes PLCs are implemented as field devices to serve as RTUs; in this case, the PLC is often referred to as an RTU.

Programme **Program**

Syntactic unit satisfying the rules of a certain programming language; it consists of descriptions (declarations) and commands or instructions necessary to fulfil some function or solve some task or problem.

Proof of identity, Evidence of identity **Průkaz totožnosti**

Identity information for an entity required for authentication of that entity. Identity evidence includes information related to a claimant that is needed for a successful authentication.

Protocol **Protokol**

Agreement or standard, which controls or enables a link, communication and data transfer among computers, in general among end devices. Protocols can be implemented by hardware, software, or a combination of both.

Protocol Analyser **Analyzátor protokolů**

*See **Network Sniffer***

Proximity Sensor **Senzor vzdálenosti**

A non-contact sensor with the ability to detect an item within a specified range.

Proxy Server **Proxy Server**

A server that services the requests of its clients by forwarding those requests to other servers.

Proxy trojan **Proxy trojan**

Masks other computers as infected. Enables the attacker to abuse the infected computer for an access to other computers in the network and thus aids the attacker to hide its identity.

Pseudonym **Pseudonym**

An alternative name of an entity, synonyms are alias and aka (also known as). Entity cannot be identified using pseudonym without additional information about connection between a pseudonym and an etity identity.

Pseudonymisation **Pseudonymizace**

The processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

Pseudo-random number generator (CPRBG) **Generátor pseudonáhodných čísel**

A deterministic programme which generates a statistically random sequence of numbers. As such programmes are deterministic, the generated sequence starts to repeat itself with a period. Input data for the pseudo-random generators are

random sequences called „random seed“, which uniquely determine the course of the programme (generator). Data obtained from an HW system (e.g., temperature, time) or an output sequence from a physical generator (TRNG) can serve as the „random seed“.

Public cloud service provider — **Poskytovatel služeb veřejného cloudu**

Party which makes cloud services available according to the public cloud model

Public domain software — **Software veřejné domény**

Software that has been placed in the public domain, in other words there is absolutely no ownership such as copyright, trademark, or patent.

Public information system — **Veřejný informační systém**

Information system providing services to the public and having relations to information system of the public administration.

Public IP address — **Veřejná IP adresa**

*The IP address that is routable on the **Internet**. Such an address is then accessible from the whole **Internet** network unless prohibited, for example, by **firewall** or router configuration.*

Public key — **Veřejný klíč**

A key of an entity's asymmetric key pair, which can be made public. A public key is paired with a private key.

Public key certificate — **Certifikát veřejného klíče**

Public key information of an entity signed by an appropriate certification authority and thereby protected against forgery.

Public key encryption — **Šifrování veřejným klíčem**

Encryption performed using an asymmetric algorithm.

Public Key Infrastructure (PKI) — **Infrastruktura veřejných klíčů**

This in cryptography denotes infrastructure for the management and distribution of public keys from asymmetric cryptography. PKI, thanks to the transfer of confidence, enables the use of unfamiliar public keys for the verification of electronic signature without having to verify each individually. The transfer of confidence can be implemented either using the certification authority (X.509) or by the trusted network (e.g. PGP).

Public sector portal — **Portál veřejné správy**

Information system created and operated with the intention of facilitating remote access to, and communication with, the necessary information from the public administration.

Public telecommunication network **Veřejná komunikační síť**

A network of electronic communications serving, wholly or predominantly to provide publicly available services of electronic communications, and which supports information transfer among the endpoints of the network, or a network of electronic communications through which radio and television broadcast are provided as a service.

Public telephone network **Veřejná telefonní síť**

A network of electronic communications to provide publicly available telephone services, and which allows for the transmission of voiced speech as well as other forms of communications, such as facsimiles and data transmissions, among the endpoints of the networks.

Publicly available electronic communications service **Veřejně dostupná služba elektronických komunikací**

Service of electronic communications from whose use no one may be a priori excluded.

Published cryptographic algorithm **Veřejně známý kryptografický algoritmus**

An algorithm, which has been published, is publicly available and based on open sources. Usually, it is a cryptographic standard to be used without any limitations. System security is based on a cryptographic key which not known (Kerckhoff's principle). It applies to symmetric and asymmetric encryption algorithms as well as other functions used in cryptography. These algorithms and functions keep being tested by the public against all sorts of attacks and if they withstand these, are considered secure. At the same time, a potential attacker has all the information for a targeted attack (except the cryptographic key). New types of attacks and an increase in computing power lead to an increase in the length of cryptographic keys and the adoption of new standards to keep these standards secure.

Rack **Rack / Rozvaděč**

A mechanical chassis electrically equipped and designed to attach and electrically connect units (cards) and ICS processors into a single functional unit (PLC/PAC).

Radio access network **Rádiová přístupová síť**

Part of a mobile telecommunication system that implements a radio access technology such as WCDMA or LTE to provide access for end-user devices to the

core network. Note: The radio access network resides between the end-user device and the core network. A mobile phone is an example of an end-user device.

Random number generator (RBG) **Generátor náhodných čísel**

An HW or SW device (or a combination of both) which generates a sequence of random numbers. These numbers are mutually independent, and it is impossible to predict the next number from the preceding ones. The generator can be based on a random physical phenomenon or a contingency processed by a mathematical algorithm. The quality of the random number generator is verified by statistical analysis. This quality is decisive in the generation of, for example, symmetric cryptographic keys, on whose randomness depends encryption security.

Random number, random bit **Náhodné číslo, náhodný bit**

A parameter varying in time whose value cannot be predicted for content or time.

Ransomware **Ransomware**

A programme, which encrypts data and offers to decrypt them after a ransom payment (e.g., virus, Trojan horse).

Real-Time **V reálném čase**

Pertaining to the performance: computation of certain results during the actual time that the related physical process is running, so that the results could be used to control the physical process.

Recovery point objective (RPO) **Bod obnovy dat**

Point to which information used by an activity must be restored to enable the activity to operate on resumption. Can also be referred to as "maximum data loss".

Recovery time objective (RTO) **Doba obnovy chodu**

A period of time following an incident within which product or service must be resumed or activity must be resumed or resources must be recovered.

Re-dial, Pharming crime ware **Přesměrovávače**

Programmes (subset of Malware) whose task is to redirect users to certain pages instead of those originally intended to be visited. On these pages there is an installation of other Crimeware (virus), or there is a substantial increase in the Internet connection fee (using telephone lines with a higher rate).

Redundancy **Redundance**

*The general meaning is redundancy, abundance. In **IT** it is used in the sense of backup. For example, a redundant (backup) power supply, redundant (backup) data.*

Redundant Control Server **Redundantní řidicí server**

A backup to the control server that maintains the current state of the control server to replace it without delay in case of outage.

Regional internet registry (RIR) **Regionální Internetový Registr**

The organisation looking after the assignment of public IP address ranges, autonomous systems in its geographical scope. There are five RIRs at present: RIPE NCC – Europe and Near East, ARIN – USA and Canada, APNIC – Asia – Pacific Region, LACNIC – Latin America, AfriNIC – Africa.

Registration authority **Registrační autorita**

An entity responsible for providing assured user identities to the certification authority.

Relay **Relé**

An electromagnetic device that interrupts an electrical circuit by physically moving conductive contacts. The resultant motion can be coupled to another mechanism such as a valve or breaker.

Release **Vydání, vydaná verze**

The aggregate of one or more new or changed configuration items which are put into the operational environment as the result of one or more changes.

Reliability **Spolehlivost**

Property of a system and its parts to perform its mission accurately and without failure or significant degradation.

Relying party **Relying party**

A server providing access to a secure software application.

Remote access **Vzdálený přístup**

A process of accessing network resources from another network, or from a terminal device, which is not permanently connected, physically or logically, to the network it is accessing.

Remote Access Point **Vzdálený přístupový bod**

Certain devices, areas and locations of a control network for remotely configuring control systems and accessing process data. E.g. using a mobile device to access data over a WLAN, or using a laptop and modem connection to remotely access an ICS system.

Remote Diagnostics **Vzdálená diagnostika**

Diagnostic activities conducted by individuals communicating externally to an information system security perimeter.

Remote Maintenance **Vzdálená údržba**

Maintenance activities conducted by individuals communicating external to an information system security perimeter.

Remote Network Monitoring (RMON) **Monitorování sítě na dálku**

RMON is a part of the MIB module contained in SNMP which contains the specification to monitor individual network nodes.

Remote Terminal Unit (RTU) **Vzdálená termínálová jednotka**

(1) A computer with wireless interfacing used in remote situations where communications via wire or optics are unavailable. Usually used to communicate with remote field equipment.
(2) A special purpose data acquisition and control unit designed to support DCS and SCADA remote stations. RTUs are field devices often equipped with network capabilities, which can include wired and wireless radio interfaces to communicate to the supervisory controller. Sometimes PLCs are implemented as field devices to serve as RTUs; in this case, the PLC is often referred to as an RTU.

Remote User **Vzdálený uživatel**

User at a site other than the one at which the network resources being used are located.

Replay, replay attack **Replay, replay útok**

Situation when a copy of a legitimate transaction (data sequence) is intercepted, repeatedly replayed by an unauthorised subject usually with illegal intent (e.g. to open a car with a central lock).

Request **Dotaz**

Request for information, in general as a formal request sent to a database or to a browser, or a signal from one computer to another, or to a server with the request for concrete information or data item.

Request for comment (RFC) **Request For Comment**

*It is used to denote standards describing internet protocols, systems and other items related to internet operation. For example, RFC 5321 describes the **SMTP** protocol for the exchange and processing of electronic mail.*

Request for change **Žádost o změnu**

Proposal to make a change of a service, element of a service or a system of service control.

Requirement **Požadavek**

Need or expectation that is stated, generally implied or obligatory.

Residual data **Zbytková data**

*Data left behind in a data medium after the erasure of a file or part of it. It need not be, however, only data left after the erasure of disc files; unwanted residual data can be left on the local computer, for example, even by work using a remote connection (**VPN**). It could be data collected (into a cache), for example, of an application.*

Residual risk **Zbytkové riziko**

Risk remaining after risk management (treatment).

Resilience of a system **Odolnost systému**

The ability of an organisation, system or computer network to withstand without any harm any attempt of disruption. The resilience of a system is its capability to operate reliably without regard to impacts from the outside. A system with such a capability behaves effectively if some of its parameters have a random character and are different from the supposed ones.

Review **Přezkoumání**

Activity undertaken to determine the suitability, adequacy and efficiency of the subject matter to achieve established objectives.

Review object **Předmět přezkoumání**

A specific centity, object, person and other, subject to review.

Review objective **Cíle přezkoumání**

Statement giving the reason for review.

Risk **Riziko**

(1) Danger, the possibility of damage, loss, failure.
(2) Effect of uncertainty on objectives.
(3) Possibility that a certain threat would utilise the vulnerability of an asset or group of assets and cause damage to an organization.

Risk acceptance **Přijetí rizika**

Informed decision to take a particular risk.

Risk analysis **Analýza rizik**

Process to comprehend the nature of risk and determine the level of risk.

Risk assessment **Posuzování rizika**

Overall process of risk identification, risk analysis and risk evaluation.

Risk attitude **Postoj k riziku**

Approach of an organisation towards assessing risk and, also, dealing with risk, sharing risk, taking over or refusal of risk.

Risk avoidance **Vyhnutí se riziku**

Decision not to allow an involvement into risk situations, or to exclude these.

Risk communication **Komunikace rizika**

Exchange or sharing of information between the decision-maker and other participating parties.

Risk criteria **Kritéria rizika**

Terms of reference against which the significance of risk is evaluated.

Risk estimation **Odhad rizika**

Process to determine values of probability and consequences of risk.

Risk evaluation **Hodnocení rizik**

Process of comparing the results of risk analysis with risk criteria to determine whether the risk and/or its magnitude is acceptable or tolerable.

Risk identification **Identifikace rizik**

Process of finding, recognising, and describing risks.

Risk management **Řízení rizik**

Coordinated activities to direct and control an organisation with regard to risks.

Risk management framework **Rámec řízení rizik**

(1) Set of components providing the fundamentals and organisational arrangement for the design, implementation, monitoring, re-analysis and continuousl improvement of risk management in the whole organisation. (2) A controlled process that integrates information security and risk management activities into the system development life cycle.

Risk management plan **Plán řízení rizik**

Scheme in the framework of risks specifying access, parts of management and sources to be used for risk management.

Risk management policy **Politika řízení rizik**

Statement on the overall intentions and direction of an organisation related to risk management.

Risk management process **Proces řízení rizik**

Systematic application of management policies, procedures and practices to the activities of communicating, consulting, establishing the context and identifying, analysing, evaluating, treating, monitoring and reviewing risk.

Risk owner **Vlastník rizika**

Person or entity with the accountability and authority to manage a risk.

Risk profile **Profil rizik**

Description of any set of risks.

Risk reduction **Redukce rizik**

Activity to lower the probability and lessen negative consequences, or both of these parameters linked to risk.

Risk retention **Podstoupení rizik**

Accepting the burden of a loss or benefit from profit ensueing from a certain risk.

Risk source **Zdroj rizika**

Element, which either alone or in combination with other elements, has the internal capability to cause a risk.

Risk transfer **Přenos rizik**

Sharing of costs with another party or sharing of benefits from profit flowing from risk.

Risk treatment **Zvládání rizika, ošetření rizika**

Process to modify (change) risk.

Role **Role**

Aggregate of specified activities and necessary authorisations for a subject operating in the information or communication system.

Role-based access control (RBAC) **Řízení přístupu dle rolí**

Access control based on access permissions to objects, which are assigned as attributes to specific roles.

Rootkit **Rootkit**

Programmes making it possible for insidious software to mask its presence in a computer. Thus they can hide from the user selected running processes, files on disc or other system data. They exist for Windows, LINUX and UNIX.

Router **Směrovač, router**

A network device that is used to establish and control the communication between different networks by selecting paths or routes based upon routing protocols and algorithms. Common uses for routers include connecting a LAN to a WAN and connecting MTUs and RTUs to a long-distance network medium for SCADA communication.

Safety Instrumented System (SIS) **Bezpečnostní přístrojový systém (SIS)**

A system that is composed of sensors, logic solvers, and final control elements whose purpose is to take the process to a safe state when predetermined operational conditions are violated. Often also called emergency shutdown system (ESS), safety shutdown system (SSD), and safety interlock system (SIS).

Sandbox **Sandbox**

Security mechanism serving to separate running processes from the operating system proper. It is used, for example, for testing suspicious software.

Sanitize **Vyčistit**

A process to remove information from media such that data recovery is not possible at a given level of effort.

SCADA **SCADA**

(1) Supervisory control and data acquisition; (2) Cyber security of the industrial controlling systems.

SCADA server / Master Terminal Unit (MTU) **SCADA server / Master terminal unit**

A device (master) that controls RTU and PLC placed in production (slave).

Scam **Podvod**

Fraud or confidence trick.

Script **Skript**

Set of instructions written in some formal language, which control the workings of devices, programme or system.

Secret (proprietary) algorithm **Tajný (proprietární) algoritmus**

An algorithm which is kept secret. Its author and guarantor can be a state institution, and it may be targeted for use exclusively for state bodies. However, the owner of the proprietary algorithm can be a private company which developed it and uses it in its products. The security of these algorithms may be evaluated by a state institution or an independent laboratory and is usually attested to by a certificate. Even these algorithms can be based on standards. A potential enemy has no information about the algorithm for a targeted attack.

Secret key **Tajný klíč**

An encryption key used in symmetric cryptography. It is used both to encrypt and decrypt data. It is a (shared) secret to be shared by any party authorised to encrypt and decrypt data. This is the reason why the key must be kept secret – hence secret key.

Sector criteria **Odvětvová kritéria**

Technological or operational values to determine an element of critical infrastructure in the sectors of energy, water management, food and agriculture, health, transport, communication and information systems, financial market and currencies, emergency services and public administration.

Secure shell (SSH) **Secure shell**

A protocol that provides secure remote login utilising an insecure network.

Secure socket layer (SSL) **Secure socket layer**

*Protocol or a layer inserted between the transport layer (e.g. **TCP/IP**) and the application layer (e.g. **HTTP**) which enables communication security by encryption and authentification of the communicating parties.*

Security **Bezpečnost**

Property of an element (e.g. an information system) which is at a certain level protected against losses, or also a state of protection (at a certain level) against losses. IT security covers protection of confidentiality, integrity and availability during processing, storage, distribution and presentation of information.

Security account manager **Správce zabezpečení účtů**

Administrator for securing the accounts in the Windows operating system, e.g. a database, where user passwords are kept (passwords in Windows NT operating system may be kept, for example, in the directory c:\\winnt\repair and c:\\winnt\config).

Security aims **Bezpečnostní cíle**

State of security which the given system or product has to reach.

Security assurance **Bezpečnostní dohled**

Control role, which verifies whether the security objectives are or will be met.

Security audit **Bezpečnostní audit**

Independent revision and analysis of records in the data processing system as well as activities for testing of the suitability of system controls, checking compliance with accepted security policy and operational procedures, detection of security infringements and recommendation for any indicated changes in the control, security policy and procedures. Independent testing of the information system activity and records thereof. The objective is to determine if checks are appropriate if there is compliance with security policy, the recommendation of eventual changes in the system of countermeasures. As a rule, it is done by an external or an internal auditor.

Security authority **Bezpečnostní autorita**

The entity accountable for the administration of security policy within the security domain.

Security category **Bezpečnostní kategorie**

Grouping of sensitive information used when controlling data access.

Security classification **Bezpečnostní klasifikace**

The determination which level of protection for data or information is required before access, together with noting this level of protection.

Security clearance **Bezpečnostní prověření**

Clearance given to an individual for accessing data or information on or below the specified security level.

Security domain **Bezpečnostní doména**

A group of users and systems subject to a common security policy.

Security event **Bezpečnostní událost**

Event, which may result in or cause the infringement of information systems and technologies and rules defined for the protection (security policy).

Security filter **Bezpečnostní filtr**

Trusted computer system enabling security policy for data passing through the system.

Security gateway **Bezpečnostní brána**

Point of connection between networks, or between subgroups within networks, or between software applications within different security domains intended to protect a network according to a given security policy.

Security incident **Bezpečnostní incident**

Infringement or an imminent threat of infringement, of security policies, security principles or standard security rules of operation for the information and communication technologies.

Security incident management **Zvládání bezpečnostních incidentů**

Actions of detecting, reporting, assessing, responding to, dealing with, and learning from information security incidents.

Security information and event management (SIEM) **Management bezpečnostních informací a událostí**

A system whose task is to acquire, analyse and correlate data – events in the network. SIEM systems combine the methods of detection and analysis of

abnormal events in the network, provide information usable for network management and operated services.

Security level **Bezpečnostní úroveň**

Combination of a hierarchic security classification and security category, representing sensitivity of an object or security clearance of an individual.

Security Management Centre (SMC) **Středisko správy klíčů**

Organisation body that ensures the management of cryptographic keys and the configuration of cryptographic devices in a network. The centre generates cryptographic keys for the cryptographic devices in a network, provides for their electronic distribution and implements strategy for communication of cryptographic devices in the network.

Security manager **Bezpečnostní manažer**

Employee role to act as a guarantee for IT security with the definition of responsibilty and authority.

Security measures **Bezpečnostní opatření**

The management, operational, and technical measures (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and information in it.

Security measures-countermeasures **Bezpečnostní opatření – protiopatření**

An action, device, procedure, or technique that reduces a threat, vulnerability, or an attack:
(1) by eliminating or preventing it,
(2) by minimising the harm it can cause,
(3) or by discovering and reporting it so that corrective action can be taken.

Security measures-safeguards **Bezpečnostní opatření – zabezpečení**

Protective measures to ensure security requirements put on the system. May vary in character (physical protection of equipment and information, personnel security – checking of employees, organisational measures – operational rules, and similar).

Security Plan **Plán bezpečnosti**

A formal document that provides an overview of the security requirements for the information system and describes the security controls in place or planned for meeting those requirements.

Security policy **Bezpečnostní politika**

Rules, directives and procedures that govern the management, protection and distribution of information assets, including sensitive information, within an

organisation and its systems, particularly those which impact the systems and their elements.

Security policy of an organisation **Bezpečnostní politika organizace**

Set of security rules, procedures and recommendations for an organisation.

Security policy of network **Bezpečnostní politika sítě**

Set of statements, rules and examples that explain an organisation's approach to the use of its network resources, and specify how its network infrastructure and network services should be protected.

Security requirements **Bezpečnostní požadavky**

Requirements put on the information system, which follow from laws, instructions, legal amendments, binding standards, internal regulations of an organisation; environment where the system operates and the mission it fulfills; necessary for ensuring confidentiality, availability and integrity of information processed in the system.

Security roles **Bezpečnostní role**

Defined roles in accordance with the law on cyber security (examples: committee to manage cyber security, cyber security manager, cyber security designer, guarantor of assets) which define responsibilities linked to cyber security management.

Security software disabler **Security software disabler**

*It blocks software to secure the **PC (Firewall, Antivirus)**.*

Security standards **Bezpečnostní standardy**

Set of recommendations and general principles to define, maintain and improve information security inside an organisation.

Security vulnerability **Bezpečnostní zranitelnost**

Intentional error or unintended defect or software error in general or in the firmware of the communication infrastructure equipment, which may be used by a potential attacker for harmful activity. These vulnerabilities are either known or published but yet untreated by the manufacturer, or hidden and undetected. In case of hidden vulnerabilities, it is important whether these are detected sooner by the attacker, manufacturer, security analyst or user. Security vulnerabilities are therefore potential security threats. Security vulnerabilities can be eliminated by consequential security patches for the system.

Sensitive data **Citlivá data**

Protected data having fundamental importance for the operation of an organisation. Its leakage, abuse, unauthorised alteration or unavailability would

mean damage to the organisation, or, as the case may be, the organisation would be unable to meet its objectives.

Sensitive information **Citlivá informace**

Information which, on the basis of a decision by the relevant authority, must be protected, because access to it, modification, destruction, or loss would cause a substantial damage to someone or something.

Sensitivity **Citlivost**

Measure of importance assigned to information by the owner of the information, describing the need for protection.

Sensor **Senzor, čidlo**

A device that measures or reads some specific physical property or value and converts it into an electrical or optical signal, which can be evaluated by an observer or instrument.

Server **Server**

Computer system or programme that provides services to other computers or programmes.

Server cluster **Serverová farma**

Group of network servers used to increase the efficiency of internal processes by distributing load among individual linked components to speed up computing processes by using the power of more servers. When one server in the farm fails, another one can replace it.

Service **Služba**

(1) Activity of the information system meeting the given requirements of an authorised subject related to the function of the operating system. (2) Means of delivering value to users by facilitating results users want to achieve without the ownership of specific physical or logical resources and the risks related to ownership.

Service component **Prvek služby**

Independent component of a service which, when united with other components provides the whole service.

Service continuity **Kontinuita služeb**

Capability to manage risks and events which could seriously impact services, with the objective of providing continuous services at the agreed levels.

Service level agreement (SLA) **Smlouva o úrovni služeb**

A contract between the service provider and the service recipient that defines the parameters of technical support and the parameters of the service provided,

including how they are measured and the consequences that result from the service provider's failure to comply with them.

Service level declaration (SLD) **Prohlášení o úrovni služeb**

*Specification of the offered services, which may change on the basis of individual agreements according to the actual needs of individual customers. Hence, a more detailed SLA. See **SLA**.*

Service management **Řízení služeb**

Set of capabilities and processes to manage and control the activities and sources of the service provider for the design, handover, delivery and improvement of services so that the requirements placed on them be met.

Service pack **Aktualizační balík**

Collection (pack) of several updates, which could all be installed at the same time.

Service provider **Poskytovatel služby**

Any natural or legal person providing any of the services of the information society.

Service request **Žádost o službu**

Request for information, advice, access to service, or for a previously agreed change.

Service requirement **Požadavky na službu**

Needs of customers and users of services, including requirements for the service level and the needs of a service provider.

Service set identifier (SSID) **Service set identifier**

*Unique identifier (name) of every wireless (**WiFi**) computer network.*

Servo Valve **Servo ventil**

An actuated valve whose position is controlled by an actuator.

Sexting **Sexting**

Electronic distribution of text messages, photographies or videos with sexual content. These materials often originate in partner relations. Such materials, however, may represent a risk that one partner, out of various motives, would publish photographies or videos of the other partner.

Shared secret **Sdílené tajemství**

Secret used in authentication of an entity that is known only to the entity and the verifier.

Shareware **Shareware**

Freely distributed software protected by copyright. In case the user decides to use this software longer than the author permits, the user is obliged to satisfy conditions for use. These can be, for example, payment of a certain financial amount, user registration, etc.

Sharing **Sdílení**

Possibility to have a portion at the same time of one or more information sources, memory or devices.

Shred **Skartovat**

Destroy the medium by cutting or breaking it into small pieces.

Side-channel attack **Útok postranním kanálem**

An attack based on information gained from the physical implementation of a cryptosystem, rather than on the brute force or theoretical weaknesses in the underlying algorithm. A side-channel attack may use, for example, timing information, power consumption, or electromagnetic emissions.

Signing **Podepisování**

Signature generation process that takes a message and a signing key of a signer to produce a signature.

Simple mail transfer protocol (SMTP) **Simple mail transfer protocol**

Internet protocol for the transmission of messages of electronic mail. It describes communication among mail servers.

Simple Network Management Protocol (SNMP) **Simple Network Management Protocol**

The basic TCP/IP protocol for network management. Network administrators use SNMP to monitor and map network availability, performance, and error rates.

Simulation **Simulace**

Use of a data processing system to extract selected properties in the behaviour of a physical or abstract system.

Single Loop Controller **Řídicí jednotka s jednou smyčkou**

A controller that controls a very small or critical process.

Single-sign-on identity, SSO identity **Jednotná identita**

Identity that includes a single identity assertion that can be verified by a relying party in multiple domains.

Smart Grid **Inteligentní síť**

A power electrical and communications network that allows real-time control of power generation and consumption, both locally and globally.

Sniffer **Sniffer**

Programme for the eavesdropping of all the protocols which a computer receives/sends (it is used, for example, for eavesdropping of access names or passwords, numbers of credit cards).

Social engineering **Sociální inženýrství**

Act of purposeful manipulation of people into performing particular actions or divulging confidential information.

Social network **Sociální síť**

An interconnected group of people who interact. It is formed by interests, family ties or other reasons. This idea is at present often used in connection with internet and the onset of webs which are directly targeted at social networks (Facebook, Lidé.cz etc.), social networks can also form in interest communities around certain web sites, for example at their forums.

Software **Software (programové vybavení)**

Set of programmes used in a computer which execute data processing or a concrete task. The software can be further subdivided into a) system software – input/output devices, operating systems or graphics operation systems; b) application software – applications, simple utilities or complex programming systems; c) firmware – hardware control programme.

Software as a Service (SaaS) **Software jako služba**

The capability provided to the consumer to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g. web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

Software piracy **Softwarové pirátství**

Unauthorised use, copying or distribution or software.

Spam **Nevyžádaná pošta**

Unsolicited mail such as commercials, or another unsolicited message, usually of a commercial character, which is distributed on the Internet. Most often these are offers for aphrodisiacs, medicaments or pornography. Unless the system is adequately protected, unsolicited mail can make up a substantial part of the electronic correspondence.

Spamming **Hromadné rozesílání nevyžádané pošty**

Mass distribution of unsolicited messages by electronic means – most often by electronic mail.

Spanning Tree Protocol (STP) **Protokol kostry grafu**

The Spanning Tree Protocol (STP) is a network protocol that ensures a loop-free topology for any bridged Ethernet local area network. The basic function of STP is to prevent bridge loops and the broadcast radiation that results from them. Spanning tree also allows a network design to include spare (redundant) links to provide automatic backup paths if an active link fails, without the danger of bridge loops, or the need for manual enabling/disabling of these backup links.

Spear phishing **Spear phishing (rybaření oštěpem)**

*More sophisticated attack than **Phishing,** which uses prior obtained information about the victim. Thanks to a more focused targeting on a concrete user this method attains higher effect than a standard attack of the **Phishing** type. See **Phishing**.*

Spoofing **Úmyslné oklamání, podvržení**

Activity with the objective of deceiving (misleading) a user or operator usually by sporting a false identity.

Spyware **Spyware**

The programme, which secretly monitors the behaviour of an authorised computer or system user. The findings are sent by these programmes continuously (e.g. at every startup) to the subject which created the programme or distributed it. Such programmes are frequently installed on the target computer together with another programme (utility, computer game). However, they bear no relation to it.

SQL injection **SQL injection**

Injection technique, which abuses security errors occurring in the database layer of an application. This security error manifests itself by infiltrating unauthorised characters into an SQL command of an authorised user, or by taking over user access, to execute the SQL command.

State of cyber danger **Stav kybernetického nebezpečí**

Under cyber danger, we understand such a state when there is a large measure of danger to information security in information systems or security of services or electronic communications.

Statement of applicability **Prohlášení o aplikovatelnosti**

Documented statement describing the objectives of measures and the measures, which are relevant and applicable for the ISMS of a given organisation. From the point of view of the Cyber Security Ordinance, a documented statement containing an overview of the security measures required by this Ordinance that (a) have not

been applied, including justification, (b) have been applied, including the method of implementation.

Statistical Process Control (SPC) **Statistické řízení procesů**

The use of statistical techniques to control the quality of a product or process.

Steady State **Ustálený stav**

A state when a specific property, such as value, speed, periodicity, or amplitude, exhibits only negligible change over an arbitrarily long period.

Stealth **Obtížná zjistitelnost**

Prevention or limitation of object's identification.

Storage Area Network (SAN) **Síť uložiště**

Network whose primary purpose is the transfer of data between computer systems and storage devices and among storage devices. Note: A SAN consists of a communication infrastructure, which provides physical connections, and a management layer, which organizes the connections, storage devices, and computer systems so that data transfer is secure and robust.

Stream Cipher **Proudová šifra**

Symmetric encryption system with the property that the encryption algorithm involves combining a sequence of plaintext symbols with a sequence of keystream symbols one symbol at a time, using an invertible function. Two types of stream cypher can be identified: synchronous stream cyphers and self-synchronous stream cyphers, distinguished by the method used to obtain the keystream.

Structure text **Structure text (strukturovaný text)**

IEC 61113-3 PLC programming language. It is most similar to traditional programming languages. This is a classical representation of syntactic composite commands.

Structured query language (SQL) **SQL**

Standard query language used to work with data in relational databases.

Stuxnet **Stuxnet**

Computer worm created to attack industrial control systems of the SCADA type used to control large industrial enterprises, for example, factories, power generating plants, product lines and even military objects.

Subject **Subjekt**

In computer security, an active entity which can access objects.

Subject of critical infrastructure **Subjekt kritické infrastruktury**

The operator of an element of critical infrastructure; if it is an operator of an element of the European critical infrastructure, the operator is considered to be a subject of the European critical infrastructure.

Subnet **Podsíť**

Segment of a network that shares a common address component.

Supervisory Control **Dispečerské řízení**

Control process when the output of one control unit or computer is used as input to another control unit. See Control Server.

Supervisory control and data acquisition (SCADA) **Dispečerské řízení a sběr dat**

A computer system for dispatcher control and data acquisition. It could be industrial control systems or computer systems for monitoring and process control. The processes could be industrial ones (e.g. electrical energy generation, manufacture and purification of fuel), infrastructural (e.g. treatment and distribution of drinking water, taking away and purification of sewage, oil and gas pipes, civilian systems of antiaircraft defence – sirens, and large communication systems), and facilities (e.g. airports, railway stations and hubs).

Supplier **Dodavatel**

Organization or an individual that enters into agreement with the acquirer for the supply of a product or service. Note: Other terms commonly used for supplier are contractor, producer, seller, or vendor. The acquirer and the supplier can be part of the same organization. Types of suppliers include those organizations that permit agreement negotiation with an acquirer and those that do not permit negotiation with agreements, e.g. end-user license agreements, terms of use, or open source products copyright or intellectual property releases.

Supply chain **Dodavatelský řetězec**

Set of organizations with linked set of resources and processes, each of which acts as an acquirer, supplier, or both to form successive supplier relationships established upon placement of a purchase order, agreement, or other formal sourcing agreement. Note: A supply chain can include vendors, manufacturing facilities, logistics providers, distribution centres, distributors, wholesalers, and other organizations involved in the manufacturing, processing, design and development, and handling and delivery of the products, or service providers involved in the operation, management, and delivery of the services. The supply chain view is relative to the position of the acquirer.

Symmetric Algorithm **Symetrický algoritmus**

Encryption algorithm which uses the same cryptographic key for both encryption and decryption. This key must be available only to the sender and the recipient, and this is why this key is denoted as a „secret key".

Symmetric Cryptography / Cryptographic technique **Symetrická kryptografie**

A cryptographic technique that uses the same secret key for both the originator's and the recipient's transformation. Note: Without knowledge of the secret key, it is computationally infeasible to compute either the originator's or the recipient's transformation.

SYN-cookies **SYN-cookies**

*Element of defence against a flooding by packets in the **TCP** protocol with the attribute **SYN**. See **SYN-Flood**.*

SYN-flood **SYN-flood**

Cyber attack (Denial of Service type) on a server by flooding with packets in the TCP protocol. The attacker sends a flood of TCP/SYN packets with a forged heading of the sender. The server accepts every such packet as a normal request for a connection. The server then sends out the SYN-ACK packet and waits for the ACK packet. This however never arrives as the heading of the sender was forged. Such a semi-open request blocks out, for some time, other legitimate requests for a connection. See DoS, DDoS, SYN-cookie.

System administrator **Správce systému**

Person responsible for the management and maintenance of a computer system.

System Integrity **Integrita systému**

Quality of a data processing system fulfilling its operational purpose and at the same time preventing unauthorised users from making changes in resources or from using the resources or from improper use of these. Property that a system performs its intended function without disruption, without intentional or accidental non-automated system manipulation.

Tampering **Manipulování**

Act of deliberately making or allowing change(s) to digital evidence (i.e. intended or purposeful spoliation).

TCP SYN flood **Zahlcení TCP SYN**

*Type of a **DDoS** attack, it sends a flood of **TCP/SYN** packets with a forged heading of the sender. Each such packet is accepted by the server as a normal request for a connection. Server then sends out a **TCP/SYN-ACK** packet and waits for **TCP/ACK**. This however never arrives as the user heading was forged. Thus a half-open request blocks, for some time, other legitimate requests for a connection.*

Technical Measures **Technická opatření**

The security measures or countermeasures for an information system that are primarily implemented and executed by the information system through mechanisms contained in the hardware, software, or firmware components of the system.

Temperature Sensor **Teplotní sensor, čidlo**

A sensor that reads the temperature of the environment and issues an electrical signal related to its temperature.

TEMPEST **TEMPEST**

Codename by the US National Security Agency to secure electronic communications equipment from compromising emanations, which, if intercepted and analysed, may disclose the information transmitted, received, handled, or otherwise processed.

TERENA **TERENA**

Trans-European Research and Education Networking Association, a European international organisation supporting activities in the area of internet, infrastructures and services in the academic community.

TF-CSIRT **TF-CSIRT**

*International forum enabling the cooperation of **CSIRT** teams on a European level. It is divided into two groups – a closed one, which is open only to accredited teams, and an open one, which is accessible to all parties interested in the **CSIRT** teams' work. TF-CSIRT is one of the activities of the **TERENA** international organisation. Working group TF-CSIRT meets usually several times per year.*

Third party **Třetí strana**

Person or organisation independent both of the person or the organisation which submits the object to be judged for compliance (product, service) and also independent of the purchaser of the object.

Threat **Hrozba**

Potential cause of an unwanted incident, which may result in damage to a system or organisation.

Threat agent **Původce hrozby**

Originator and/or initiator of deliberate or accidental man-made threats.

Threat analysis **Analýza hrozeb**

Analysis of activities and events, which could negatively affect IT service quality (system of data processing and transfer) and/or data proper.

Threat Event **Událost hrozby**

An event or situation that has the potential for causing undesirable consequences or impacts.

Threat Source **Zdroj hrozby**

The intent and method targeted at the intentional exploitation of a vulnerability or a situation or method that may accidentally trigger a vulnerability.

Time bomb **Časovaná bomba**

Logical bomb activated at a predetermined time.

Time-stamp **Časové razítko**

Time variant parameter which denotes a point in time with respect to a common time reference.

Time-stamping authority (TSA) **Autorita časového razítka**

Trusted third party trusted to provide a time-stamping service.

Time-stamping service **Služba časového razítka**

Service providing evidence that a data item existed before a certain point in time.

Top level domain (TLD) **Doména nejvyšší úrovně**

This is the internet domain at the highest level in the tree of internet domains. In the domain name, top-level domain is given at the end (e.g. in nic.cz, CZ is the top level domain). Top-level domains are fixed by the internet standards organisation IANA:
a) National TLD (country-code TLD, ccTLD) unites domains in one country. Their name has two letters, with exceptions corresponding to country code per ISO 3166-1, e.g. CZ for the Czech Republic;
b) Generic TLD (generic TLD, gTLD) is common for a given type of subjects (e.g. aero, biz, com, info, museum, org,...) not tied to one concrete country (with exceptions TLD mil and gov which out of historical reasons are assigned for military and government computer networks in the U.S.A.);
c) Infrastructure TLD used for the internal mechanisms of the internet. At present, there is just one such TLD: arpa, used by the DNS system.

Top management **Vrcholové vedení**

A person or a group of persons who lead the organisation at the highest level.

Topology **Topologie**

Topology is a qualitative geometry describing positions of individual elements (for example: communication nodes).

TOR (anonymity network) **TOR (anonymní síť)**

A free software for enabling anonymous communication, oftenly used to access DarkNet. The name is an acronym derived from the original software project name The Onion Router.

Torrent **Torrent**

*A file with the extension .torrent, which contains information about one or more files to be downloaded. See **BitTorrent**.*

Traffic analysis **Analýza datového provozu / komunikace**

Simple and advanced mathematical and visual methods for the analysis of data traffic TCP/IP in a computer network.

Transition **Přechod**

Activity related to a shift of new or altered service into or out of the operational environment.

Transmission control protocol (TCP) **Transmission control protocol**

*A basic protocol from the protocol set of the **Internet**; more precisely it represents the transport layer. Using the TCP, applications on interconnected computers can link up and transmit data over the links. The protocol guarantees a reliable delivery as well as delivery in the right order. TCP also differentiates data for multiple concurrently running applications (e.g. a web server and email server) running on the same computer. TCP is supported by many of the application protocols and applications popular on the Internet, including **WWW**, email and **SSH**.*

Transport layer security (TLS) **Bezpečnost transportní vrstvy**

*A cryptographic protocol that provides communication security over the Internet. It uses asymmetric cryptography for authentication of key exchange, symmetric encryption for confidentiality and message authentication codes for message integrity. Several versions of the protocols are in widespread use in applications such as web browsing, electronic mail, Internet faxing, instant messaging and voice-over-IP (**VoIP**).*

Transport layer security (TLS) **Transport layer security**

*A cryptographic protocol that provides communication security over the Internet. They use asymmetric cryptography for authentication of key exchange, symmetric encryption for confidentiality and message authentication codes for message integrity. Several versions of the protocols are in widespread use in applications such as web browsing, electronic mail, Internet faxing, instant messaging and voice-over-IP (**VoIP**).*

Triple DES **3DES**

A block symmetric encryption algorithm based on the triple application of the DES standard. It could be used in the form of EDE (K1, K2, K3) using key lengths of 168 bits or (K1,K2,K1) with the key length of 112 bits.

Trojan horse, trojan **Trojský kůň**

A programme, which performs a useful function on the surface, but in reality, also has some hidden harmful function. The trojan horse does not replicate itself; it is distributed thanks to the visible utility it provides.

Trusted computer system **Důvěryhodný počítačový systém**

Data processing system having sufficient computer security to allow for a concurrent access to data to users with different access rights and to data with different security classification and security categories.

Trusted introducer **Trusted introducer**

*The authority uniting European security teams of the type CERT/CSIRT. At the same time, it also helps in creating the CERT/CSIRT teams and provides for their accreditation and certification. It is operated by the TERENA organisation. See **TERENA.***

Trusted third party (TTP) **Důvěryhodná třetí strana**

Security authority, or its agent, trusted by other entities with respect to security-related activities.

UDP flood **Zahlcení UDP**

*A type of an attack using the User datagram protocol (**UDP**). The attacker sends out an unspecified number of packets to a random port of the system of the victim. Receiving system of the victim is unable to determine which application requested such a packet, which generates an ICMP packet of undeliverabilty of the **UDP** packet. If more **UDP** packets arrive in the receiving port of the victim, the system may collapse.*

Unauthorised Access **Neautorizovaný přístup**

A logical or physical access without permission to a network, system, application, data, or other resources.

Unidirectional Gateway **Jednosměrná brána**

A device consisting of hardware and software. The hardware permits a unidirectional data flow from one network to another, while data transfer in the opposite direction is physically impossible. The software part replicates databases and emulates protocol servers and devices.

Uniform resource locator (URL) **Uniform resource locator**

Source identifier describing the location of a concrete source, including a protocol, serving to link to this source. The best known such an example is http://www.somedomain.somewhere.

Universal unique identifier (UUID) **Universální unikátní identifikátor**

*An identifier standard used in software construction, standardised by the Open Software Foundation (**OSF**) as part of the Distributed Computing Environment (**DCE**).*

URL trojan **URL trojan**

*It redirects infected computers connected via the dial-in Internet connection to more expensive rates. See **Dialer** and **Trojan Horse**.*

User **Uživatel**

Any natural or legal person using a service of the information society in order to look for, or make access to, information.

User datagram protocol (UDP) **User datagram protocol**

An Internet networking protocol for unconnected communications (RFC 768).

User identification / User ID **Identifikace uživatele / ID uživatele**

Character string or a formula used by a data processing system for user identification.

User profile **Uživatelský profil**

Description of a user typically used for access control. It may include data such as user ID, user name, password, access rights and other attributes.

Validation **Potvrzení správnosti**

Confirmation, through the provision of objective evidence, that the requirements for a specific intended use or application have been fulfilled. Note 1 to entry: Validation is carried out on a process to ensure that it is fit for purpose, i.e. to ensure that the process, as implemented, produces expected results in a consistent, repeatable, and reproducible manner.

Valve **Ventil**

A mechanical device regulating the flow of fluids (gases, fluidised solids, slurry, etc.) in piping. It may interrupt the flow, regulate its volume and direct it to another branch of the system. In the Czech mechanical engineering terminology, the vent also includes taps, slide valves and flap valves.

Verification **Prověření**

A demonstrable confirmation that specified requirements have been fulfilled.

Virtual asset **Virtuální aktivum**

Representation of an asset in the Cyberspace. Note: In this context, currency can be defined as either a medium of exchange or a property that has value in a specific environment, such as a video game or a financial trading simulation exercise.

Virtual currency **Virtuální měna**

Monetary virtual assets.

Virtual local area network (VLAN) **Virtuální lokální síť**

*Logically independent network in the framework of one or more devices. Virtual networks can be defined as the domains of all-directional broadcast (See **LAN**) with the objective of making the logical network organisation independent of the physical network.*

Virtual machine (VM) **Virtuální stroj**

Software-defined complete execution stack consisting of virtualized hardware, operating system (guest OS), and applications.

Virtual private network (VPN) **Virtuální privátní síť**

A private computer network allowing for the connection of remote users to the target LAN via the Internet. Security is tackled using an encrypted tunnel between two points (or among one and several points). The identity of both parties is verified using digital certificates when making the connection.

Virus **Virus**

Type of malware spreading from one computer to another by attaching itself to other applications. Consequently, it may cause unwanted and dangerous activity. Usually, it has a built-in mechanism for further distribution or mutations.

Virus analysis **Analýza počítačového viru**

Complex activity including the analysis of computer virus behaviour (how it spreads, hides, damage caused by the virus), analysis of virus code, finding of the virus and its removal from files, or rectification of damage caused by the virus. More also in Disassembly, Debugger, Tracing, Code emulation.

Virus Definitions **Definice virů**

Predefined signatures for known malware used by antivirus detection algorithms.

Virus signature **Charakteristika (signatura) viru**

Unique bit string which sufficiently identifies the virus and which can be used by a scanning programme to detect virus presence.

Vulnerability **Zranitelnost**

Weakness of an asset or control that can be exploited by one o more threats.

Vulnerability analysis **Analýza zranitelnosti**

Systematic analysis of a system and operating services in view of security weaknesses and the efficiency of security measures.

Vulnerability assessment **Hodnocení zranitelností**

Process of identifying, quantifying, and prioritising (or ranking) the vulnerabilities in a system.

Vulnerability management **Řízení zranitelností**

The cyclical practice of identifying, classifying, remediating, and mitigating vulnerabilities. This practice generally refers to software vulnerabilities in computing systems; however, it can also extend to organisational behaviour and strategic decision-making processes.

Wardriving **Wardriving**

Searching for insecure wireless Wi-Fi networks by a person sitting in a means of transport, using a notebook, PDA or smartphone.

Warez **Warez**

A term from the computer slang denoting copyright-protected creations, which are treated in violation of the copyright. Warez is sometimes split into gamez (computer games), appz (applications), crackz (cracks) and also moviez (films). Today, the most frequent way of distribution is mainly the Internet.

Watchdog timer **Časový hlídač**

An electronic timer that is used to detect and recover from computer malfunctions. During normal operation, the computer regularly restarts the watchdog timer to prevent it from elapsing, or "timing out". If due to a hardware fault or program error, the computer fails to restart the watchdog, the timer will elapse and generate a timeout signal. The timeout signal is used to initiate corrective action or actions. The corrective actions typically include placing the computer system in a safe state and restoring normal system operation.

Web vandalism **Webový vandalizmus**

The attack which alters (defaces) web pages or causes a service denial (denial-of-service attacks).

Webtapping **Odposlech webu**

Monitoring of web pages, which may contain classified or sensitive information, and of people, who have access to them.

White box testing **Znalostní testování**

Testing which includes inspection of the implementation details.

White hat **White hat**

An ethical hacker who is often employed as an expert in computer security, programmer or network administrator. He or she specialises in penetration tests and other testing methodologies to ensure IT security in an organisation.

Whitelist **Whitelist, bílá listina**

A list of discrete entities, such as hosts or applications that are known to be benign and are approved for use within an organisation or information system.

Whois **Whois**

Internet service to find contact data of the owners of internet domains and IP addresses.

Wide Area Network (WAN) **Globální síť**

A physical or logical network that provides data communications to a larger number of independent users than are usually served by a local area network (LAN) and that is usually spread over a larger geographic area than that of a LAN.

WiFi **WiFi**

Wireless technology for data distribution ("by air"), suitable for the creation of network infrastructures in places where the building of a classical cable network is impossible, difficult or not cost-effective (cultural monuments, sports facilities, fairgrounds). Suitably located successive points of access along the route from the transmitter to the recipient are sufficient for data transmission.

WiMax **WiMax**

Telecommunication technology providing wireless data transmission using various transmission modes, from point-to-multipoint to completely mobile internet access for the transmission.

Wireless local area network (WLAN) **Bezdrátová lokální síť**

A computer network that links two or more devices using wireless communication within a limited area.

Wireshark **Wireshark**

*Formerly **Ethereal**. Protocol analyser and packet sniffler, which enables eavesdropping of all protocols which the computer receives and sends via an interface. Wireshark can decode the whole packet and show it in a way as sent out by the computer. Its advantage is that it is distributed under a free licence **GNU/GPL**.*

Wiretapping **Odposlech**

This is any tapping of a telephone transmission or conversation done without the consent of both parties, by accessing the telephone signal proper.

Workstation **Pracovní stanice**

Functional unit, usually with specific computing capabilities, having user input and output devices, such as. a programmable terminal or a stand-alone computer.

World wide web (WWW) **World wide web**

*Graphically-oriented service of the **Internet** – a system of interconnected hypertext pages using formatted text, graphics, animation and sounds.*

Worm **Červ**

*Autonomous programme (a subset of **Malware**) capable of creating its copies which, it then sends out to other computer systems (networks), where these pursue further activities they have been programmed for. Often it may serve to detect security holes in systems or mail programmes.*

X.509 **X.509**

*The standard for systems based on the public key (**PKI**) for simple signatures. X.509 specifies, for example, the format of a certificate, lists of cancelled certificates, parameters of certificates and methods for checking the validity of certificates.*

Zombie **Zombie**

Infected computer, which is part of botnet networks.

Notes:

Použité zkratky / Abbreviations used

Zkratka Abbreviation	Česky	English
ACI	Informace řízení přístupu	Access Control Information
ACL	Seznam pro řízení přístupu	Access Control List
APT	Pokročilá a trvalá hrozba	Advanced Persistent Threat
ARP	Protokol ARP	Address Resolution Protocol
ASIM	Automatické monitorování výskytu bezpečnostního incidentu	Automated Security Incident Measurement
BCM	Řízení kontinuity organizace	Business Continuity Management
BCMS	Systém řízení kontinuity organizace	Business Continuity Management System
BIA	Analýza dopadů na činnosti organizace	Business Impact Analysis
BIOS	Základní vstupně – výstupní systém	Basic Input Output System
BSOD	Modrá obrazovka smrti	Blue Screen of Death
CA	Certifikační autorita	Certification Authority
CAPTCHA	Zcela automatizovaný veřejný Turingův test odlišující počítače od lidí	Completely Automated Public Turing Test to Tell Computers From Humans
CAS	Systém řízeného přístupu	Controlled Access System
CC	Creative commons	Creative Commons
CERT	Skupina pro reakci na počítačové hrozby	Computer Emergency Response Team
CI	Konfigurační položka	Configuration Item
CIK	Kryptografický iniciační klíč	Crypto Ignition Key
CIRC	Schopnost pro reakci na počítačové hrozby	Computer Incident Response Capability
CMDB	Konfigurační databáze	Configuration Management Database
CNA	Útok na počítačovou síť	Computer Network Attack

CNE	Vytěžování počítačové sítě	Computer Network Exploitation
COMPUSEC	Počítačová bezpečnost	Computer Security
COMSEC	Bezpečnost komunikací	Communication Security
CPO	Vedoucí pro ochranu osobních údajů	Chief Privacy Officer
CSIRT	Skupina pro reakce na počítačové bezpečnostní incidenty	Computer Security Incident Response Team
CSP	Poskytovatel služby autorizačních údajů	Credential Service Provider
CVE	Běžné chyby zabezpečení a ohrožení	Common Vulnerabilities and Exposures
CZE	Česká republika	Czech Republic
ČR	Česká republika	Czech Republic
DCE	Distribuované výpočetní prostředí	Distributed Computing Environment
DDOS	Distribuované odmítnutí služby	Distributed Denial Of Service
DMZ	Demilitarizovaná zóna	Demilitarized Zone
DNS	Systém doménových jmen	Domain Name System
DNSSEC	Bezpečnostní rozšíření systému doménových jmen	Domain Name System Security Extensions
DOS	Odmítnutí služby	Denial Of Service
DPI	Podrobná inspekce paketů	Deep Packet Inspection
DRP	Plán obnovy po havárii	Disaster Recovery Plan
EMA	Elektromagnetická analýza	Electromagnetic Analysis
EME	Elektromagnetické vyzařování	Electromagnetic Emanations
ENISA	Agentura pro elektronickou a informační bezpečnost	European Network and Information Security Agency
EU	Evropská unie	European Union
FIRST	Fórum pro bezpečnostní týmy	Forum for Incident Response and Security Teams
FTP	Protokol pro přenos souborů	File Transfer Protocol

H4H	Hackers for hire	Hackers For Hire
HSM	Hardwarový bezpečnostní modul	Hardware Security Module
HTTP	Protokol pro přenos hypertextových dokumentů	Hypertext Transfer Protocol
HTTPS	Bezpečnostní nadstavba protokolu pro přenos hypertextových dokumentů	Hypertext Transfer Protocol Secure
IANA	Úřad pro přidělování čísel na Internetu	Internet Assigned Numbers Authority
ICANN	Internetová společnočnost pro přidělování jmen a čísel na internetu	Internet Corporation for Assigned Names and Numbers
ICMP	Internet control message protocol	Internet Control Message Protocol
ICT	Informační a komunikační technologie	Information And Communication Technology
IdM	Řízení identit	Identity Management
IDS	Systém detekce průniku	Intrusion Detection System
INFOSEC	Bezpečnost informací / informačních systémů	Information Security
IO	Informační operace	Information Operation
IP	Internet protokol	Internet Protocol
IPS	Systém prevence průniku	Intrusion Prevention System
IRC	Internetové směnové povídání	Internet Relay Chat
IS	Informační systémy	Information Systems
ISMS	Systém řízení bezpečnosti informací	Information Security Management System
ISP	Poskytovatel služeb internetu	Internet Service Provider
IT	Informační technologie	Information Technology
LAN	Lokální síť	Local Area Network
LTE	Dlouhodový vývoj	Long Term Evaluation
LIR	Lokální internetový registr	Local Internet Registry
MBCO	Minimální úroveň chodu organizace	Minimum Business Continuity Objective

MIB	Databáze řízení v komunikační síti	Management Information Base
MITM	Člověk uprostřed	Man In The Middle
NAT	Překlad síťových adres	Network Address Translation
NATO	Severoatlantická aliance	North Atlantic Treaty Organization
NATO CCD COE	Kooperativní špičkové centrum kybernetické obrany NATO	NATO Cooperative Cyber Defence Centre Of Excellence
NATO CDMA	Výkonný úřad kybernetické obrany NATO	NATO Cyber Defence Management Authority
NBAD	Detekce anomálního chování sítě	Network Behavior Anomaly Detection
NCIRC TC	NATO CIRC – Technické centrum	NATO Computer Incident Response Capability – Technical Centre
NIC	Síťová karta	Network Interface Card
NNEC	NATO Network Enabled Capability	Nato Network Enabled Capability
OS	Operační systém	Operating System
OSE	Otevřené bezpečnostní prostředí	Open Security Environment
OSF	Open software foundation	Open Software Foundation
P2P	Rovný s rovným	Peer To Peer
PC	Osobní počítač	Personal Computer
PGP	Dost dobré soukromí	Pretty Good Privacy
PII	Osobně identifikovatelné informace (údaje)	Personally Identifiable Information
PKI	Infrastruktura veřejných klíčů	Public Key Infrastructure
RF	Rádiové vlny	Radio Frequency
RFC	Request for comment	Request For Comment
RIR	Regionální Internetový Registr	Regional Internet Registry
RPO	Bod obnovy dat	Recovery Point Objective
RTO	Doba obnovy chodu	Recovery Time Objective
SaaS	Software jako služba	Software-as-a-Service

SAN	Síť uložiště	Storage Area Network
SCADA	Dispečerské řízení a sběr dat	Supervisory Control And Data Acquisition
SIEM	Management bezpečnostních informací a událostí	Security Information and Event Management
SLA	Dohoda o úrovni služeb	Service Level Agreement
SLD	Prohlášení o úrovni služeb	Service Level Declaration
SMS	Systém řízení služeb	Service Management System
SMTP	Simple mail transfer protocol	Simple Mail Transfer Protocol
SPC	Statiské řízení procesů	Statistical Process Control
SQL	Structured query language	Structured Query Language
SŘBI	Systém řízení bezpečnosti informací	Information Security Management System
SSH	Secure shell	Secure Shell
SSID	Service set identifier	Service Set Identifier
SSL	Secure socket layer	Secure Socket Layer
TCP	Transmission control protocol	Transmission Control Protocol
TERENA	Trans-evropské výzkumné a vzdělávací síťové fórum	Trans-European Research and Education Networking Association
TLD	Doména nejvyšší úrovně	Top Level Domain
TLS	Bezpečnost transportní vrstvy	Transport Layer Security
TSA	Autorita časového razítka	Time-Stamping Authority
TTP	Důvěryhodná třetí strana	Trusted Third Party
UDP	User datagram protocol	User Datagram Protocol
URL	Uniform resource locator	Uniform Resource Locator
UUID	Universální unikátní identifikátor	Universal Unique Identifier
VA/VM	Hodnocení zranitelností a řízení zranitelností	Vulnerability Assessment and Vulnerability Management
VM	Virtuální stroj	Virtual Machine
VLAN	Virtuální lokální síť	Virtual Local Area Network
VPN	Virtuální privátní síť	Virtual Private Network

WCDMA	Širokopásmový vícenásobný přístup s kódovým dělením	Wideband Code Division Multiple Access
WWW	World wide web	World Wide Web
XSS	Cross-site scripting	Cross-Site Scripting

Použité zdroje / Sources used

Česky

ČSN EN ISO 9000:2006 Systémy managementu kvality – Základní principy a slovník

ČSN ISO 31000:2010 Management rizik – Principy a směrnice

ČSN EN ISO/IEC 27000:2020 Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Přehled a slovník

ČSN EN ISO/IEC 27000:2017 Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Přehled a slovník

ČSN EN ISO/IEC 27000:2014 Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Přehled a slovník

ČSN ISO/IEC 27005:2013 Informační technologie – Bezpečnostní techniky – Řízení rizik bezpečnosti informací

https://www.cybersecurity.cz/ ve verzi 25. 10. 2011 a 29. 2. 2012

http://www.govcert.cz/ ve verzi 25. 10. 2011

http://www.nic.cz/ ve verzi 01. 03. 2012

http://www.wikipedia.org/ ve verzi 1. 3. 2012 a 1. 4. 2015

ISO/IEC 20000–1:2011 Informační technologie – Management služeb –

English

ISO/IEC 9000:2006 Quality management systems – Fundamentals and vocabulary

ISO 31000:2010 Risk management – Principles and guidelines

ISO/IEC 27000:2020 Information technology – Security techniques – Information security management systems – Overview and vocabulary

ISO/IEC 27000:2017 Information technology – Security techniques – Information security management systems – Overview and vocabulary

ISO/IEC 27000:2014 Information technology – Security techniques – Information security management systems – Overview and vocabulary

ISO/IEC 27005:2011 Information technology – Security techniques – Information security risk management

https://www.cybersecurity.cz/ in Version 25. 10. 2011 and 29. 2. 2012

http://www.govcert.cz/ in Version 25. 10. 2011

http://www.nic.cz/ in Version 01. 03. 2012

http://www.wikipedia.org/ in Version 1. 3. 2012 a 1. 4. 2015

ISO/IEC 20000–1:2011 Information technology – Service management –

Část 1: Požadavky na systém řízení služeb	Part 1: Service management system requirements
ISO/IEC 27003:2010 Informační technologie – Bezpečnostní techniky – Směrnice pro implementaci systému řízení informační bezpečnosti	ISO/IEC 27003:2010 Information technology – Security techniques – Information security management system implementation guidance
ISO/IEC 27031:2011 Informační technologie – Bezpečnostní techniky – Směrnice pro připravenost informační a komunikační technologie pro zabezpečení kontinuity organizace	ISO/IEC 27031:2011 Information technology – Security techniques – Guidelines for information and communication technology readiness for business continuity
ISO/IEC 27033 – Informační technologie – Bezpečnostní techniky – Bezpečnost sítě	ISO/IEC 27033 – Information technology – Security techniques – Network security
ISO/IEC 27039:2015 – Informační technologie – Bezpečnostní techniky – Výběr, uvedení do chodu a provoz systémů pro zjištění vniknutí	ISO/IEC 27039:2015 – Information technology – Security techniques – Selection, deployment and operations of intrusion detection systems
ČSN ISO/IEC 27032:2013 Informační technologie – Bezpečnostní technologie – Směrnice pro kybernetickou bezpečnost	ISO/IEC 27032:2012 (EN) Information technology – Security techniques – Guidelines for cybersecurity
ITIL® výkladový slovník v češtině, v1.0, 29. července 2011 založen na výkladovém slovníku v angličtině v1.0 z 29. 7. 2011	ITIL encyclopedic dictionary in Czech, v1.0, 29 July 2011, based on the encyclopedic dictionary in English v1.0, 29 July 2011
JTC1/SC27/SD6 Informační technologie – Bezpečnostní techniky – Stálý dokument 6 (SD6): Terminologický slovník IT bezpečnosti	JTC1/SC27/SD6 Information technology – Security techniques – Standing Document 6 (SD6): Glossary of IT Security Terminology
ČSN ISO/IEC 22301:2013 Společenská bezpečnost – Systémy řízení kontinuity organizace – Požadavky	ISO/IEC 22301:2012 (EN) Societal security – Business continuity management systems – Requirements
Jordán, Ondrák: Infrastruktura komunikačních systémů I. CERM. /	Jordán, Ondrák: Infrastructure of Communication Systems I. CERM. /

Sosinsky: Mistrovství: Počítačové sítě. CPRESS	Sosinsky: Championship: Computer Networks. CPRESS
Klíma Vlastimil: články „Základy moderní kryptologie – Symetrická kryptografie I-III“, Crypto-World, 2005	Klíma Vlastimil: articles „Fundamentals of modern cryptology - Symmetric cryptography I-III“, Crypto-World, 2005
Kybernetická bezpečnost resortu obrany v letech 2011 až 2013: Pojmový aparát a seznam zkratek, Ministerstvo obrany	Cyber security of the Defense Department between 2001 and 2013: Concepts and a list of abbreviations, MoD.
Peter Mell, Timothy Grance: The NIST Definition of Cloud Computing, Special Publication 800-145, 2011	Peter Mell, Timothy Grance: The NIST Definition of Cloud Computing, Special Publication 800-145, 2011.
Šestá mezinárodní konference o kybernetických konfliktech. P. Brangetto, M. Maybaum, J. Stinissen (Eds.), 2014 NATO CCD COE Publications, Talinn, “Triptych of Cyber Security“: A Classification of Active Cyber Defence, Robert S. Dewar, 2014	6th International Conference on Cyber Conflict P.Brangetto, M.Maybaum, J.Stinissen (Eds.) 2014 NATO CCD COE Publications, Tallinn, The “Triptych of Cyber Security”: A Classification of Active Cyber Defence, Robert S. Dewar, 2014
Talinn Manual, ISBN 978-1-107-02443-4, Cambridge University Press 2012	Tallinn Manual, ISBN 978-1-107-02443-4, Cambridge University Press 2013
Veřejně dostupné informace (Internet)	Publicly available sources (Internet)
Vyhláška č. 316/2014 Sb. o kybernetické bezpečnosti	Regulation No. 316/2014 Coll. On Cyber Security
Zákon č. 181/2014 Sb. o kybernetické bezpečnosti	Law No. 181/2014 Coll. On Cyber Security

Výkladový slovník kybernetické bezpečnosti

Páté doplněné a upravené vydání

Cyber Security Glossary

Fifth supplemented and revised edition

Autoři / Authors:
Petr Jirásek, Luděk Novák, Josef Požár

Editoři / Editors:
Petr Jirásek, Milan Kný

Přeložili do angličtiny / English Translation:
Karel Vavruška, Petr Jirásek

Vydali / Publishers:
Centrum kybernetické bezpečnosti, z.ú.
Dopravní 500/9, 104 00 Praha 10
www.kybercentrum.cz

Česká pobočka AFCEA
Dolnoměcholupská 12, 102 00 Praha 10
www.afcea.cz

Tisk / Print:
Margita Pincová Vančátová, Sedlčany

Tištěný náklad / Print run: 400 ks / pcs.

Praha 2022
ISBN 978-80-908388-4-0
Digitální kopie určená pro internet / Digital copy intended for the Internet