PŘÍLOHA 14: ZKRATKY A POUŽÍVANÉ POJMY

Informační systém se vztahuje na hlavní část povinných osob podle § 3 písm. c) až f) zákona o kybernetické bezpečnosti – správce nebo provozovatele informačních nebo komunikačních systémů kritické informační infrastruktury, významných informačních systémů, nebo informačních systémů základní služby. Hlavním společným jmenovatelem vymezení tohoto pojmu je **služba**, pro kterou daný informační nebo komunikační systém existuje. Je tomu tak, ať už jde v případě informačního a komunikačního systému kritické informační infrastruktury o službu, na kterou by mělo narušení funkce tohoto systému závažný dopad, v případě významného informačního systému o službu, k jejímuž zajištění je tento informační systém využívaný, nebo v případě informačního systému základní služby o službu, jejíž poskytování je na fungování tohoto informačního systému závislé. Informační nebo komunikační systém je tedy v zákoně o kybernetické bezpečnosti vždy vymezen službou, pro kterou existuje.

Používané pojmy

Aktivum je cokoliv, co má hodnotu pro jednotlivce nebo organizaci.[1]

Akceptovatelné riziko je riziko, které je přijatelné pro povinnou osobu a není nutné jej zvládat pomocí dalších bezpečnostních opatření.[2]

Analýza rizik zahrnuje ohodnocení kombinace hrozby a zranitelnosti s ohledem na aktiva a výpočet finální hodnoty.

Asset Management lze přeložit jako správu aktiv.

Bezpečnost informací je zajištění důvěrnosti, integrity a dostupnosti informací a dat.[3]

Bezpečnostním opatřením se rozumí souhrn úkonů, jejichž cílem je zajištění bezpečnosti informací v informačních systémech a dostupnosti a spolehlivosti služeb a sítí elektronických komunikací v kybernetickém prostoru.[4]

Citlivé osobní údaje jsou speciální kategorií podle GDPR, která zahrnuje údaje o rasovém či etnickém původu, politických názorech, náboženském nebo filozofickém vyznání, členství v odborech, o zdravotním stavu, sexuální orientaci a trestních deliktech či pravomocném odsouzení osob. Tyto údaje mohou subjekt údajů samy o sobě poškodit ve společnosti, v zaměstnání, ve škole či mohou zapříčinit jeho diskriminaci. Do kategorie citlivých údajů GDPR nově zahrnuje genetické a biometrické údaje. Zpracování citlivých osobních údajů podléhá mnohem přísnějšímu režimu, než je tomu u obecných údajů.[5]

---

[1] JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti.* 3., aktualiz. vyd. Praha: Policejní akademie ČR v Praze, 2015. ISBN 978-80-7251-436-6.
[2] § 2 písm. b) vyhlášky o kybernetické bezpečnosti
[3] § 2 písm. c) zákona o kybernetické bezpečnosti
[4] § 4 odst. 1 zákona o kybernetické bezpečnosti
[5] Citlivé osobní údaje | GDPR.cz. *GDPR | Obecné nařízení o ochraně osobních údajů — prakticky* [online]. Dostupné z: https://www.gdpr.cz/gdpr/heslo/citlive-osobni-udaje/

Dostupnost je vlastnost přístupnosti a použitelnosti na žádost oprávněné entity.[6]

Důvěrnost je vlastnost, že informace není dostupná nebo není odhalena neoprávněným jednotlivcům, entitám nebo procesům.[7]

GAP analýza neboli analýza mezer je nástroj pro srovnání požadovaného výsledku s reálným výsledkem. Cílem je najít mezery mezi těmito dvěma stavy. Tento typ analýzy je používán např. jako rozdílová analýza mezi skutečným stavem v organizaci oproti požadavkům VKB.

Garant aktiva je bezpečnostní role, která je odpovědná za zajištění rozvoje, použití a bezpečnost aktiva.[8] Garant aktiva spolupracuje s ostatními osobami zastávajícími bezpečnostní role, především dává relevantní vstupy do hodnocení aktiv a rizik.

GovCERT je označení pro Vládní CERT, který je součástí NÚKIB a poskytuje služby dle § 20 ZKB.

Hodnocení rizik zahrnuje identifikaci rizik, analýzu rizik a vyhodnocení rizik.

Hrozba je potenciální příčina kybernetické bezpečnostní události nebo kybernetického bezpečnostního incidentu, která může způsobit škodu. [9]

Identifikace rizik zahrnuje identifikování relevantních kombinací hrozeb a zranitelností s ohledem na aktiva.

Integrita je vlastnost přesnosti a úplnosti aktiv.[10]

Kritéria pro akceptovatelnost stanovují hranici, kdy mohou být rizika akceptována a kdy je nutné snižovat hodnotu rizika zaváděním bezpečnostních opatření.

Kybernetická bezpečnostní událost je událost, která může způsobit narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací.[11] Jde tedy o situaci, kdy může dojít k narušení kybernetické bezpečnosti a tím ke způsobení kybernetického bezpečnostního incidentu.

Kybernetický bezpečnostní incident je narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací v důsledku kybernetické bezpečnostní události.[12] Jinými slovy dojde k situaci, kdy byla porušena kybernetická bezpečnost.

Metodika hodnocení rizik obsahuje postup k provedení hodnocení rizik včetně stanovení kritérií pro akceptovatelnost.

---

[6] JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti.* 3., aktualiz. vyd. Praha: Policejní akademie ČR v Praze, 2015. ISBN 978-80-7251-436-6.
[7] Tamtéž
[8] § 7 odst. 3 vyhlášky o kybernetické bezpečnosti
[9] § 2 písm. e) vyhlášky o kybernetické bezpečnosti
[10] JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti.* 3., aktualiz. vyd. Praha: Policejní akademie ČR v Praze, 2015. ISBN 978-80-7251-436-6.
[11] § 7 odst. 1 zákona o kybernetické bezpečnosti
[12] § 7 odst. 2 zákona o kybernetické bezpečnosti

Národní CERT zajišťuje v rozsahu stanoveném ZKB sdílení informací na národní a mezinárodní úrovni v oblasti kybernetické bezpečnosti (viz § 17 ZKB).

Need-to-know princip znamená, že informace by měla být dostupná pouze tomu, kdo ji potřebuje vědět v nezbytně nutném rozsahu.

Osobní údaje jsou jakékoli informace o identifikovaném nebo identifikovatelném subjektu údajů. Identifikovatelnou fyzickou osobou je fyzická osoba, kterou lze přímo či nepřímo identifikovat, zejména odkazem na určitý identifikátor (jméno, číslo, síťový identifikátor) nebo na jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby. Mezi obecné osobní údaje řadíme jméno, pohlaví, věk a datum narození, osobní stav, ale také IP adresu a fotografický záznam. Vzhledem k tomu, že se GDPR vztahuje i na podnikající fyzické osoby, řadíme mezi osobní údaje i tzv. organizační údaje, kterými jsou například e-mailová adresa, telefonní číslo či různé identifikační údaje vydané státem.[13]

Plán zvládání rizik je přehledový dokument obsahující:

- cíle a přínosy bezpečnostních opatření pro zvládání jednotlivých rizik,
- určení osoby zajišťující prosazování bezpečnostních opatření pro zvládání rizik,
- potřebné finanční, technické, lidské a informační zdroje,
- termíny zavedení opatření,
- popis vazeb mezi riziky a příslušnými bezpečnostními opatřeními,
- způsob realizace bezpečnostních opatření.14

Podpůrné aktivum je chápáno jako technické aktivum, zaměstnanci a dodavatelé podílející se na provozu, rozvoji, správě nebo bezpečnosti informačního nebo komunikačního systému.[15]

Povinná osoba je orgán nebo osoba, která je povinna zavést bezpečnostní opatření podle zákona o kybernetické bezpečnosti.[16]

Primární aktivum je definováno jako informace nebo služba, kterou zpracovává nebo poskytuje informační nebo komunikační systém.[17]

Prohlášení o aplikovatelnosti je přehledový dokument, který obsahuje přehled bezpečnostních opatření požadovaných vyhláškou o kybernetické bezpečnosti, a to tak, že uvádí bezpečnostní opatření, která:

- nebyla aplikována, včetně odůvodnění toho, proč nebyla aplikována,
- byla aplikována, včetně způsobu jejich aplikace (plnění).18

[13] Osobní údaje | GDPR.cz. *GDPR | Obecné nařízení o ochraně osobních údajů — prakticky* [online]. Dostupné z: https://www.gdpr.cz/gdpr/heslo/osobni-udaje/
[14] § 5 odst. 1 písm. g) vyhlášky o kybernetické bezpečnosti
[15] § 2 písm. f) vyhlášky o kybernetické bezpečnosti
[16] § 2 písm. b) vyhlášky o kybernetické bezpečnosti
[17] § 2 písm. g) vyhlášky o kybernetické bezpečnosti
[18] § 5 odst. 1 písm. f) vyhlášky o kybernetické bezpečnosti

Rizikem je možnost, že určitá hrozba využije zranitelnosti aktiva a způsobí škodu.[19]

Řízení aktiv je proces zahrnující vytvoření metodiky pro identifikaci a hodnocení aktiv, identifikaci a hodnocení aktiv, určení a evidenci vazeb mezi primárními a podpůrnými aktivy, stanovení přípustných způsobů používání aktiv, určení způsobu jejich likvidace a určení a evidování garantů aktiv.

Řízení rizik je činnost zahrnující hodnocení rizik, výběr a zavedení opatření ke zvládání rizik, sdílení informací o riziku a sledování a přezkoumání rizik.[20] Součástí řízení rizik je také vytvoření metodiky hodnocení rizik, vytvoření plánu zvládání rizik, prohlášení o aplikovatelnosti a zprávy o hodnocení rizik.

Sdílení informací o riziku zahrnuje informování zainteresovaných stran (stakeholderů), jako jsou např. garanti, výbor kybernetické bezpečnosti a další.

Sledování a přezkoumávání rizik zahrnuje monitoring a provádění hodnocení rizik v pravidelných intervalech.

Systém řízení bezpečnosti informací (dále jen „ISMS“) je část systému řízení povinné osoby založená na přístupu k rizikům informačního nebo komunikačního systému, která stanoví způsob ustavení, zavádění, provozování, monitorování, přezkoumání, udržování a zlepšování bezpečnosti informací a dat.[21] Často používaná zkratka ISMS vychází z anglického názvu Information Security Management System.

Technickým aktivem se rozumí takové technické vybavení, komunikační prostředky a programové vybavení informačního nebo komunikačního systému a objekty, ve kterých jsou tyto systémy umístěny, jejichž selhání může mít dopad na informační nebo komunikační systém.[22]

TLP je metodika, která určuje, jakým způsobem je možné využívat poskytnuté informace. Více informací viz např. https://www.first.org/tlp/.

Výbor pro řízení kybernetické bezpečnosti je definovaná bezpečnostní role v souladu se zákonem o kybernetické bezpečnosti, představující organizovanou skupinu tvořenou osobami, které jsou pověřeny celkovým řízením a rozvojem informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury nebo významného informačního systému, anebo se významně podílejí na řízení a koordinaci činností spojených s kybernetickou bezpečností těchto systémů.[23]

Významná změna je změna, která má nebo může mít vliv na kybernetickou bezpečnost a představuje vysoké riziko.[24]

Výběr opatření zahrnuje volbu vhodných bezpečnostních opatření, kterými bude snižována hodnota příslušných rizik.

[19] § 2 písm. h) vyhlášky o kybernetické bezpečnosti
[20] § 2 písm. i) vyhlášky o kybernetické bezpečnosti
[21] § 2 písm. j) vyhlášky o kybernetické bezpečnosti
[22] § 2 písm. k) vyhlášky o kybernetické bezpečnosti
[23] JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti.* 3., aktualiz. vyd. Praha: Policejní akademie ČR v Praze, 2015. ISBN 978-80-7251-436-6.
[24] § 2 písm. o) vyhlášky o kybernetické bezpečnosti

Vyhodnocení rizik zahrnuje porovnání hodnoty rizika s kritérii pro akceptovatelnost a rozhodnutí, zda bude riziko akceptováno nebo bude snižováno zaváděním bezpečnostních opatření.

Významná změna je změna, která má nebo může mít vliv na kybernetickou bezpečnost a představuje vysoké riziko.[25]

Zavádění opatření zahrnuje proces implementace bezpečnostních opatření.

Zpráva o hodnocení rizik je dokumentovaným shrnutím závěrů hodnocení rizik.

Zranitelnost je slabé místo aktiva nebo slabé místo bezpečnostního opatření, které může být zneužito jednou nebo více hrozbami.[26]

Zvládání rizik zahrnuje výběr opatření, vytvoření Plánu zvládání rizik a zavádění opatření.

[25] § 2 písm. o) vyhlášky o kybernetické bezpečnosti
[26] § 2 písm. p) vyhlášky o kybernetické bezpečnosti

Používané zkratky

ADSL	Asymmetric Digital Subscriber Line
BIA	Analýza dopadů (Business Impact Analysis)
CD	Kompaktní disk (Compact Disc)
CERT	Computer Emergency Response Team
CIA	Důvěrnost, Integrita, Dostupnost (Confidentiality, Integrity, Availability)
CSIRT	Computer Security Incident Response Team
ČR	Česká republika
DB	Databáze
DMZ	Demilitarizovaná zóna
DPO	Pověřenec pro ochranu osobních údajů (Data Protection Officer)
DVD	Digitální víceúčelový disk (Digital Versatile Disc)
EDGE	Enhanced Data rates for GSM Evolution
EPS	Elektrická požární signalizace
EU	Evropská unie
EZS	Elektronický zabezpečovací systém
FW	Firewall
GDPR	General Data Protection Regulation
GPRS	General Packet Radio Service
HA	Vysoká dostupnost (High Availability)
HDD	Pevný disk (Hard Disk Drive)
HW	Hardware
ICT	Informační a komunikační technologie (Information and Communication Technologies)
ID	Identifikace (Identification)
IDS	Intrusion Detection System
IPS	Intrusion Prevention Systems
IS	Informační a komunikační systém

ISMS	Systém řízení bezpečnosti informací (Information Security Management System)
ISZS	Informační systém základní služby
IT	Informační technologie
KB	Kybernetická bezpečnost
KII	Kritická informační infrastruktura
LAN	Lokální síť (Local Area Network)
LTE	Vysokorychlostní technologie Long Term Evolution
Ministerstvo	Ministerstvo certifikací
MS	Microsoft
MT	Mobilní telefon
NATO	Severoatlantická aliance (North Atlantic Treaty Organization)
NB	Notebook
NGFW	Next Generation Firewall
NIA	Národní identitní autorita
NÚKIB	Národní úřad pro kybernetickou a informační bezpečnost
OS	Operační systém
PC	Osobní počítač (Personal Computer)
PDCA	Plan, Do, Check a Act
PKI	Public Key Infrastructure
PoA	Podpůrné aktivum
PrA	Primární aktivum
RAID	Diskové pole (Redundant Array of Inexpensive Disks)
SIEM	Security Information and Event Management
SLA	Smlouva o úrovni poskytovaných služeb (Service Level Agreement)
SPOC	Jednotné kontaktní místo (Single Point of Contact)
SSL	Secure Sockets Layer
SSD	Datové médium (Solid State Drive)

SW	Software
TLP	Traffic Light Protocol
USB	Universal Serial Bus
ÚOOÚ	Úřad pro ochranu osobních údajů
VIS	Významný informační systém
VKB	Vyhláška č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti)
VLAN	Virtuální LAN
Výbor KB	Výbor pro řízení kybernetické bezpečnosti
VZ	Veřejná zakázka
Wi-Fi	Bezdrátové připojení (Wireless Fidelity)
ZKB	Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti)
5G	Sítě 5. generace