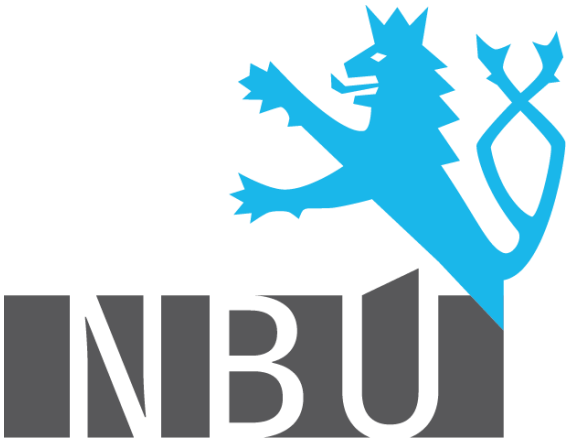
NÁRODNÍ BEZPEČNOSTNÍ ÚŘAD
Národní centrum kybernetické bezpečnosti



ZPRÁVA O STAVU KYBERNETICKÉ BEZPEČNOSTI ČESKÉ REPUBLIKY ZA ROK 2016

OBSAH

ÚVOD

V roce 2016 bylo potvrzeno, že zajištění kybernetické bezpečnosti patří ke klíčovým výzvám státu, na které Česká republika musí reagovat. Přelomovou událostí v tomto ohledu bylo listopadové usnesení Vlády České republiky č. 1049, ve kterém schválila rozvoj kapacit a schopností Národního centra kybernetické bezpečnosti (NCKB) do roku 2025. Rychlejšímu rozvoji napomůžou i organizační změny, které v průběhu roku buď proběhly, nebo byly schváleny. První z nich jsou organizační změny uvnitř NCKB a druhou je vládou schválené usnesení č. 1178 o oddělení NCKB ze struktur Národního bezpečnostního úřadu a vytvoření samostatného Národního úřadu pro kybernetickou a informační bezpečnost v druhé polovině roku 2017.

Dalším z milníků v posilování kybernetické bezpečnosti v ČR bylo zahájení kontrol kritické informační infrastruktury a významných informačních systémů. Ochrana těchto orgánů a osob je jedním z hlavních úkolů NCKB a započaté kontroly jsou zásadním krokem směrem k posílení odolnosti systémů KII a významných informačních systémů. Neméně důležitým úkolem byla příprava novelizace zákona o kybernetické bezpečnosti (ZKB), která vyplývá z potřeby nastolení souladu se směrnicí Evropského parlamentu a Rady EU o bezpečnosti sítí a informačních systémů (směrnice NIS). V souvislosti se zaváděním požadavků směrnice NIS se ukazuje, že Česká republika se přijetím ZKB zařadila mezi nejlépe připravené členské státy.

Rok 2016 se pro kybernetickou bezpečnost nesl ve znamení dalšího rozvoje mezinárodní spolupráce. Na bilaterální úrovni došlo díky vyslání cyber attachés k významnému prohloubení vztahů se Spojenými státy a Izraelem. Na poli mezinárodních institucí získala Česká republika díky vyslání cyber attaché do Bruselu lepší přehled o projednávaných otázkách souvisejících s kybernetickou bezpečnostní v EU a NATO. Do budoucna to umožní účinnější prosazování národních priorit a lepší koordinaci aktivit jednotlivých rezortů činných v dané oblasti. Reputace ČR jako důvěryhodného partnera byla posílena i mezinárodními kybernetickými cvičeními, kterých se pravidelně účastní a které sama i pořádá.

K posílení kybernetické bezpečnosti došlo i díky široké spolupráci na národní úrovni. NBÚ jako národní gestor aktivně spolupracoval s ostatními rezorty na zajištění jednotného postoje ČR směrem do zahraničí. Spolu s akademickou sférou se podílel na přípravě budoucích odborníků a na navyšování povědomí o kybernetické bezpečnosti. V rámci České republiky se rozvíjely i další bezpečnostní týmy jako například národní CERT tým (CSIRT.CZ). Technická spolupráce s ním a dalšími týmy dále prohloubila již probíhající sdílení informací, zkušeností se zranitelnostmi a společnou práci na vývoji nových technických nástrojů.

Rok 2016 neustále připomínal důležitost kybernetické bezpečnosti. Útoky na ukrajinský energetický sektor, proniknutí do systémů Demokratické strany v USA v průběhu volební kampaně či dva rekordní DDoS útoky, z nichž ten druhý poprvé ve velkém měřítku zapojil přístroje tzv. Internetu věcí (Internet of Things), ukazují na výzvy, před kterými Česká republika stojí. Stav kybernetické bezpečnosti ČR lze charakterizovat jako stav rostoucího povědomí o rizicích vyplývajících ze stále důležitější role, kterou kyberprostor hraje ve fungování veřejné správy a v každodenním životě občanů ČR. Nicméně tento pozitivní trend je narušován zvyšující se sofistikovaností kybernetických hrozeb, což zároveň umožňuje relativní lehkost, se kterou se tyto hrozby šíří.

1. ROZVOJ NCKB

Národní centrum kybernetické bezpečnosti (NCKB) se člení na odbor vládní CERT (GovCERT.CZ) a odbor kybernetických bezpečnostních politik (OKBP).

GovCERT.CZ [1] řeší kybernetické bezpečnostní incidenty po technické stránce, provádí penetrační testy, analýzu malware a zajišťuje sdílení informací o incidentech, zranitelnostech a trendech v kybernetické bezpečnosti s IT komunitou i veřejností. OKBP se soustředí na netechnické aspekty kybernetické bezpečnosti, zejména na tvorbu a implementaci kybernetické bezpečnostní politiky ČR, určování kritické informační infrastruktury (KII) a posuzování významných informačních systémů (VIS) podle zákona o kybernetické bezpečnosti (ZKB) a prováděcích právních předpisů, mezinárodní spolupráci, osvětu a vzdělávání nebo publikační činnost. Nově zřízené oddělení strategických informací a analýz posílí analytické kapacity národního centra.

Zásadní událostí pro rozvoj NCKB bylo usnesení vlády č. 1178 ze dne 19. prosince 2016, ve kterém vláda rozhodla o oddělení NCKB ze struktury Národního bezpečnostního úřadu (NBÚ) a vytvoření Národního úřadu pro kybernetickou a informační bezpečnost v druhé polovině roku 2017. Neméně důležité bylo Usnesení Vlády ČR ze dne 28. Listopadu 2016 č. 1049, ve kterém schválila návrh rozvoje kapacit a schopností Národního centra kybernetické bezpečnosti do roku 2025. Plán rozšíření předpokládá navýšení personální kapacity centra na 300-400 zaměstnanců do roku 2025 a výstavbu nové budovy v Brně – Černých polích.

NCKB pokračovalo v roce 2016 ve zvyšování kvalifikace svých pracovníků formou specializovaných školení, stáží a kurzů. Pracovníci GovCERT.CZ získali certifikace společnosti SANS, pracovníci OKBP se účastnili celé řady školení a kurzů zaměřujících se na kybernetickou bezpečnost v kontextu mezinárodního práva, terorismu či metod analýzy z otevřených zdrojů. Odborníci NCKB rovněž zvyšovali povědomí o činnosti centra skrze aktivní účast na domácích a mezinárodních expertních konferencích a seminářích.

V roce 2016 byly v souladu se zákonem o kybernetické bezpečnosti (ZKB) zahájeny kontroly systémů kritické informační infrastruktury (KII) a významných informačních systémů (VIS).[2]

[1] Více o činnosti GovCERT.CZ v 7. kapitole
[2] Více ve 2. kapitole

Důležitou činností centra v roce 2016 byla příprava transpozice evropské směrnice NIS.[3]

V prvních měsících roku 2016 byla dokončena certifikace GovCERT.CZ, který se k 1. dubnu stal plným členem mezinárodní platformy FIRST (Forum for Incident Response and Security Teams) sdružující vládní a soukromé CERT/CSIRT týmy z celého světa.[4]

V průběhu roku byla spuštěna nová verze veřejné části webových stránek sloužící jako informační portál širší a odborné veřejnosti. Neveřejná část je téměř dokončena a k jejímu předání a spuštění by mělo dojít na začátku roku 2017. Tento nový systém usnadní správu stránek a jejich plnění obsahem. Neveřejná část s kontrolou přístupu pak umožní sdílení informací ve větší míře směrem ke správcům systémů KII a VIS a také ke spolupracujícím bezpečnostním týmům. Jedná se zejména o informace, které není možné sdílet zcela veřejně, aby k nim nezískal přístup potenciální útočník.

[3] Více ve 3. kapitole
[4] Více v 4. kapitole

2. KRITICKÁ INFRORMAČNÍ INFRASTRUKTURA A VÝZNAMNÉ INFORMAČNÍ SYSTÉMY

Ochrana kritické informační infrastruktury je jedním z hlavních úkolů NCKB. V roce 2016 byly v souladu se zákonem o kybernetické bezpečnosti zahájeny kontroly systémů kritické informační infrastruktury a významných informačních systémů.

2.1 Určování KII a VIS

2.1.1 Obecné informace ke KII

Kritická informační infrastruktura je určována Národním bezpečnostním úřadem (NBÚ) podle kritérií stanovených nařízením vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury v aktuálním znění. Proces určování, resp. posuzování, zda systémy naplňují stanovená kritéria, probíhá ve spolupráci s daným správcem systému s využitím analýz dopadu incidentů a dalších podkladů. Samotný akt určení potom probíhá podle zákona č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon), a závisí na povaze subjektu. Organizační složky státu jsou určeny na návrh NBÚ usnesením vlády, ostatní subjekty pak opatřením obecné povahy vydaným NBÚ. Obecně se jedná o takové informační a komunikační systémy, jejichž narušení by mohlo mít závažný dopad na zabezpečení základních životních potřeb, zdraví osob, bezpečnost nebo ekonomiku státu. Pro představu jsou to například systémy, na kterých jsou zcela nebo významně závislé prvky „fyzické“ kritické infrastruktury, např. elektrárny, přenosové soustavy elektrické energie, některé banky apod.

Po určení KII začíná běžet přechodná lhůta pro plnění požadavků zákona. Správci KII nemusí plnit zákonem stanovené bezpečnostní požadavky okamžitě po svém určení, ale přechodná lhůta má zajistit časový prostor, aby se mohli na regulaci a zavedení bezpečnostních opatření připravit. Tato přechodná lhůta je v případě zavádění bezpečnostních opatření roční.

Nařízení vlády č. 432/2010 Sb. stanoví dvě sady kritérií, a to kritéria průřezová a odvětvová. Aby byl systém určen jako KII, musí z každé této sady naplnit alespoň jedno kritérium. Jinými slovy musí poskytovat služby ve specifickém odvětví a narušení tohoto systému musí způsobit určitý dopad stanovený průřezovými kritérii.

Průřezová kritéria zohledňují určité společenské zájmy, které mají být chráněny. Jsou jimi život a zdraví, ekonomika a narušení či omezení služeb nezbytných pro fungování společnosti.[5]

Při hodnocení dopadu je nutné zvažovat všechny tři základní aspekty bezpečnosti informací, tedy narušení důvěrnosti, dostupnosti a integrity.

Odvětvová kritéria pak nalezneme v příloze nařízení v odvětví VI. komunikační a informační systémy. Pro kritickou informační infrastrukturu je rozhodující písmeno G. Oblast kybernetické bezpečnosti. Kritéria jsou následující:

- informační systém, který významně nebo zcela ovlivňuje činnost určeného prvku kritické infrastruktury, a který je nahraditelný jen při vynaložení nepřiměřených nákladů nebo v časovém období přesahujícím 8 hodin,
- komunikační systém, který významně nebo zcela ovlivňuje činnost určeného prvku kritické infrastruktury, a který je nahraditelný jen při vynaložení nepřiměřených nákladů nebo v časovém období přesahujícím 8 hodin,
- informační systém spravovaný orgánem veřejné moci obsahující osobní údaje o více než 300 000 osobách,
- komunikační systém, zajišťující připojení nebo propojení prvku kritické infrastruktury, s kapacitou garantovaného datového přenosu nejméně 1 Gbit/s,
- odvětvová kritéria pro určení prvku kritické infrastruktury uvedená v písmenech A. až F. se použijí přiměřeně pro oblast kybernetické bezpečnosti, pokud je ochrana prvku naplňujícího tato kritéria nezbytná pro zajištění kybernetické bezpečnosti.

Protože v KII jsou zahrnuty systémy zajišťující nejdůležitější funkce státu, jsou bezpečnostní požadavky kladené ZKB na tuto skupinu nejpřísnější. Správci KII musí naplňovat zákon v celém rozsahu, respektive zavést všechna bezpečnostní opatření specifikovaná vyhláškou č. 316/2014 Sb., o kybernetické bezpečnosti. Rámcově se jedná o:

- hlášení kontaktních údajů,
- detekci a hlášení kybernetických bezpečnostních incidentů,
- zavedení bezpečnostních opatření,
- provádění reaktivních a ochranných opatření.

[5] Přesnou specifikaci průřezových kritérií nalezneme v § 1 zmíněného nařízení vlády.

2.1.2 Obecné informace k VIS

Významný informační systém je definován v § 2 písm. d) ZKB jako informační systém spravovaný orgánem veřejné moci, který není kritickou informační infrastrukturou a u kterého narušení bezpečnosti informací může omezit nebo výrazně ohrozit výkon působnosti orgánu veřejné moci.

Z definice lze dovodit, že jako VIS může být identifikován pouze systém ve správě subjektu státní sféry. Soukromý sektor je tedy z této úpravy vyloučen. Pokud by systém naplnil kritéria pro KII i VIS, určí se jako KII, neboť přísnější regulace má přednost. Z regulace VIS jsou dále vyloučeny obce.

Identifikace konkrétních VIS je závislá na vyhlášce č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích. VIS jsou oproti KII definovány zajištěním působnosti orgánu veřejné moci. Zatímco narušení KII by tedy mohlo mít dopad na úroveň celého státu, narušení VIS by mohlo mít dopad na zajištění fungování a výkonu působnosti konkrétního orgánu veřejné moci.

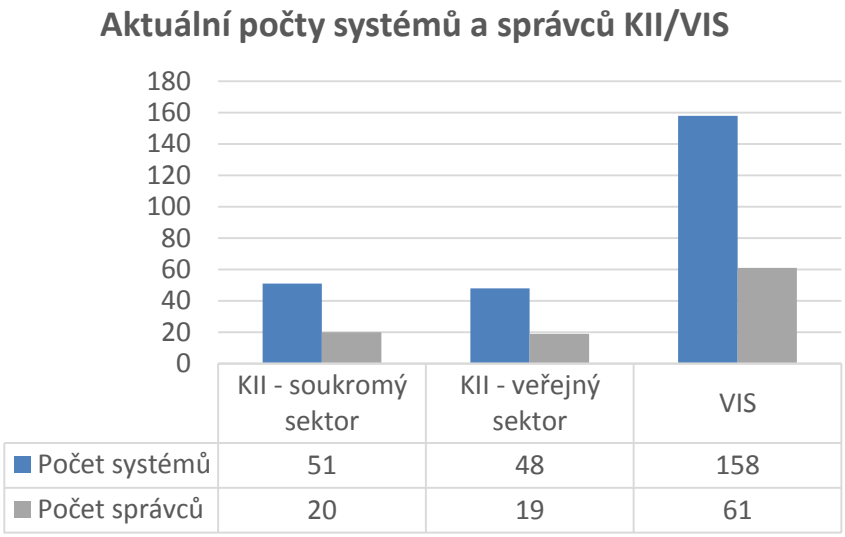
Rozdíl oproti KII je u VIS také v procesu určení. Naplnění kritérií VIS musí posoudit sám správce systémů. Pokud kritéria naplní, vzniká mu povinnost nahlásit kontaktní údaje NBÚ a začít se řídit ZKB. NCKB v této oblasti poskytuje metodickou podporu a konzultace.

2.1.3 Aktuální počty KII a VIS

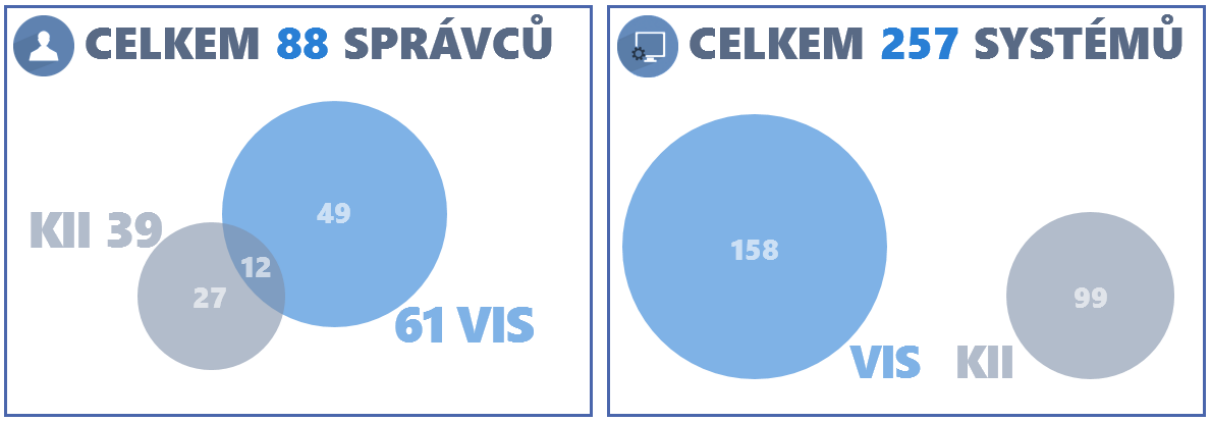
Aktuální počet systémů KII a VIS ilustruje graf 1 a obr. 1. Systém KII může být ve správě jak institucí veřejného sektoru, tak soukromého. Z obrázku č. 1 vyplývá, že v počtu systémů i správců jsou tyto sektory téměř vyrovnané.

K 31. prosinci 2016 bylo NCKB evidováno 48 KII a 158 VIS ve správě 80 orgánů veřejné moci a 51 KII a 20 správců v soukromém sektoru.

Obrázek 1 nahlíží na oblast z jiného pohledu. Je z něj zřejmé, že pod NCKB v současné době spadá celkem 257 informačních či komunikačních systémů klasifikovaných jako KII či VIS, které spravuje celkem 88 správců. Téměř tři čtvrtiny těchto subjektů sídlí v Praze. V rámci základní zákonné povinnosti, tj. nahlášení kontaktních údajů, obdrží NBÚ ke každému systému průměrně kontaktní údaje na 3 odpovědné osoby.



Graf 1: aktuální počty systémů KII a VIS



Obr. 1: Souhrn systémů KII a VIS

2.2 Kontrola dodržování zákona o kybernetické bezpečnosti

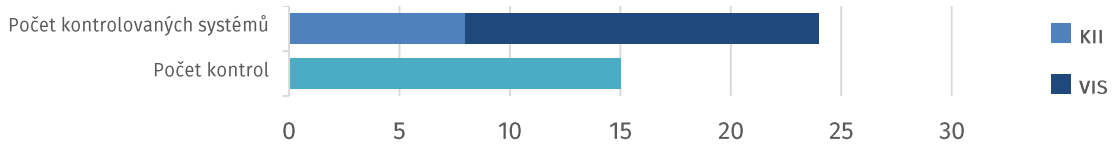
Začátkem roku 2016 byly u povinných osob zahájeny kontroly [6] dodržování zákona o kybernetické bezpečnosti. Výkonem kontroly je na základě tohoto zákona pověřen Národní bezpečnostní úřad), faktický výkon kontroly je pak zajišťován odborníky z Národního centra kybernetické bezpečnosti.

Kontroly byly u správců vždy prováděny po uplynutí tzv. přechodné lhůty (roční lhůta na zavedení požadovaných bezpečnostních opatření).

[6] Kontroly se řídí zákonem č. 255/2012 Sb., o kontrole

Většina z kontrol vykonaných za rok 2016 byla zaměřena na významné informační systémy. Menší podíl kontrol se zaměřoval na kritickou informační infrastrukturu.

NBÚ provedl kontrolu u celkem 15 povinných osob (správců). Předmětem proběhlých kontrol bylo celkem 24 systémů.



Graf 2: Typy a počet kontrolovaných systémů

2.2.1 Kritéria kontroly

Hlavním kritériem kontroly je ZKB a jeho prováděcí právní předpis vyhláška č. 316/2014 Sb., o kybernetické bezpečnosti (VKB). Kontroly probíhají v souladu se zákonem č. 255/2012 Sb., o kontrole (Kontrolním řádem). Proces kontroly se principiálně blíží procesu auditu dle ISO 19 011 a norem řady ISO 27k.

Kontroly v roce 2016 byly až na výjimku tzv. metodické. V případě identifikování neshody (porušení některého z požadavků zákona) u metodických kontrol nebyl podáván podnět na zahájení správního řízení. Důvodem k tomuto opatření je snaha pracovat s povinnými osobami na nápravě a ohled na krátkou účinnost zákona o kybernetické bezpečnosti.

2.2.2 Plán kontrol

Provádění kontrol se řídí interním plánem NBÚ, který schvaluje ředitel NBÚ, a který je sestavován kvartálně.

Kontrolovaný subjekt předem od kontrolního týmu obdrží oznámení o plánované kontrole a tzv. „Průvodce kontrolou ZKB“, což je příručka, která má za cíl kontrolovaný subjekt připravit na proces kontroly.

Samotné kontrole na místě často předchází tzv. přezkoumání dokumentace, tedy proces posouzení požadovaných bezpečnostních politik a souvisejících dokumentů.

2.2.3 Co je kontrolováno

Jak již bylo zmíněno, kontrolují se veškeré požadavky ZKB a VKB. Kontrolní tým má k tomuto účelu k dispozici seznam kontrolních bodů. Tento seznam vychází převážně z VKB (oblast organizačních opatření, technických opatření a zvládání incidentů). Počet reálně kontrolovaných bodů je závislý např. na typu kontrolovaného systému, technologiích, na způsobu plnění zákonných požadavků apod.

Při kontrolách je využívána metoda vzorkování. Tzn., že z celkového souboru kontrolních bodů, procesů a informací jsou systematicky vybrány jen některé. Na základě posouzení těchto vzorků jsou formulovány závěry týkající se celku.

2.2.4 Délka trvání kontroly

Doba trvání kontroly se odvíjí od rozsahu kontroly, u proběhlých kontrol se pohybovala v rozmezí od dvou do čtyř dní. Průběh konkrétní kontroly vychází z předem sestaveného a oboustranně schváleného programu (časový harmonogram kontrolních činností).

2.2.5 Výstup z kontroly

Na závěr kontroly je vypracován protokol o kontrole, který obsahuje:

- základní informace o kontrole,
- manažerské shrnutí,
- kontrolní zjištění,
- stanovené termíny pro nápravná opatření,
- poučení,
- přílohy.

Protokol je zpravidla předán kontrolované osobě v poslední kontrolní den.

2.2.6 Typy kontrolních zjištění

Kontrolní zjištění popisuje výsledek hodnocení shromážděných důkazů z kontroly (nález). Pro účely kontroly rozlišujeme následující typy zjištění:

- **Neshoda**, kterou se rozumí nesplnění požadavku podle stanovených kritérií nebo odchýlení praxe od dokumentovaných postupů v organizaci (nesoulad). Zjištění typu neshoda je důvodem k zahájení správního řízení. U neshod je dále uváděn i termín, do kterého musí dojít k nápravě.
- **Potenciální riziko**. Jde o typ zjištění, kdy kontrolující upozorňuje na možné riziko.
- **Příležitost ke zlepšení.** Jde o typ zjištění, které má charakter doporučení a vychází ze zkušeností kontrolujícího.
- **Shoda**. Shodou se rozumí splnění požadavků podle stanovených kritérií (soulad). Nálezy shod nejsou zahrnuty do kontrolního protokolu.
- **Pozoruhodné úsilí**. Pozoruhodným úsilím se rozumí nadstandardní hodnocení dané oblasti.

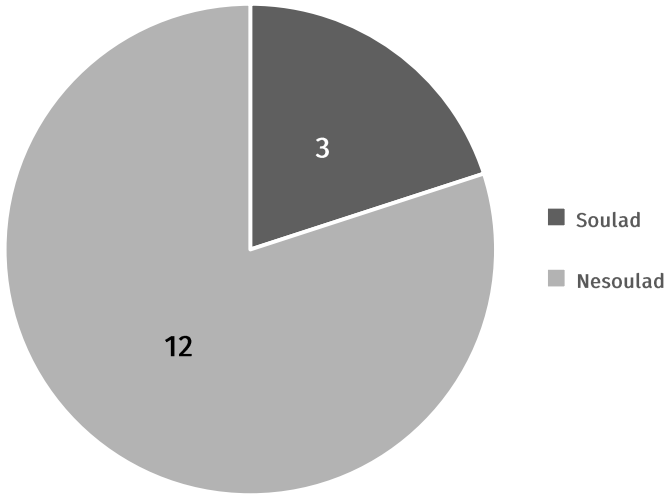
2.2.7 Námitky

Kontrolovaná osoba má právo ve stanovené lhůtě podat námitky ke konkrétním zjištěním z protokolu o kontrole. Námitky musí být podány v souladu s Kontrolním řádem, tedy do

dvou týdnů od obdržení vyhotoveného protokolu. Pokud tak kontrolovaný subjekt neučiní, kontrola je uplynutím této lhůty řádně ukončena. Možnosti podat námitky zatím využily dva subjekty, přičemž v obou případech bylo rozhodnuto, že jsou neopodstatněné a byly zamítnuty.

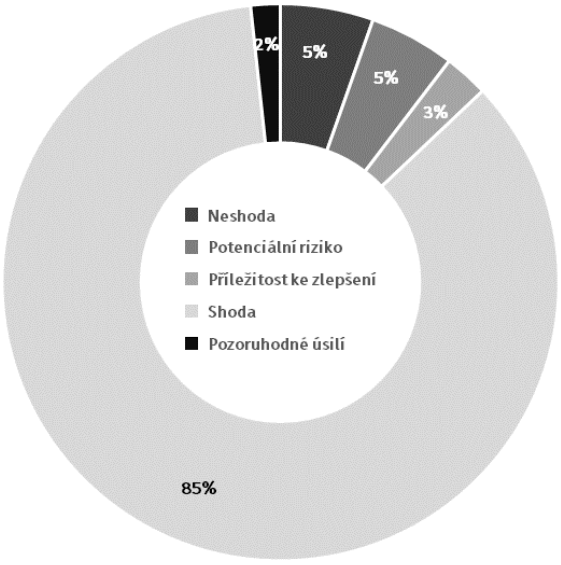
2.2.8 Výsledky proběhlých kontrol

Graf 3 přibližuje, že z celkového počtu 15 provedených kontrol byl ve 3 případech zjištěn celkový soulad (tedy nezjištěna žádná neshoda). V ostatních 12 případech byl shledán nesoulad (tedy dvanáct kontrolovaných subjektů se dopustilo porušení zákona o kybernetické bezpečnosti).



Graf 3: Celkové výsledky kontrol ZKB za rok 2016

Poměr jednotlivých zjištění všech provedených kontrol za rok 2016 znázorňuje graf č. 4.



Graf 4: Poměr jednotlivých zjištění za rok 2016

2.2.9 Nejčastější zjištění

Seznam nejčastějších zjištění vycházejících z dosavadních kontrol provedených v r. 2016 je uveden v příloze č. 1. Cílem výčtu těchto častých zjištění je zamezit dalšímu opakování těchto nedostatků u ostatních subjektů.

Obecně je důležité poznamenat, že splnění požadavků zákona o kybernetické bezpečnosti rozhodně není možné řešit „pouhým“ nákupem a nasazením řešení třetí strany. Jde o soubor procesních, organizačních a technických opatření a nástrojů, které je zapotřebí správně aplikovat, aby byly naplněny nejen potřeby zákona, ale i potřeby organizace.

2.3 Technická bezpečnost systémů KII/VIS

Od června 2015 realizuje NBÚ - NCKB projekt „Systém detekce kybernetických bezpečnostních událostí“ analyzující síťový provoz v klíčových sítích státu. Důvodem je problematická ochrana perimetru sítě („efekt mizejícího perimetru“), ke které přispívají zejména

- stále se zlepšující (spear) phishingové metody,
- neukázněnost uživatelů (využívání neprověřených flash disků, instalace nepovoleného softwaru, návštěvy závadných stránek),
- rozvoj mobilní výpočetní techniky, smartphonů a tabletů, které mohou být zapojovány do sítě, atd.

Vektorů útoku je mnoho, a pokud o nákazu sítě usiluje technicky vybavený aktér ochotný investovat peníze a čas, jako je tomu v případě tzv. APT (Advanced Persistent Threats), je pravděpodobnost průniku vysoká a analýza síťového provozu může administrátorům poskytnout cenná vodítka.

Systém bude sledovat síťový provoz a kromě komunikace na adresy se špatnou reputací bude mimo jiné schopen za pomoci metod behaviorální analýzy vyhledat anomální datové přenosy, tj. data proudící v nezvyklý čas, nezvyklém formátu či objemech. Usnadní tak detekci řady negativních jevů: malwaru, komunikace do sítí a na adresy se špatnou reputací, skenování sítě zvnějšku, brute-force pokusů o prolomení autentizace u služeb nabízených sítí, DoS/DDoS útoků, zapojení počítačů do botnet sítí a dalších.

Partneři budou zároveň s NBÚ sdílet pečlivě zvolenou množinu údajů výhradně z perimetru svých sítí, což umožní dohledat i bezpečnostní incidenty, které by v rámci jednoho rezortu nebyly detekovány, případně nebyly vyhodnoceny jako nebezpečné. NBÚ bude na oplátku s partery sdílet seznamy závadných IP adres a domén a další aktualizace. Systém tak v důsledku zvýší důvěrnost, integritu a dostupnost dat v sítích obsahujících řadu klíčových prvků informační infrastruktury státu.

V první fázi se do Systému detekce kromě samotného NBÚ zapojí i Ministerstvo financí, Ministerstvo práce a sociálních věcí a Ministerstvo spravedlnosti. Systém pokryje nejen sítě ministerstev, ale i většinu jimi přímo řízených organizací. Po spuštění systému pak bude NCKB okruh zapojených institucí dále rozšiřovat.

Koncem roku 2016 začal GovCERT.CZ spolu s Ministerstvem vnitra (MV) připravovat projekt scrubbing centra (zařízení umožňující filtrování DoS/DDoS útoků). Cílem je vybudovat centrum pro orgány státní správy. Ty, v případě zasažení volumetrickým útokem, budou moci příchozí provoz přesměrovat přes toto zařízení. Čistý provoz je pak směrován zpět k napadené organizaci.

Tým GovCERT.CZ rovněž realizoval projekt „Analýza metadat ministerstev České republiky“. Cílem projektu bylo zajištění informací, které by mohly sloužit pro přípravu útoku. Tato činnost je preventivního charakteru a má usnadnit administrátorům zabezpečení ICT infrastruktury. Dále byly realizovány penetrační testy webových aplikací na základě nově vytvořené metodologie vycházející z testovací struktury Open Web Application Security Project (OWASP). Tyto testy jsou nabízeny vládním institucím a správcům prvků KII/VIS. V rámci projektu externího penetračního testování byly provedeny dílčí testy, které vedly k zapojení subsystémů infrastruktury organizace. Zkušenosti z těchto projektů byly využity k aktualizaci technického cvičení Cyber Czech 2016 připravovaného NBÚ.

3. LEGISLATIVA A KONCEPČNÍ DOKUMENTY

V roce 2016 NBÚ připravoval ve spolupráci s dotčenými resorty transpozici evropské směrnice NIS, která proběhne formou novelizace ZKB na začátku roku 2017. Další důležitou činností byla implementace Akčního plánu NSKB.

3.1 Národní strategie kybernetické bezpečnosti a Akční plán

Informace o plnění Národní strategie kybernetické bezpečnosti (NSKB) na období let 2015 až 2020, respektive jejího Akčního plánu je zpracovaná na základě vstupů jednotlivých subjektů v příloze č. 6.

3.2 Legislativní vývoj

Snahy o zavedení minimálních bezpečnostních standardů pro důležité informační a komunikační systémy a o lepší koordinaci při zajišťování kybernetické bezpečnosti, které na vnitrostátní úrovni vedly k přijetí zákona o kybernetické bezpečnosti, nalezly v roce 2016 konkrétní vyústění i na evropské úrovni v podobě směrnice č. 2016/1148 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii, tzv. směrnice NIS.

Směrnice NIS upravuje dvě obecné kategorie subjektů, tzv. provozovatele základních služeb a poskytovatele digitálních služeb, kteří budou v různé míře muset zavádět bezpečnostní opatření a hlásit bezpečnostní incidenty způsobilé narušit klíčové společenské a ekonomické činnosti zajišťované jimi provozovanými službami, resp. kontinuitu poskytování svých služeb. Tyto subjekty coby nové kategorie doplní stávající povinné osoby podle § 3 ZKB, tj. orgány a osoby zajišťující provoz sítí elektronických komunikací, poskytování služeb elektronických komunikací, provozovatele významných sítí, správce kritické informační infrastruktury a správce významných informačních systémů.

Směrnice NIS kromě identifikace provozovatelů základních služeb a stanovení požadavků na bezpečnostní opatření, na detekci incidentů a na jejich hlášení ukládá členským státům také povinnost zpracovat národní strategii kybernetické bezpečnosti, určit vnitrostátní příslušné orgány, jednotná kontaktní místa pro styk se zahraničními protějšky a pro regulovaná odvětví zřídit bezpečnostní týmy CSIRT a zajistit jejich fungování. Česká republika řadu těchto opatření zavedla již v souvislosti s přijetím ZKB. Členské státy rovněž budou spolupracovat v rámci dvou směrnicí zřizovaných platforem, Skupiny pro spolupráci pro otázky strategické povahy a Sítě CSIRT pro spolupráci technickou.

Vzhledem k transpoziční lhůtě 21 měsíce od vstupu směrnice v platnost NBÚ již během finálních fází vyjednávání začal ve spolupráci s dotčenými rezorty a dalšími subjekty připravovat transpoziční novelu, jejíž návrh vláda schválila dne 23. listopadu 2016 a následně k dalšímu projednání postoupila Poslanecké sněmovně Parlamentu ČR. Nová právní úprava by měla vejít v účinnost v polovině roku 2017.

Navrhovaná novelizace ZKB částečně reaguje i na nedostatky zjištěné aplikační praxí v prvních dvou letech účinnosti zákona.

V roce 2016 byla rovněž novelizována vyhláška č. 317/2014 Sb., o významných informačních systémech, jejíž příloha stanoví seznam těchto systémů a musela být v souvislosti s pokračující identifikací nových systémů aktualizována.

3.3 Bílá místa

V roce 2016 upozornil NBÚ vládu České republiky na existenci bílých míst v zajišťování kybernetické bezpečnosti. Tato bílá místa byla identifikována na základě aktivit pracovníků NCKB v průběhu prvního roku účinnosti ZKB.

Zásadní charakteristikou bílých míst je absence některých důležitých sektorů v soustavě KII. Bílá místa také upozornila na nedostatečnou úpravu vztahů mezi správci KII či VIS a dodavateli ICT služeb, která mohla ohrozit samotné fungování některých systémů. V neposlední řadě dokument poukázal na další rizika vyplývající např. z nedostatku odborníků na kybernetickou bezpečnost ve veřejné správě nebo z aplikace některých dalších zákonů, které nereflektovaly požadavky kladené na kybernetickou bezpečnost. NBÚ následně v roce 2016 vládu informoval o řešení bílých míst, které probíhají na legislativní, administrativní i metodické úrovni.

4. MEZINÁRODNÍ SPOLUPRÁCE

Mezinárodní spolupráce představuje jeden z hlavních pilířů zajišťování kybernetické bezpečnosti státu. Na poli mezinárodních organizací jsou pro Českou republiku tradičními partnery Severoatlantická aliance a Evropská unie. V příštím roce by se mohl seznam organizací a fór, kterých se ČR účastní, opět rozrůst. NCKB aktivně zkoumá příležitosti zapojení se například do Global Forum on Cyber Expertise, kde dochází ke sdílení know-how a osvědčených postupů při budování kybernetických kapacit. Na poli bilaterálních vztahů se pak díky vyslání cyber attachés výrazně prohloubily strategické vztahy se Spojenými státy americkými a Izraelem.

V oblasti mezinárodní spolupráce vedle NBÚ působí i další rezorty, zejména Ministerstvo obrany (MO), Ministerstvo zahraničních věcí (MZV) či Ministerstvo průmyslu a obchodu (MPO).

4.1 Evropská unie

Nejvýraznějším počinem v oblasti kybernetické bezpečnosti na evropské úrovni v roce 2016 bylo bezesporu přijetí směrnice NIS (viz kapitola 3.2 výše). Návrh předložený Evropskou komisí v roce 2013 doznal v průběhu vyjednávání značných změn, zejména v otázce rozsahu dopadu této regulace. Vzhledem k tomu, že Česká republika již má zaveden fungující rámec regulace kybernetické bezpečnosti, na jednání se aktivně podílela s poměrně silnou vyjednávací pozicí a podařilo se tak mimo jiné zúžit okruh poskytovatelů digitálních služeb a minimalizovat úroveň jejich povinností. V této oblasti je zároveň uplatněn princip maximální harmonizace, zabraňující ukládání povinností nad rámec směrnice a povinnosti tak budou harmonizovány napříč všemi členskými státy.

Od okamžiku přijetí směrnice NIS se zástupci České republiky účastní přípravných jednání dvou kooperačních platforem, Skupiny pro spolupráci a Sítě CSIRT. Podílí se rovněž na práci komitologického výboru připravujícího implementační akty předvídané směrnicí NIS.

Síť bezpečnostních týmů CSIRT je skupina sdružující evropská pracoviště typu CSIRT a CERT-EU. Posláním skupiny je podpořit rychlou a účinnou spolupráci, vytvoření důvěryhodné komunikační platformy a sdílení osvědčených postupů. ČR v této skupině zastupuje vládní a národní CERT. V roce 2016 proběhla trojice přípravných setkání, jejichž cílem bylo formulovat základní dokumenty (mandát a jednací řád). Primárním cílem pro následující rok je podpora členských států, které v této skupině dosud nemají zástupce, při budování národního CERT a zajištění základní úrovně služeb.

Dalším významným fórem pro kybernetickou bezpečnost na půdě EU byla i v roce 2016 pro Českou republiku skupina přátel předsednictví pro kybernetické otázky (Friends of Presidency on Cyber Issues), která se pravidelně schází od r. 2013. V uplynulém roce byl na

její půdě draftován Diplomatic Toolbox formulující možné diplomatické nástroje, které mají členské státy k dispozici při řešení závažných kybernetických útoků. S nástupem slovenského předsednictví se pak pozornost přenesla zejména na navyšování kybernetické odolnosti a kybernetických kapacit. K tomuto tématu byly připraveny závěry Rady ke sdělení Komise k „posílení evropského systému kybernetické odolnosti a podpoře konkurenceschopného a inovativního odvětví kybernetické bezpečnosti“, následně přijaté Radou pro obecné záležitosti. V roce 2016 byl též schválen nový jednací řád a mandát skupiny. S těmito změnami došlo k povýšení skupiny na stálou pracovní skupinu a změně jejího názvu na Horizontální pracovní skupinu pro kybernetické otázky (Horizontal Working Party on Cyber Issues).

Díky zřízení stálé pozice cyber attaché v Bruselu Česká republika v roce 2016 získala lepší přehled o projednávání otázek souvisejících s kybernetickou bezpečností napříč jednotlivými orgány EU a pracovními skupinami Rady, což do budoucna umožní účinnější prosazování národních priorit a lepší koordinaci aktivit jednotlivých rezortů činných v oblasti kybernetické bezpečnosti a záležitostech s ní souvisejících. V roce 2016 byl takto např. kromě Ministerstva zahraničních věcí koordinován postup s Ministerstvem obrany, Ministerstvem vnitra a Ministerstvem spravedlnosti v rámci jejich rezortní agendy.

Příkladem takové úspěšné mezirezortní koordinace je realizace únorové návštěvy hodnotitelů v rámci sedmého kolo vzájemných hodnocení pořádaných Pracovní skupinou pro obecné záležitosti (GENVAL), na níž se NBÚ podílel s ministerstvy vnitra a spravedlnosti, policií a Nejvyšším státním zastupitelstvím. Aktuální sedmé kolo je věnováno provádění a fungování evropských politik týkajících se kyberkriminality a boje proti ní. Hodnotící zpráva České republiky byla skupinou GENVAL projednána v prosinci 2016, podle předběžných závěrů s pozitivním ohlasem.

Za účelem podpory výzkumných aktivit došlo v červenci 2016 k vytvoření smluvního partnerství veřejného a soukromého sektoru pro kybernetickou bezpečnost s názvem European Cyber Security Organization (ECSO). Za Českou republiku se k asociaci připojila Národní agentura pro komunikační a informační technologie (NAKIT), která bude moci na základě svého partnerství v rámci programu Horizont 2020 vyjednávat s Evropskou komisí podobu nové ECSO výzvy.

V rámci unijního výzkumného programu pro výzkum a inovace Horizont 2020 byl aktivní i NBÚ. Úřad se zapojil do tří výzkumných konsorcií z oblasti kybernetické bezpečnosti. Podpořené projekty se zaměřují na inovativní metody sdílení informací bezpečnostních CERT/CSIRT týmů a jejich partnerských organizací, pokročilé zpracování různých druhů dat za využití prvků umělé inteligence a vývoj *„SCADA honeypotů“,* tedy návnad lákajících a automaticky analyzujících malware napadající průmyslové řídicí systémy.

4.2 Evropská agentura pro bezpečnost sítí a informací (ENISA)

Česká republika je v ENISA zastoupena skrze účast na formálních a neformálních jednáních. Dva zástupci NBÚ působí jako člen a alternát v představenstvu ENISA, kde se podílejí na schvalování programu, plánu prací a rozpočtu ENISA. Další zástupce NBÚ je členem užší pracovní skupiny ENISA pro podporu tvorby a implementace národních strategií kybernetické bezpečnosti. V ČR slouží i tzv. National Liaison Officer (pracovník NBÚ), který v každé členské zemi EU vykonává funkci referenčního bodu v specifických otázkách kybernetické bezpečnosti, zprostředkovatele spolupráce a podporovatele aktivit ENISA.

ENISA i v roce 2016 pokračovala v poskytování poradenství Evropské komisi a členským státům EU při tvorbě a implementaci politik týkajících se kybernetické bezpečnosti, koordinovala opatření vydávaná pro zabezpečení jejich sítí a informačních systémů a prostřednictvím kurzů a školení podporovala budování kapacit CERT v jednotlivých členských státech. Zaměřila se přitom zejména na témata a výzvy související s nově přijatou evropskou směrnicí NIS.

4.3 Severoatlantická aliance (NATO)

Nejvýznamnější události v NATO se stal varšavský summit, během něhož uznali nejvyšší představitelé členských států kybernetický prostor jako další operační doménu. Cílem bylo vyzdvihnout roli, kterou kybernetická obrana a bezpečnost (v terminologii NATO „cyber defence“) hraje v aliančních operacích. Bylo také znovu zdůrazněno, že kybernetická obrana je součástí kolektivní obrany a že Spojenci jsou připraveni uplatnit tento princip i dle čl. 5 Severoatlantické smlouvy.

Během summitu byl přijat také Cyber Defence Pledge, na jehož finální podobě se podílelo i NCKB. Státy se v tomto dokumentu zavázaly budovat a posilovat bezpečnost národních sítí a informační infrastruktury a navýšit tak svou i alianční odolnost proti kybernetickým útokům. V návaznosti na Cyber Defence Pledge schválila Severoatlantická rada metriku, jejímž cílem je zhodnotit, zda spojenci vskutku navyšují své kybernetické schopnosti, jak se na summitu zavázali. Za Českou republiku bude hodnocení zpracovávat NBÚ spolu s Ministerstvem obrany. První zprávu o stavu českých kybernetických schopností odevzdají členské státy NATO v únoru 2017.

Na spolupráci s NATO se v oblasti kybernetické obrany podílí i Ministerstvo obrany. Spolu s NBÚ spolupracují na přípravě pozic na jednání v Cyber Defence Committee (CDC)

a v případě potřeby i jiných orgánů NATO. Společně se v roce 2016 také účastnily aliančních cvičení Cyber Coalition a Locked Shields. [7]

Jednání Severoatlantické rady a CDC podpořilo NCKB v roce 2016 i přípravou analýz aktuálního dění v kybernetickém prostoru. Tyto analýzy sloužily velvyslanci ČR při NATO jako podklady pro jednání a v rámci CDC byly distribuovány zástupcům aliančních států.

Česká republika na půdě NATO pokračovala v aktivní účasti na dvou Smart Defence projektech. Prvním z nich je Multinational Cyber Defence Education and Training (MN CD ET), jehož národním kontaktním bodem je zaměstnankyně NBÚ. Cílem projektu je vyplnit mezery ve vzdělávání a školení v oblasti kybernetické obrany a bezpečnosti. ČR v rámci projektu nadále rozvíjela svou činnost ve dvou pracovních skupinách. V první z nich pokračovala ve vytváření společné taxonomie. Ve druhé se podílela na přípravách vzniku magisterských programů zaměřených na mezinárodní právo v kybernetickém prostoru a na technický aspekt kybernetické bezpečnosti. Zástupci Masarykovy univerzity, kteří jsou do projektu spolu s NBÚ zapojeni, nabídli pro potřeby těchto programů výuku několika předmětů. Zejména jejich předměty zaměřené na právní otázky kybernetické bezpečnosti byly členy projektu hodnoceny velmi pozitivně.

Druhým Smart Defence projektem byl Multinational Malware Information Sharing Platform (MN MISP), na jehož účasti pokračovalo v roce 2016 Ministerstvo obrany. Cílem projektu je poskytovat platformu pro sdílení technických informací o škodlivém kódu a bezpečnostních incidentech. Spojenci a partnerské země zapojené do projektu řešili možnosti rozšíření funkcionality provozované platformy, tak aby mohlo dojít k efektivnějšímu sdílení informací a tím k rychlejšímu rozpoznání kompromitace systému a zvýšila se pravděpodobnost detekování infekce.

Česká republika se již třetím rokem také aktivně podílela na činnosti NATO Cooperative Cyber Defence Centre of Excellence (CCDCoE), které se zaměřuje na výzkumnou a vědeckou činnost v oblasti kybernetické bezpečnosti a obrany. ČR je členem Řídícího výboru (Steering Committee) centra a do jeho právní divize byl počátkem roku 2014 vyslán pracovník NBÚ a na základě jeho pracovních výsledků požádalo vedení centra o prodloužení jeho vyslání o další rok. Jako tzv. voluntary national contribution publikuje analýzy, podílí se na přípravě kybernetických cvičení a organizaci konferencí pořádaných centrem. Jednou z těchto konferencí je světově známý CyCon. Během letošního ročníku na něm vystoupila i zástupkyně NCKB, která prezentovala český přístup k institutu kybernetického nebezpečí definovaného v ZKB.

[7] Viz kapitola 4.12

4.4 Organizace pro bezpečnost a spolupráce v Evropě (OBSE)

Práce OBSE v oblasti opatření pro budování důvěry a předcházení konfliktů v souvislosti s aktivitami v kyberprostoru, tzv. kybernetických CBMs („*Confidence building measures*“) v roce 2016 dosáhla dalšího milníku, když v březnu 2016 účastnické státy přijaly druhou sadu kybernetických CBMs.

V doplnění k první sadě z roku 2013 se účastnické státy v rámci specializované neformální pracovní skupiny dohodly na dobrovolné bázi podporovat semináře, debaty a jiné kooperativní mechanismy umožňující výměnu informací, podporovat využívání chráněných komunikačních kanálů svými představiteli a experty a vyjasňovat si technické, právní a diplomatické mechanismy týkající se žádostí souvisejících s využíváním ICT, rozvíjet partnerství veřejného a soukromého sektoru, regionální a subregionální spolupráci či podporovat mechanismy pro koordinované zveřejňování zranitelností.

Kromě nových CBMs účastnické státy jednaly o možnostech implementace přijatých CBMs. V té souvislosti v listopadu 2016 proběhlo první cvičení spočívající v ověření prostupnosti komunikačních kanálů („ComCheck“).

Pro Českou republiku, zastoupenou v předmětné pracovní skupině NBÚ a MZV, je tato platforma mj. užitečným zdrojem informací o postojích a politikách v oblasti kybernetické bezpečnosti uplatňovaných státy mimo EU či NATO.

4.5 Central European Cyber Security Platform (CECSP)

Středoevropská platforma kybernetické bezpečnosti byla založena z české a rakouské iniciativy v květnu 2013. Jejími členy jsou vedle dvou zmíněných zemí ještě Maďarsko, Polsko a Slovensko a jejím hlavním úkolem je vytvořit vhodné prostředí pro sdílení know-how a osvědčených postupů mezi zeměmi, které k sobě mají tradičně blízko.

Poslední technické jednání CECSP roku 2016 se uskutečnilo v říjnu. Česká republika na něm prezentovala svůj vývoj v oblasti kybernetické bezpečnosti a pokračovala v diskuzi nad sdílením technických informací, včetně používaných standardů a nástrojů.

4.6 OECD

V roce 2016 se NBÚ coby národní gestor kybernetické bezpečnosti zapojil do činnosti mezirezortní pracovní skupiny MZV pro spolupráci ČR s Organizací pro ekonomickou spolupráci a rozvoj. Problematika kybernetické bezpečnosti má důležité místo i v ekonomickém rozvoji, na který se tato organizace zaměřuje; odráží se např. v instrumentech týkajících se řízení digitálních bezpečnostních rizik, rozvoje digitální ekonomiky nebo ochrany práv spotřebitele, které OECD přijala v letech 2015-2016.

V roce 2017 proto NBÚ chce dále rozvíjet spolupráci s MPO, zejména ve vztahu k zastoupení České republiky v pracovní skupině OECD pro informační bezpečnost a soukromí

4.7 Bilaterální a další spolupráce

V roce 2016 došlo k významnému prohloubení vztahů se Spojenými státy a Izraelem, v nichž začali působit čeští cyber attachés. Spolupráce byla posílena i s dalšími zahraničními partnery, ke kterým patří Korejská republika či Singapur.

Působení kybernetického odborníka v Tel Avivu bylo v roce 2016 primárně zaměřeno na vybudování povědomí mezi hlavními izraelskými hráči v oblasti kybernetické bezpečnosti o procesu implementace zákona o kybernetické bezpečnosti v České republice.

Vedle vyslání cyber attaché bylo významnou událostí v česko-izraelských vztazích podepsání Memoranda o porozumění. Memorandum, které bylo podepsáno během květnového jednání vlád (G2G), vytvoří užší rámec spolupráce mezi NBÚ a izraelským Národním úřadem pro kybernetickou bezpečnost (NCSA - National Cyber Security Authority). V návaznosti na závěry jednání G2G proběhla v polovině prosince v prostorách MZV prezentace izraelských a českých firem v oblasti kybernetické bezpečnosti. Na organizaci semináře se za českou stranu podílel Svaz průmyslu a dopravy, Ministerstvo obrany a Česko-izraelská smíšená obchodní komora. Hlavním cílem semináře byla výměna zkušeností na vládní úrovni při ochraně kritické infrastruktury a setkání českých a izraelských firem vyvíjejících řešení pro ochranu před kybernetickými hrozbami.

Na základě výše zmíněného memoranda jak NBÚ, tak NCSA začaly pracovat na vytvoření zabezpečeného komunikačního kanálu a jednat o možnosti uskutečnění strategického table-top cvičení přepraveného NBÚ pro seniorní představitele státní sféry. Jak je popsáno v kapitole 4.11.4, scénář tohoto cvičení byl několikrát úspěšně odzkoušen v USA. Izraelská strana také projevila zájem zúčastnit se českých technických kybernetických cvičení jako pozorovatel.

Dalším z projektů mezi ČR a Izraelem je NATO Science for Peace and Security Programme (SPS). Hlavním tématem projektu je ochrana kritické informační infrastruktury a budování povědomí o kybernetických hrozbách. Projekt má být realizován v roce 2017 a zúčastní se ho nejen zástupci ČR a Izraele, ale i dalších států, které budou k účasti na projektu přizvány.

Strategická spolupráce byla prohloubena i se Spojenými státy americkými. Vyslání českého cyber attaché na zastupitelský úřad ve Washingtonu, D. C., vedlo k navázání kontaktů s představiteli několika amerických státních institucí, mezi něž patřila ministerstva vnitřní bezpečnosti a zahraničí. Komunikace byla zahájena i se zástupci ministerstva energetiky a jeho podřízeného pracoviště Idaho National Laboratory, které se specializuje na výzkum a vývoj ochrany kritické informační infrastruktury nejen v oblasti jaderné energetiky.

Spolupráce s Ministerstvem energetiky byla v září podpořena návštěvou vedení NBÚ a NCKB, během níž proběhlo jednání i s přední expertkou na kybernetickou bezpečnost Melissou Hathaway a zástupci National Cyber Forensics and Training Alliance v Pittsburghu. V druhé polovině roku pak byla navázána spolupráce s americkým ICS CERT (Industrial Control Systems), jejíž součástí byla návštěva zaměstnanců NCKB ICS laboratoří v Idahu spojená se cvičením.

V rámci spolupráce NBÚ a americké FBI se vedoucí pracovník NCKB účastnil dvouměsíční stáže v National Cyber-Forensics and Training Alliance (NCFTA). Hlavním cílem stáže, na kterou byli vysláni zástupci států z celého světa, bylo navázat spolupráci při sdílení informací o kybernetických incidentech a o probíhajících vyšetřování kybernetických zločinů. Poznatky o kooperaci veřejného sektoru se soukromými organizacemi a akademickým světem, která v USA efektivně funguje, použije NCKB při budování svých nových kybernetických kapacit.

Kontakty byly navázány i s americkými akademickými institucemi George Washington University a Georgetown University. Na National Defense University ve Washingtonu pak český cyber attaché představil činnost NBÚ v oblasti kybernetické bezpečnosti.

V rámci naplňování strategického partnerství ČR s Korejskou republikou, uzavřeného v roce 2015 proběhly c červnu 2016 první bilaterální konzultace o otázkách kybernetické bezpečnosti. Za českou stranu na jejich přípravě spolupracoval NBÚ s MZV, MPO, MO a MV. Účastnící debatovali o národních přístupech k zajišťování kybernetické bezpečnosti a k ochraně kritické informační infrastruktury, o rozvoji mezinárodních norem pro kyberprostor, možnostech dvojstranné spolupráce nebo perspektivách regionálních globálních aktivit, jichž se obě země účastní. Korejská delegace vyjádřila zájem uspořádat druhé kolo konzultací v roce 2017 v Soulu.

Bilaterální spolupráce s Velkou Británií byla navázána ještě před reorganizací jejího systému zajišťování kybernetické bezpečnosti a pokračovala i po vzniku nového britského Národního centra kybernetické bezpečnosti.

Ve vztahu k Singapuru se zástupci NBÚ v říjnu zúčastnili Singapore International Cyber Week, v jehož rámci aktivně participovali na mezinárodním sympoziu „International Cyber Leaders´ Symposium“ k tématu „Building Secure and Resilient Cyberspace“. Návštěva jim poskytla příležitost iniciovat bilaterální spolupráci se Singapurem v oblasti kybernetické bezpečnosti.

NBÚ v roce 2016 pokračoval v poskytování asistence státům, které budují svůj systém kybernetické bezpečnosti. Tento rok se Úřad v rámci dvou evropských projektů zaměřil na balkánské státy.

V rámci pokračujícího projektu Enhancing Cyber Security český zástupce spoluorganizoval workshop pro členy makedonských, kosovských a moldavských CERT/CSIRT týmů,

který se konal v Kišiněvě. Hlavním cílem bylo předat zkušenosti s budováním obdobného pracoviště v České republice. Workshop byl rozdělen do dvou částí – technické a teoretické. Obě vedle přednášek obsahovaly i cvičení, během nichž měli účastníci za úkol řešit bezpečnostní incidenty.

V rámci instrumentu TAIEX školili pracovníci NCKB představitele organizací ze šesti balkánských zemí, kteří se ve svých státech zabývající kybernetickou bezpečností. Čeští zástupci jim předávali zkušenosti s tvorbou koncepčních materiálů, ochranou KII či s tvorbou kybernetických cvičení.

4.8 Spolupráce se soukromým sektorem

Vytvoření spolehlivého prostředí pro sdílení informací a zajištění bezpečnějšího kyberprostoru nelze dosáhnout bez pomoci soukromého sektoru a předních technologických společností. NBÚ v únoru 2016 podepsalo memorandum o porozumění se společností Cisco, na jehož základě byly vytvořeny podmínky pro výměnu informací o bezpečnostních hrozbách, trendech a osvědčených postupech mezi oběma organizacemi. Memorandum navázalo na již smluvně upravenou spolupráci České republiky s Microsoftem, se kterým se ČR stala třetí zemí na světě, která se zapojila do bezpečnostního programu „Botnet Feeds“.

4.9 GÉANT / Trusted Introducer

GovCERT.CZ je již od roku 2014 akreditovaným členem evropského sdružení Trusted Introducer. Tato instituce působí v rámci evropské organizace GÉANT a sdružuje bezpečnostní týmy vládní, národní, akademické a komerční sféry z celého světa. V rámci členství se GovCERT.CZ účastnil pravidelných neveřejných jednání této komunity, která slouží ke sdílení know-how, vyvíjených aplikací, zkušeností a informací o řešených incidentech. Dalším přínosem byla výměna dat a informací o nakažených stanicích, webových stránkách, zranitelnostech, kampaních a dalších informací užitečných pro CERT/CSIRT komunitu. V neposlední řadě GovCERT.CZ v roce 2016 těžil rovněž z přístupu k uzavřenému, šifrovanému mailing listu a ověřeným kontaktům, které v případě závažného problému slouží k včasnému varování zahraničních bezpečnostních týmů.

4.10 FIRST

FIRST (Forum for Incident Response and Security Teams) je celosvětová platforma, která sdružuje týmy zabývající se řešením incidentů. Tato platforma není omezena pouze na týmy typu CERT, ale jejími členy jsou i další bezpečnostní týmy z komerční, akademické a státní sféry, které se této problematice věnují. Úkolem FIRST je vytvářet prostor pro diskuzi a sdílení zkušeností mezi bezpečnostními týmy a podporovat aktivity související s předcházením vzniku incidentů a řešením incidentů. Každoroční konference, kterou FIRST pořádá, přivádí zástupce bezpečnostních týmů z celého světa na jedno místo a pomáhá tak ke zvyšování důvěry mezi bezpečnostními týmy.

Vládní CERT se stal členem této platformy v listopadu 2015. V roce 2016 GovCERT.CZ úspěšně prošel procesem certifikace a k 1. 4. 2016 se tak stal jejím plným členem. Plné členství mu zaručuje možnost účasti na jednáních a konferencích a také přístup k informacím sdíleným v rámci této platformy. Plné členství také slouží jako záruka určité vyzrálosti týmu a přispívá k vyšší důvěře zahraničních partnerů.

4.11 The Honeynet Project

Dva členové GovCERT.CZ jsou od roku 2015 součástí výzkumné organizace „Honeynet Project“ (Honeynet.org), kde se společně s kolegy převážně z univerzitního prostředí podílejí na vývoji nových a úpravách stávajících open-source nástrojů využitelných pro boj s kybernetickými hrozbami. Do budoucna je plánováno zveřejňování nově získaných poznatků ze síťových pastí (honeypotů) v rámci komunity zapojené do projektu.

V průběhu roku pracovali zaměstnanci GovCERT.CZ na automatizovaném nasazení honeypotů s využitím nástroje Docker. Pokračovala optimalizace rozhraní pro sběr, uložení a vizualizaci dat zachycených honeypoty GovCERT.CZ. Toto rozhraní by mělo být k dispozici pro případné zájemce. Data zachycená honeypoty GovCERT.CZ budou zaslány na centrální kolektor a k dispozici pro analytickou práci pak budou v podobě vizualizací a detailního filtrování jednotlivých dat. V období od 1. 1. 2016 do 31. 12. 2016 honeypoty GovCERT.CZ zaznamenaly celkem 595014 útoků.

4.12 Mezinárodní kybernetická cvičení

Cvičení kybernetické bezpečnosti jsou dlouhodobě vnímána jako vhodný nástroj pro testování technických znalostí a schopností, pro ověření komunikačních kanálů, rozhodovacích pravomocí a interních postupů při řešení kybernetických bezpečnostních incidentů. Cvičení jsou rovněž vhodným nástrojem pro poukázání na nedostatky a následné navržení opravných prostředků. Česká republika se pravidelně účastní řady mezinárodních cvičení kybernetické bezpečnosti, ve kterých její představitelé obsazují přední pozice. NBÚ pak i sám pro zahraniční partnery cvičení pořádá.

4.12.1 Locked Shields

Česká republika se i v roce 2016 zapojila do v pořadí již sedmého ročníku největšího mezinárodního technického cvičení kybernetické bezpečnosti Locked Shields (LS16). Toto cvičení je každoročně pořádáno NATO CCDCoE v Tallinnu v Estonsku. Cvičení se konalo ve dnech 18. – 22. dubna 2016 a zapojilo se do něj přes 500 lidí. Za účelem co nejreálnější simulace byly použity nejnovější technologie, síťové prvky a útočné metody. Cvičení se odehrávalo ve speciálním virtualizovaném prostředí s desítkami počítačů a serverů, kde stál tzv. červený tým útočníků proti modrým týmům obránců. Úkolem modrých týmů bylo bránit se připraveným hacktivistickým kampaním, špionážním, sabotážním a ostatním kybernetickým útokům vedených na jejich sítě členy červeného týmu.

Český modrý tým byl složen ze zástupců bezpečnostních týmů státní, komerční i akademické sféry a obsadil přední příčky žebříčku složeného z 20 týmů z celkem 19 zemí. V rámci právních scénářů český tým dosáhl rovněž nadprůměrného výsledku.

Česká republika byla v roce 2016 opět zastoupena nejen vlastním modrým týmem, ale i dvěma pracovníky NCKB, kteří podpořili bílý tým, jenž se podílí na celkové organizaci, tvorbě scénářů a také na hodnocení připravených úkolů. Účast českého modrého týmu i přidělených zástupců v bílém týmu byla potvrzena i v příštím ročníku cvičení.

4.12.2 Cyber Coalition

V roce 2016 se Česká republika v zastoupení MO a NBÚ již po šesté zúčastnila mezinárodního aliančního cvičení kybernetické bezpečnosti Cyber Coalition. Účast obou složek byla umožněna na základě Memoranda o porozumění a spolupráci v oblasti kybernetické obrany mezi NATO a Českou republikou. Primárním záměrem bylo procvičit technickou i netechnickou koordinaci při řešení kybernetických bezpečnostních incidentů a zlepšit vzájemnou informovanost o stávajících obranných schopnostech. Do cvičení se zapojilo více než 700 techniků a IT odborníků, vládních zaměstnanců a expertů na kybernetickou bezpečnost z 33 států. Na národní úrovni bylo cvičení organizováno zástupci MO a NBÚ a účastnily se ho tzv. společné týmy složené ze zástupců několika resortů. Mezi ně patřili zástupci státní správy (MO, NBÚ, Úřad pro zahraniční styky a informace, Bezpečnostní informační služba, Vojenské zpravodajství, Ministerstvo zahraničních věcí, Policie), soukromého sektoru (CSIRT.CZ) a akademické sféry (CSIRT-MU). Česká republika si vedla nadprůměrně ve všech scénářích.

4.12.3 CMX

Ve dnech 9. – 16. března 2016 proběhlo cvičení orgánů krizového řízení NATO CMX 2016. Jedná se o procedurální cvičení orgánů krizového řízení a je plánováno společným úsilím velitelství NATO a strategického velitelství NATO (SHAPE). Jeho záměrem je procvičit pracovní postupy v rámci konzultací a kolektivního rozhodování na úrovni vedení Aliance dle čl. 5 Severoatlantické smlouvy, včetně detailního plánovacího procesu a demonstrace alianční připravenosti ke kolektivní reakci v situacích dle čl. 4 a 5 Severoatlantické smlouvy. Hlavním tématem letošního cvičení bylo řešení krizové situace ve východní a jihovýchodní Evropě, kde došlo k napadení spojenců protivníky z východního a jižního směru současně. Kybernetické útoky představovaly pouze jednu z linek celého scénáře.

Za Českou republiku se cvičení CMX 2016 mimo jiné účastnily následující subjekty: Stálá delegace ČR při NATO (SD ČR); Vláda ČR; Bezpečnostní rada státu; Ústřední krizový štáb; krizové štáby a další určení pracovníci ÚSÚ. Dále se cvičení účastnili zástupci z ministerstev, zpravodajských služeb a další.

4.12.4Table-top cvičení pro zahraniční partnery

V roce 2016 NBÚ opět uspořádal dvě cvičení připravená na míru pro zahraničního partnera. Akce se skládala ze specializovaného školení a návazného strategického table-top cvičení reflektující aktuální dění ve světě.

První cvičení proběhlo v červnu na zastupitelském úřadě ve Washingtonu, D.C. Cvičení bylo zorganizováno za pomoci zde vyslaného cyber attaché. Akce se účastnili zástupci diplomatického sboru, různých think-tanků a bezpečnostní komunity z České republiky, Slovenska, Polska, Maďarska, Estonska a Spojených států amerických. Druhé cvičení se uskutečnilo na Velitelství pro transformaci NATO ACT v Norfolku. Účastníky cvičení zde byli civilní a vojenští činitelé z různých divizí mezinárodního sekretariátu. Na základě hodnocení účastníků doporučilo NATO ACT, aby se cvičení připravené NCKB zařadilo do celo-aliančních NATO cvičení.

Všichni účastníci ocenili aktuálnost událostí ve scénáři, které jim umožnily lépe pochopit propojení politického vývoje a kybernetických incidentů ve střední a východní Evropě.

4.12.5Cyber Europe

Cvičení Cyber Europe je organizováno každé dva roky agenturou ENISA. Letos se jej zúčastnili zástupci z 26 zemí EU a Evropského sdružení volného obchodu. Toto technicko-operační cvičení začalo v dubnu 2016. V polovině října pokračovalo dvoudenním technickým cvičením, kde se sešli zástupci z více než 300 organizací zahrnující národní a vládní centra kybernetické bezpečnosti, ministerstva, evropské instituce a další. V tomto roce byl ve scénáři zařazen rozsáhlý blackout. Za Českou republiku je primárním zástupcem národní CERT, jenž plní koordinační roli. NBÚ/GovCERT.CZ se účastnil obou fází konaných v roce 2016.

5. NÁRODNÍ SPOLUPRÁCE

Široká spolupráce na národní úrovni je nezbytná pro zajištění kybernetické bezpečnosti České republiky. NBÚ jako národní gestor dané oblasti aktivně spolupracuje s ostatními rezorty státní sféry a snaží se tak udržovat jednotný postoj ČR směrem do zahraničí. Spolu s akademickou sférou se podílí na přípravě budoucích odborníků a na navyšování povědomí o kybernetické bezpečnosti. S bezpečnostními týmy CSIRT sdílí informace a zkušenosti se zranitelnostmi a podílí se na vývoji nových technických nástrojů.

5.1 Spolupráce vládního CERT a CSIRT.CZ

Vládní tým CERT a národní tým CSIRT.CZ mezi s sebou tradičně sdílí informace, zkušenosti a know-how týkajících se zranitelností. V rámci českého zapojení v projektu The Honeynet Project také spolupracují na přípravě sdílení informací z honeynetů a společně se účastní mezinárodních cvičení kybernetické bezpečnosti.

Sdružení CZ.NIC, coby provozovatel Národního CERT týmu, v rámci projektu PROKI (Predikce a obrana před kybernetickými hrozbami), který byl podpořen v rámci programu Bezpečnostního výzkumu České republiky 2015-2020, zahájil v roce 2016 pilotní provoz a započal i zasílaní výstupních zpráv subjektům, které se dobrovolně do pilotního provozu nahlásily. Zároveň probíhalo rozšiřování dosavadních zdrojů dat o významná data z projektů, jako jsou například N6 nebo Shadowserver Foundation. V oblasti dalšího zlepšování incident handlingu sdružení vytvořilo a zveřejnilo nástroj na jednodušší automatizované zpracování rozsáhlých incidentů a automatizované rozesílaní adekvátních částí do koncových sítí spadajících do působnosti Národního CERT týmu. Celkově tým vyřešil od začátku roku do poloviny prosince 2016 přes 1 000 incidentů. Do služby na sledování škodlivého obsahu v doméně .CZ přidal k hledání phishingových stránek a stránek nakažených malwarem dohledávaní stránek s pozměněným obsahem (defacementem).

V roce 2016 se sdružení CZ.NIC a tým CSIRT.CZ zapojily do projektu Safer Internet a od července začali provozovat službu Internet Hotline, která slouží pro hlášení nezákonného obsahu na Internetu. Dle typu a závažnosti incidentů jsou pak hlášení předávána Policii České republiky k zahájení vyšetřování nebo jiným partnerům k řešení. V rámci prevence a vzdělávaní se členové týmu CSIRT.CZ účastnili jako řečníci na různých konferencích, pořádali školení pro odbornou i širokou veřejnost. Počet osvětových aktivit se zvýšil hlavně v měsíci říjnu, který je již tradičně věnován kybernetické bezpečnosti. Měsíc kybernetické bezpečnosti je organizován pod záštitou Evropské komise a Evropské organizace pro síťovou a informační bezpečnost (ENISA).

5.2 Spolupráce GovCERT.CZ s dalšími bezpečnostními týmy CSIRT

Spolupráce s českými bezpečnostními týmy probíhala zejména v oblasti sdílení informací. Týmy mezi sebou sdílely data a informace o kybernetických incidentech, o zkušenostech s jejich řešením a vývoji nových instrumentů. Konkrétním příkladem mohou být informace o zařízeních zapojených do botnetů, které vládní CERT každý den odeslal v průměru deseti českým CSIRT/CERT týmům.

Za účelem zefektivnění výměny informací spolupracuje GovCERT.CZ s CSIRTem Masarykovy univerzity (CSIRT-MU) a sdružením CESNET (CESNET-CERTS) na projektu Sdílení a analýza bezpečnostních událostí (SABU). Cílem projektu je vyvinout inteligentní analýzu a systém účinného předávání informací o kybernetických incidentech mezi bezpečnostními týmy v České republice. Ve finále by projekt SABU měl umožnit predikci dalšího vývoje útoků a tak omezit jejich dopad na národní kyberprostor. V roce 2016 proběhlo několik schůzek týkajících se vývoje tohoto projektu a jeho budoucího směřování. Nasazení SABU v ČR i zahraničí je plánováno na rok 2019.

Spolupráce NBÚ s bezpečnostními týmy probíhá i při cvičeních kybernetické bezpečnosti. Na národní úrovni udržuje GovCERT.CZ úzké vztahy s týmem CSIRT-MU. Spolupráce s ním proběhla v technické oblasti při přípravě a realizaci národních technických cvičení, kterými letos byly Cyber Czech 2015#2 a Cyber Czech 2016#1. S ohledem na cvičení mezinárodní je častým partnerem NBÚ Centrum CIRC v rezortu Ministerstva obrany (CIRC-MO), jehož pracovníci se spolu se zaměstnanci GovCERT.CZ podílí na řešení kybernetických scénářů.

5.3 Police ČR a zpravodajské služby

Pro zajištění kybernetické bezpečnosti země je také nezbytná spolupráce národní autority pro kybernetickou bezpečnost s organizacemi zodpovědnými za kybernetickou obranu ČR a boj s počítačovou kriminalitou, jimiž jsou Vojenské zpravodajství a Policie ČR. Zástupci těchto orgánů se každý měsíc scházejí a vyměňují si informace o aktuálních hrozbách, proběhlých incidentech či o důležitých událostech v oblasti kybernetické bezpečnosti.

Policie České republiky v roce 2016 pokračovala v plnění úkolů vycházejících z Akčního plánu k Národní strategii kybernetické bezpečnosti České republiky na období let 2015 až 2020. Byly provedeny potřebné organizační změny a především se navýšily personální kapacity organizačních článků, které se specializují na odhalování a vyšetřování kybernetické kriminality, expertizní činnosti, či servisní úkony. V personální oblasti se snaží Policie České republiky zvyšovat odbornou úroveň těchto pracovišť i získáváním specialistů z civilního sektoru a důraz je kladen také na další vzdělávací proces a odborný růst. Intenzivně se také pracuje na materiálovém zabezpečení dotčených pracovišť. V daných oblastech se nadále prohlubuje spolupráce Policie České republiky se subjekty státní správy i komerční sféry. Dlouhodobě se udržuje velmi dobrá spolupráce s Národním centrem kybernetické

bezpečnosti NBÚ, kdy se mimo jiné zástupci policie pravidelně účastní cvičení kybernetické bezpečnosti. Rozvíjí se i spolupráce se zahraničními partnery a Europolem. V těchto trendech bude Policie České republiky pokračovat i v dalším roce.

S Vojenským zpravodajstvím probíhalo v průběhu celého roku navazování spolupráce a poskytování konzultací k přípravě ICS laboratoří jejich vznikajícího centra kybernetických sil. V neposlední řadě probíhaly kontinuálně se všemi zpravodajskými službami ČR – Vojenským zpravodajstvím, Bezpečnostní informační službou a Úřadem pro zahraniční styky a informace, pravidelná setkávání a konzultace v oblasti kybernetické bezpečnosti.

5.4 Ministerstvo obrany

Ministerstvo obrany a NBÚ spolu úzce spolupracují jak na technické, tak na strategické úrovni. V průběhu roku 2016 spolu připravovaly podklady pro varšavský summit a jednání orgánů NATO a jako v předchozích letech spolupracovaly na řešení mezinárodních kybernetických cvičení.

MO provozuje šest významných informačních systémů stanovených v příloze č. 1 vyhlášky č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích. MO v roce 2016 zpracovalo návrh Strategie kybernetické bezpečnosti MO a Akční plán KB MO na období let 2017 až 2020.

Na mezinárodní úrovni MO spolupracuje zejména s NATO v rámci alianční politiky v oblasti kybernetické obrany a dále rozvíjí spolupráci s Evropskou unií/European Defence Agency a se zeměmi V4. Na bilaterální úrovni spolupracuje s ozbrojenými silami USA, Izraelem a dalšími státy. V roce 2016 se uskutečnily se např. rozhovory k navázání spolupráce mezi MO a zástupci Národní gardy Texasu a Nebrasky a představiteli Cyber Security Bureau Gruzie.

5.5 Audit národní bezpečnosti

Na začátku roku 2016 vytvořilo Ministerstvo vnitra na základě rozhodnutí Bezpečnostní rady státu skupinu, jejímž úkolem bylo připravit materiál analyzující odolnost ČR vůči bezpečnostním hrozbám a navrhnout potřebná opatření v nejrizikovějších oblastech. Ve spolupráci napříč státní správou tak na konci roku vznikl materiál, který se zabýval celkem deseti tématy a „Hrozby v kyberprostoru“ byly jedním z nich. Tato problematika byla rozčleněna do pěti konkrétních hrozeb, které významně ohrožují národní bezpečnost ČR:

I) Kybernetická špionáž

II) Narušení nebo snížení odolnosti IT infrastruktury

III) Nepřátelské kampaně

IV) Narušení nebo snížení bezpečnosti eGovernmentu

V) Kyberterorismus[8]

5.6 Další meziresortní spolupráce

Kybernetická bezpečnost je nedílnou součástí a předpokladem rozvoje digitální společnosti. Jako taková má své místo v implementaci digitální agendy na vnitrostátní úrovni. NBÚ proto v roce 2016 pokračoval ve spolupráci s Úřadem vlády a s koordinátorem pro digitální agendu, mj. na přípravě a implementaci Akčního plánu pro rozvoj digitálního trhu.

S rozvojem digitální společnosti je úzce spjata i příprava Národního cloud computingu. Aby bylo jeho zabezpečení a důvěryhodnost co nejvyšší, spolupracuje NBÚ spolu s Ministerstvem financí a Ministerstvem vnitra na tvorbě jeho strategického rámce.

S Ministerstvem vnitra dále proběhla spolupráce i na výše zmíněním auditu národní bezpečnosti a na vzájemných hodnocení pořádaných EU a její Pracovní skupinou pro obecné záležitosti (GENVAL).

5.7 Akademická sféra

Akademická obec hraje důležitou roli v zajišťování kybernetické bezpečnosti a patřím k tradičním partnerům NBÚ. Zástupci obou sfér se spolu podílí na přípravě budoucích odborníků, realizují kybernetická cvičení a sdílí spolu informace a zkušenosti o kybernetických incidentech.

NBÚ v roce 2016 úzce spolupracoval zejména s Masarykovou univerzitou v Brně. Vedle příprav národních cvičení probíhala spolupráce v technické rovině i mezi týmy CSIRT-MU při Fakultě informatiky a GovCERT.CZ.[9] V právnické rovině byla spolupráce započata již přípravou ZKB a v roce 2016 pokračovala konzultacemi o jeho novele. Na půdě Masarykovy univerzity proběhla i neformální setkání právníků zabývajících se kybernetickou bezpečností, tzv. CyberCake, kterého se účastnili odborníci z akademické obce, NBÚ, justice a dalších složek státní sféry.

V rámci přípravy budoucích expertů se Národní centrum kybernetické bezpečnosti podílelo na výuce předmětů na vysokých školách. Na Fakultě sociálních studií Masarykovy univerzity v Brně (FSS MU) a na Přírodovědné fakultě Univerzity Palackého v Olomouci zajišťovali jeho zástupci výuku předmětu „Kybernetická bezpečnost“. Na vybrané přednášky byli přizváni

[8] Detailní výsledky Auditu národní bezpečnosti jsou k dispozici zde: https://www.vlada.cz/cz/media-centrum/aktualne/audit-narodni-bezpecnosti-151410/

[9] Viz kapitola 4.12

i hosté z praxe z partnerských institucí. Pro studenty FSS MU byl předmět navíc obohacen exkurzí na hlavní pracoviště NCKB a praktickou ukázkou strategického Table-Top cvičení. Výuka předmětu se předpokládá i v roce 2017. Dílčí přednášky vybraných zástupců NCKB se rovněž konaly na CEVRO Institutu a Prague Security Studies Institute.

V souvislosti s rozvojem vzdělání v oblasti kybernetické bezpečnosti byl na základě proběhlého mapování na webových stránkách www.govcert.cz zveřejněn přehled vysokoškolských studijních programů/oborů/předmětů, které se vztahují k tématu kybernetické bezpečnosti, a to jak z technického, právního či bezpečnostně-politického hlediska. Jeho účelem je poskytnout snadnou orientaci ve studijních možnostech poskytovaných vysokými školami v České republice v souvislosti s touto problematikou. Přehled má sloužit široké veřejnosti, žákům středních škol, jejich pedagogům a akademické obci.

Zaměstnanci GovCERT.CZ pomáhali studentům s jejich závěrečnými pracemi. V uplynulém roce vedli dvě bakalářské a jednu diplomovou práci na téma honeypotů. Jedna z nich byla zaměřena na rozvoj klientského honeypotu, další se zaměřila na honeypot určený pro sběr malware a poslední cílila na rozvoj honeypotu honeyD. Průběžné výstupy byly publikovány na GitHubu GovCERT.CZ (https://github.com/GovCERT-CZ) a informace sdíleny jak v rámci české kapitoly, tak mezinárodně.

5.8 Národní cvičení

5.8.1 Cyber Czech 2015 #2

V polovině března zorganizovalo NCKB společně s Ústavem výpočetní techniky Masarykovy univerzity cvičení s názvem Cyber Czech 2015 II. Jednalo se o opakování cvičení, které bylo poprvé uspořádáno v říjnu předchozího roku. Hlavním cílem bylo ověřit praktické znalosti zvládání kybernetických bezpečnostních incidentů v souvislosti s ochranou kritické informační infrastruktury ČR a procvičit postupy podle zákona č. 181/2014 Sb., o kybernetické bezpečnosti, včetně komunikace s médii při zvládání nastalé krize. Cvičení se zúčastnili zástupci z řad subjektů státní správy a subjektů KII. Jejich úkolem bylo, stejně jako v říjnu předchozího roku, bránit informační infrastrukturu fiktivní jaderné elektrárny, na kterou útočil tým hackerů, tzv. červený tým, složený ze zaměstnanců NBÚ a Masarykovy univerzity.

5.8.2 Cyber Czech 2016 – table-top

Ve dnech 23. a 24. června 2016 proběhlo strategické cvičení kybernetické bezpečnosti Cyber Czech 2016, které bylo uspořádáno Národním centrem kybernetické bezpečnosti. Jednalo se o netechnické, tzv. Table-Top[10] cvičení, jehož primárním cílem bylo procvičit rozhodovací procesy na strategické úrovni nezbytné pro efektivní řešení krize v kybernetickém prostoru, což zahrnuje i procvičení komunikace a spolupráce mezi zapojenými subjekty. Cvičení navázalo na strategické cvičení, které bylo pořádáno NBÚ ve spolupráci s European Cyber Security Initiative (ECSI) a European Defence Agency (EDA) v červnu 2015.

K simulaci komunikace a spolupráce bylo na základě zkušeností a profesionálního zaměření cvičících vytvořeno několik pracovních skupin. Skupiny byly sestaveny následovně: vláda a orgány státní správy; zpravodajské služby a silové složky; orgány činné v trestním řízení a právní experti a soukromý sektor. V tomto roce byla poprvé vytvořena mediální pracovní skupina zastoupena reálnými novináři z různých zpravodajských deníků a skupina na úrovni vedoucích představitelů. Hlavním důvodem pro rozšíření pracovních skupin bylo navození větší realističnosti cvičení. Podle zpětné vazby se vytvoření těchto nových skupin velmi osvědčilo.

5.8.3 Cyber Czech 2016 #1 – technické

V druhé polovině října pořádal NBÚ, ve spolupráci s Ústavem výpočetní techniky Masarykovy univerzity v Brně, další národní cvičení v oblasti kybernetické bezpečnosti CYBER CZECH 2016. Tentokrát se jednalo o technické cvičení, které navazovalo na předchozí table-top cvičení z června 2016 a stalo se tak druhým technickým cvičením kybernetické bezpečnosti. Hlavním cílem cvičení bylo, stejně jak v předchozích cvičeních, ověřit praktické znalosti zvládání kybernetických incidentů v souvislosti s ochranou prvků KII a procvičit postupy podle ZKB včetně komunikace s médii při zvládání nastalé krize.

Tentokrát se cvičení v roli obránců, tzv. modrých týmů, zúčastnilo dvacet čtyři zástupců z řad organizačních složek států a subjektů KII. Zastoupeny byly rovněž subjekty ze soukromé a akademické sféry. Jejich úkolem bylo bránit informační infrastrukturu fiktivní železniční stanice a zabránit vykolejení vlaku s radioaktivním odpadem. Na informační systémy útočil tým hackerů, tzv. červený tým, složený ze zaměstnanců NBÚ/NCKB a Masarykovy univerzity. V letošním roce zde byla role medií zastávána reálnými novináři, kteří dotvářeli realističnost scénáře svými dotazy na jednotlivé týmy a následnými články, které publikovali na fiktivním zpravodajském portále.

[10] Table-Top je cvičení navržené k testování teoretických schopností cvičících reagovat ve skupině na určitou krizovou situaci. Velkou výhodu tohoto druhu cvičení představuje možnost vyzkoušet si jakoukoliv hypotetickou situaci bez rizika způsobení škody či jiných důsledků.

Cvičení zasazené do tohoto kontextu bude mít v roce 2017 ještě tři iterace, přičemž dvě z nich budou v anglickém jazyce pro zahraniční partnery.

5.8.4 CommCzech – komunikační cvičení

První ročník národního komunikačního cvičení se pod záštitou NCKB konal ve dnech 3. a 4. listopadu. Cvičení bylo zaměřeno na ověření průchodnosti neklasifikovaných komunikačních kanálů a aktuálnosti údajů nahlášených povinnými subjekty dle § 16 ZKB. Cvičení se skládalo ze dvou fází. V první proběhla zkouška elektronického spojení s cílem prověřit e-mailové adresy. Na základě rozeslaného e-mailu měly příslušné subjekty maximálně do 48 hodin reagovat a potvrdit jeho přijetí. Druhá fáze probíhala simultánně a ověřovala telefonické kontakty.

Cvičení bylo velmi přínosné, neboť identifikovalo několik povinných osob, jež byly vyhodnoceny jako telefonicky, elektronicky či oběma směry nedostupné. Příslušné subjekty byly informovány a na tuto povinnost upozorněny písemně. S ohledem na svou důležitost budou komunikační cvičení pravidelně opakována.

6. ZVYŠOVÁNÍ POVĚDOMÍ A OSVĚTA

Osvěta a podpora vzdělávání v oblasti kybernetické bezpečnosti patří mezi hlavní oblasti činnosti NCKB. V roce 2016 centrum navázalo na aktivity z předchozího roku, rozvinulo stávající spolupráci a uvedlo nové projekty.

6.1Seminář k zákonu o kybernetické bezpečnosti

Národní centrum kybernetické bezpečnosti organizovalo 13. září 2016 již 2. ročník celodenního semináře k zákonu o kybernetické bezpečnosti. Seminář byl pořádán pod záštitou Studentské komory Akademického senátu Fakulty podnikatelské VUT v Brně. Letošní 2. ročník měl za cíl informovat veřejnost o novinkách z oblasti činnosti NCKB, tedy zejm. se zaměřením na zákon o kybernetické bezpečnosti a na praktické zkušenosti z oboru kybernetické bezpečnosti. Semináře se zúčastnilo okolo 200 účastníků z řad odborné veřejnosti, zástupců povinných subjektů (zejm. správců KII/VIS) a studentů.

6.2 Školení pro zaměstnance veřejné správy

V rámci aktivit pro veřejnou správu uspořádalo centrum řadu školení týkajících se pravidel bezpečného využívání ICT technologií v zaměstnání a v soukromí. Jako první proběhlo celodenní školení pro zaměstnance Úřadu vlády ČR. Školení bylo věnováno zaměstnancům na všech stupních vedení a jeho obsahem byly současné hrozby a rizika, význam digitální hygieny, základní bezpečnostní pravidla a možné následky při jejich nedodržování včetně názorné ukázky, co způsobuje např. ransomware či keylogger. Obdobné školení jsme připravili i pro vedení Ministerstva pro místní rozvoj. Na toto školení navazovala prohlídka pracoviště NCKB s podrobným výkladem k činnosti.

6.3 „Kybernetická bezpečnost v organizacích“

V Moravskoslezském kraji se konalo dvoudenní školení s názvem „Kybernetická bezpečnost v organizacích“. Bylo zaměřeno na management kybernetické bezpečnosti v organizacích a jeho součástí byl rovněž workshop síťové analýzy. Cílovou skupinou byli manažeři IT bezpečnosti, manažeři kybernetické bezpečnosti, IT administrátoři, bezpečnostní architekti, implementátoři ISMS a další role vyplývající ze ZKB. Přednášejícími byli zástupci odboru kybernetických bezpečnostních politik i zástupci odboru vládní CERT. Školení zaznamenalo pozitivní ohlas a bylo o něj zažádáno i na rok 2017.

6.4 Další aktivity k Zákonu o kybernetické bezpečnosti a implementaci bezpečnostních opatření

Na základě požadavků iniciovaných povinnými subjekty se také uskutečnilo ještě několik seminářů, a školení k ZKB a implementaci bezpečnostních opatření, která byla vedena pracovníky odboru kybernetických bezpečnostních politik.

6.5 Stáže na NCKB

Součástí zvyšování povědomí o kybernetické bezpečnosti jsou i stáže určené vysokoškolským studentům. Účelem stáží je rozšířit znalosti studentů v problematice kybernetické bezpečnosti, seznámit je se základy praxe v bezpečnostní oblasti a fungováním státních institucí. V uplynulém roce v centru absolvovalo stáž 7 studentů s technickým, bezpečnostně-politickým i právním zaměřením. K závěru roku také proběhla informační kampaň a distribuce inzerátů s preferovanými oblastmi na příslušné vysoké školy. Stáže slouží i jako zdroj budoucích pracovníků NCKB.

6.6 Středoškolská kybernetická soutěž České republiky

Z pozice odborného garanta centrum podpořilo první ročník kybernetické soutěže, která je určena všem žákům středních škol ve věku 16 – 17 let. Cílem soutěže je zvyšovat povědomí a znalosti v oblasti kybernetické bezpečnosti, identifikovat mladé talenty a také poskytnout informační podporu středoškolským pedagogům. Aktivita má tři kola, načež ti nejlepší se budou moci kvalifikovat do Evropské kybernetické soutěže, která bude pořádána v listopadu 2017.[11]

6.7 Strukturovaný dialog pro žáky středních a základních škol.

Zástupci oddělení cvičení a vzdělávání z odboru kybernetických bezpečnostních politik se zúčastnili strukturovaného dialogu v rámci projektu Junulara II na téma „Bezpečnost na internetu“, kde vystoupili jako jeden z přednášejících subjektů. Akce byla určena žákům základních i středních škol, jejímž cílem byla spontánní diskuse a zodpovídání dotazů.

6.8 „Kybernetická bezpečnost: stát, jednotlivec, škola

V několika městech Moravskoslezského kraje proběhla série workshopů z cyklu „Mediální gramotnost pro učitele“ s názvem „Kybernetická bezpečnost: stát, jednotlivec, škola –“. Obsahem byla současná rizika a hrozby dnešní společnosti v souvislosti s využíváním moderních technologií, jak se změnilo vnímání kybernetické bezpečnosti z pohledu státu a jak se bránit kybernetickým útokům z pohledu jednotlivce.

Zde byla účastníkům také představena činnost Národního centra kybernetické bezpečnosti a Akční plán k NSKB, a návrh připravované koncepce vzdělávání v problematice kybernetické bezpečnosti, kde byla vyzdvižena potřeba vzdělávání a osvěty široké veřejnosti. Workshopy byly akreditovány MŠMT.

[11] Více informací o soutěži je k nalezení na www.kybersoutez.cz.

6.9 Pilotní fáze interaktivního vzdělávacího modulu Digitální stopa

Do pilotní fáze projektu se zapojilo celkem 8 školských zařízení (6 základních škol, 1 základní škola a víceleté gymnázium a 1 víceleté gymnázium) ze 4 krajů (Jihomoravský, Olomoucký, Moravskoslezský, Středočeský). Cílovou skupinou byli žáci 6. a 7. ročníků a modul vždy postupně absolvovaly všechny třídy. Celkem se jej dosud zúčastnilo přibližně 300 žáků.

Aktivita byla zaměřena na problematiku rizikového chování a závadového jednání v online prostředí. Ústředním tématem byla kyberšikana, sexting a dalších přidružené sociálně patologické jevy. Žáci zde pracovali s internetem a vybranými sociálními sítěmi. Zde měli formou „detektivní činnosti“, vyhledat klíčové informace a zrekonstruovat konkrétní fiktivní příběh. Nalezené indicie zadávali do e-learningového testu, který jim v závěru procentuálně vyhodnotil správnost jejich odpovědí. E-learning byl prokládán krátkými naučnými texty. Po dokončení testu proběhla shrnující diskuse v kruhu, kde žáci přednesli svá zjištění a chyby, kterých se smyšlené klíčově postavy dopustily. Zároveň měli podávat návrhy jak se v online prostředí chovat bezpečně. Na závěr byly žákům i učitelům předloženy krátké evaluační dotazníky pro poskytnutí zpětné vazby k aktivitě. Silnou stránkou zvyšující atraktivitu aktivity bylo propojení žáků s realitou, práce s moderními technologiemi a možnost využití i dalších moderních zařízení, což celkově podpořilo i rozvoj jejich klíčových kompetencí. Na základě výstupů z dotazníků lze konstatovat, že aktivita byla samotnými žáky i učiteli hodnocena pozitivně a dokázali by si ji představit jako součást běžné výuky.

Mezi hlavní zjištění patří nedostatečná znalost funkcí sociálních sítí, zejména nastavení zabezpečení mezi žáky a studenty. Přesto většina z nich účet např. na Facebooku měla založen a dokonce i nemalé množství žáků mladších třinácti let. Vedle tohoto žáci projevili omezené schopnosti při práci s internetovými vyhledavači a mapovými portály. Teoretické povědomí o problematice kyberšikany apod. sice díky různým preventivním programům pro školy mají, nicméně v praxi, zejména pak v souvislosti s využíváním sociálních sítí jsou jejich znalosti, především uvědomování si možných následků, značně omezené.

I přes nemalé množství preventivních programů na základních školských zařízeních je neustálá osvěta této početné a velmi zranitelné cílové skupiny nezbytná. Měla by být tedy prováděna co nejinteraktivnějším způsobem, aby si žáci získané znalosti zautomatizovali a transformovali je v běžné návyky.

6.10 Diář

I v roce 2016 NBÚ podpořil tvorbu Školního diáře 2015/2016, pro který opět poskytl dvojstránku některých příkladů závadového jednání na internetu a stránku pravidel bezpečného chování na internetu. Diář vydává nadnárodní občanské sdružení Generation Europe a vychází ze vzdělávacího modelu, který kombinuje zábavu a vzdělání. Diář je každoročně distribuován do škol po celé České republice.

6.11 Podpora projektu „Zvol si info“

Podporujeme projekt „Zvol si info“, který vznikl z iniciativy studentů humanitních oborů Masarykovy univerzity. Jeho cílem je zvyšování mediální gramotnosti zejména u mladých lidí a podpora kritického myšlení jakožto objektivního prostředku proti mediální propagandě a dezinformaci.

7. ČINNOST VLÁDNÍHO CERT (GOVCERT.CZ)

Vládní CERT i v roce 2016 soustavně rozšiřoval své kapacity a reflektoval tak neustále se zvyšující nároky především na jeho analytické schopnosti při šetření bezpečnostních incidentů.

Vládní CERT provozuje laboratoř pro zkoumání a testování ICS/SCADA systémů. Laboratoř byla založena v roce 2015 a během roku 2016 bylo dokončeno její budování. V současné době je laboratoř plně funkční. Přínos laboratoře se projevil během cvičení kybernetické bezpečnosti, kde vládní CERT dosáhl ve scénářích průmyslových řídících systému excelentních výsledků[12]. Další rozvoj tohoto pracoviště bude odrážet potřeby vládního CERT a budoucí technologický vývoj.

Dalším specializovaným pracovištěm vládního CERT je nově vzniklá forenzní laboratoř. Jejím účelem je poskytnout prostředí a nástroje pro práci na zajištěných fyzických zařízeních (počítače, mobilní telefony, paměťová média aj.), jejich analýzu a uložení při zajištění požadované úrovně zabezpečení těchto citlivých materiálů. Uvedení forenzní laboratoře do plného provozu je očekáváno v druhé polovině roku 2017.

Během roku 2016 bylo zahájeno poskytování služby formalizovaného penetračního testování. Tato služba je poskytována na základě smlouvy orgánům státní správy. Testování typicky probíhá v časovém rámci dvou týdnů. Výstupem každého testování je neveřejná zpráva shrnující nalezené zranitelnosti a nedostatky v konfiguraci systémů spolu s doporučeními pro zesílení bezpečnosti.

Vládní CERT dlouhodobě pracuje na rozvoji schopností detekce kybernetických útoků ve státní správě. Základním bodem této snahy je program nasazení síťových sond do klíčových orgánů státu. Síťové sondy získávají a uchovávají popisná data o provozu a poskytují tak materiál pro analýzu a vyšetřování incidentů. Zároveň dovolují rozsáhlou automatizaci a rozpoznávání škodlivých a nebezpečných aktivit. Realizace tohoto projektu je očekávána v roce 2017.

Schopnost efektivního vytěžování otevřených zdrojů informací získává globálně stále více pozornosti. Vládní CERT v tomto směru buduje základní kapacity a své úsilí spojuje s OKBP. Díky informacím tohoto původu bylo proaktivně zabráněno několika útokům plánovaným různými skupinami na systémy KII/VIS ČR.

Rozvoj kapacit vládního CERT probíhal v roce 2016 také na úrovni prohlubování technických znalostí specialistů vládního CERT. Zaměstnanci absolvují pravidelná odborná školení

[12] Více v kapitole 4.12

a úspěšně skládají odpovídající certifikační zkoušky. Kvalifikace pracovníků je rozvíjena také účastí na mezinárodních cvičeních kybernetické bezpečností, které přinášejí také cenné zkušenosti.

7.1 Nejvýznamnější incidenty šetřené GovCERT.CZ za rok 2016

V průběhu roku 2016 obdrželi pracovníci GovCERT.CZ od českých i zahraničních partnerů v souhrnu 298 relevantních hlášení o kybernetických bezpečnostních incidentech. Tato hlášení byla dále vyhodnocována ve vztahu k oblasti působnosti týmu GovCERT.CZ a následně zpracována buď vlastními prostředky, nebo předána příslušným subjektům. Za uplynulý rok tak bylo z přijatých hlášení a z informací získaných vlastními prostředky vyhodnoceno, zpracováno a vyřešeno 106 kybernetických bezpečnostních incidentů spadajících do oblasti působnosti vládního CERT, tedy KII, VIS a veřejné správy.

V rámci řešení incidentů byl vždy kladen důraz na rychlé kontaktování zodpovědných osob dotčených institucí a subjektů, případně dohledání dalších možných potenciálních obětí a jejich informování o možném riziku. Na základě zpětné vazby od dotčených subjektů víme, že díky varováním zaslaných vládním CERT týmem došlo k zabránění kybernetického útoku. Pokud by vládní CERT dostával zpětnou vazbu od všech subjektů, kterým varování posílá, byl by schopen dopad svých činností vyhodnotit lépe.

První čtvrtletí roku 2016 se vyznačovalo četnými malwarovými útoky, kdy útočníci na své oběti cílili pomocí sofistikovaných podvodných zpráv, které obsahovaly škodlivou přílohu nebo odkaz směřující na podvodné webové stránky. Prvotními cíli byli zákazníci bank, zaměstnanci státní správy a další skupiny.

V lednu se stal nejvážnějším řešeným incidentem případ několika stanic v ústředí vrcholné instituce státní správy, které byly infikovány bankovním malwarem TinyBanker.

K nejzávažnějšímu útoku za měsíc únor patřilo rozšíření malwaru Dridex v systémech KII, VIS a státní správy. Dridex se šířil za pomoci makra v dokumentech MS Office, nejčastěji jako příloha nevyžádaného emailu. Po otevření dokumentu se spustilo makro, které malware stáhlo do cílového zařízení. Dridex cílil na získání přístupových údajů do internetového bankovnictví a vytváření umělých platebních příkazů.

V březnu byl kromě obvyklých hlášení podvodných webových stránek a dalších případů šíření malware skrze přílohy nevyžádaných emailových zpráv zajímavý z hlediska incidentů případ pokusu o spuštění škodlivých skriptů na vysokých portech UDP. Pokus se odehrál na jednom z routerů instituce státní správy. Vzhledem k absenci zranitelností routeru, na které skripty cílily, však nedošlo k žádným škodám.

Ve druhém čtvrtletí roku se GovCERT.CZ setkával zejména s phishingovými a DDoS útoky, které cílily kromě státních institucí i na webové stránky některých politických subjektů a veřejnoprávních médií.

Měsíc duben se z pohledu nejvýznamnějších incidentů nesl v duchu phishingových zpráv. Od organizace CERT-EU byla například obdržena informace o možném doručení spear-phishingové zprávy obsahující škodlivou přílohu na adresy nejmenované státní instituce. Závadné emaily však zastavila antivirová ochrana na poštovním serveru a zprávy tak nebyly doručeny do uživatelských mailboxů. Analýza ukázala, že útok mohl být součástí rozsáhlejší Advanced Persistent Threat (APT) mezinárodní kampaně. Následně proběhla kontrola u podobných cílů, které mohly být kampaní také ohroženy.

V květnu byl nejzávažnějším incidentem DDoS útok na portál významné instituce státní správy, kdy se neznámým útočníkům podařilo tento portál krátkodobě vyřadit z provozu. V tomto období se též zvýšil počet pokusů o DDoS ze strany hacktivitického hnutí Anonymous, což následně způsobilo krátký výpadek služeb různých webových stránek.

Začátek i průběh léta pokračoval v trendu z měsíce května. V červnu i červenci pokračovaly hrozby DDoS útoků, zejména ze strany hacktivistických skupin, které se hlásily k hnutí Anonymous. Počátek třetího čtvrtletí se také vyznačoval řešením incidentů spojených s únikem dat z databází různých webových stránek a služeb, zejména privátních subjektů. Uniklé záznamy často obsahovaly citlivé osobní a přihlašovací údaje pracovníků veřejné správy a institucí spadající do KII a VIS.

V červenci, srpnu i září se kromě uniklých dat řešil i nárůst výskytu vyděračských emailů, které po adresátech požadovaly zaplacení finančního obnosu ve virtuální měně Bitcoin výměnou za neprovedení cíleného DDoS útoku či exfiltraci citlivých dat ze systémů oběti. Tyto případy byly řešeny ve spolupráci se zodpovědnými útvary PČR.

Poslední čtvrtletí 2016 bylo z pohledu statistik ve znamení extrémů. Tým GovCERT.CZ se nejdříve setkal s prudkým nárůstem řešených incidentů a v posledních měsících roku naopak došlo k jejich útlumu. Z hlediska kategorizace incidentů se setkával zejména s šířením ransomware a malwarových infekcí obecně, dále s phishingovými a DDoS útoky.

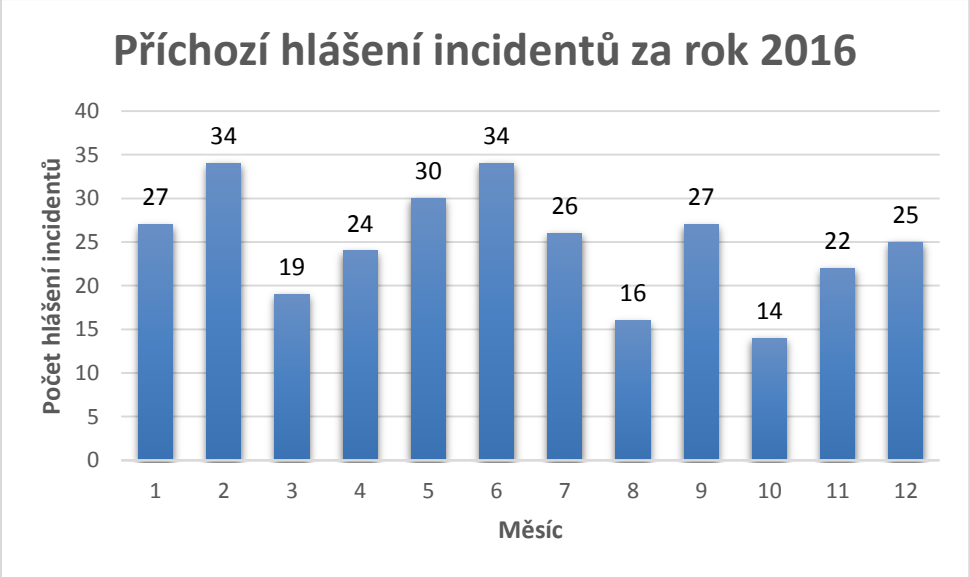
V měsíci říjnu byl zaznamenán letošní nejvyšší počet hlášených incidentů s pestrou paletou jejich typů. K nejzajímavějším patřil nahlášený případ zneužití techniky „techie talk“, což je forma sociálního inženýrství, při které se útočník snažil vydávat za jiného pracovníka a své oběti u jedné z finančních institucí podvodem přimět ke změně přístupových hesel.

Závěr roku již v menší intenzitě potvrzoval různorodost typů řešených incidentů a tak v listopadu i v prosinci pracovníci vládního týmu řešili zranitelnosti, výskyty ransomware a ojedinělé DDoS útoky na instituce státní správy.

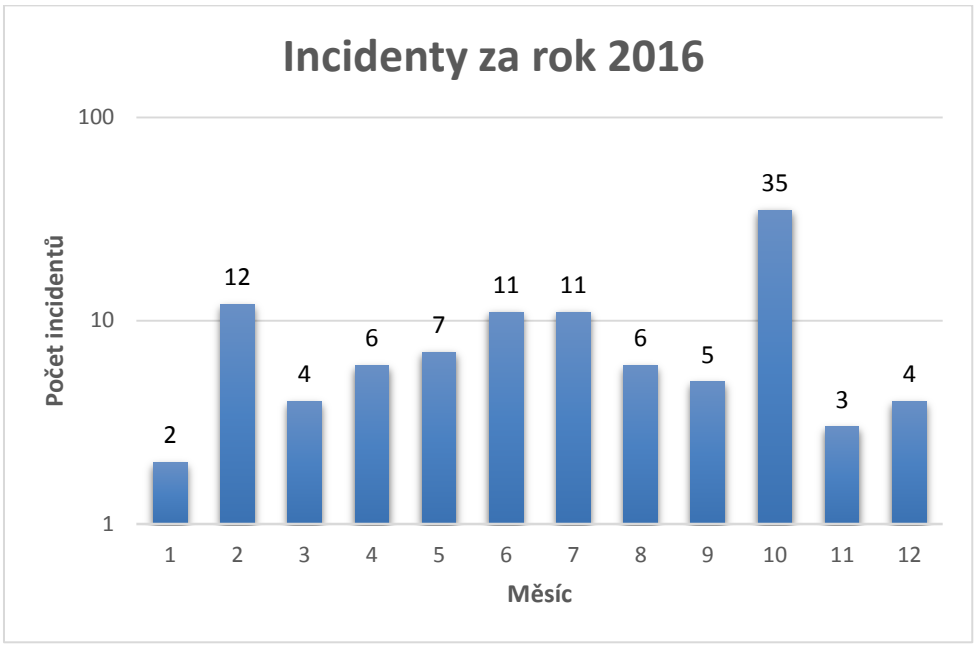
Národní bezpečnostní tým CSIRT.CZ v roce 2016 řešil ve své sféře působnosti obdobný počet incidentů jako v roce předchozím. Nejčastěji se jeho pracovníci setkávali s šířením ransomware a phishingovými útoky.

7.2 Statistické údaje o incidentech

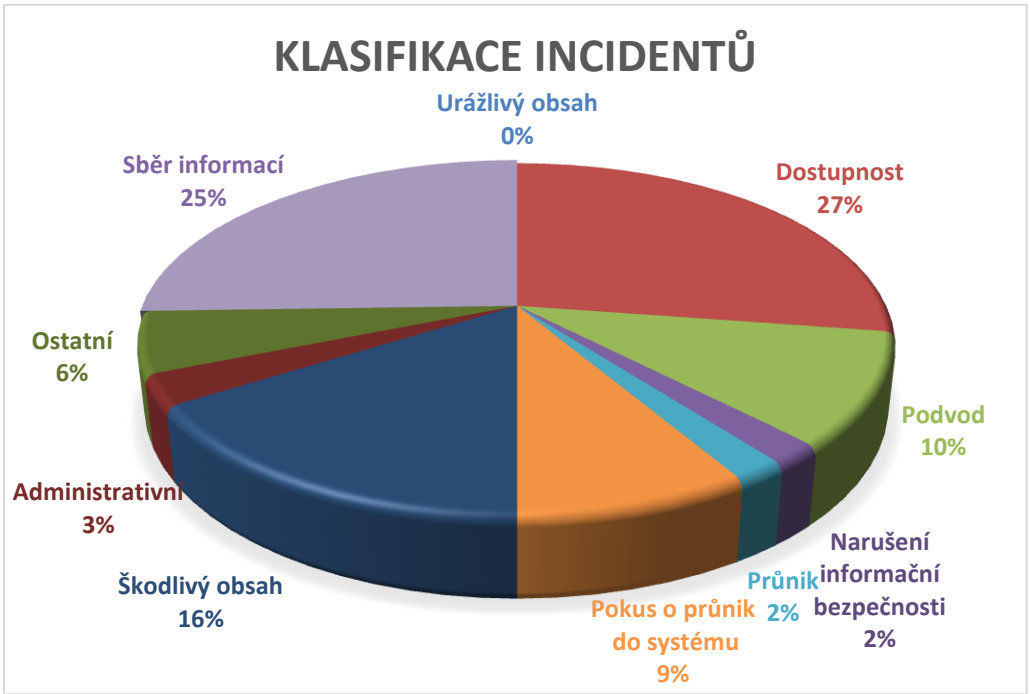
Grafy zachycují počty přijatých hlášení, řešených incidentů a jejich klasifikaci v roce 2016.



Graf 5: počet příchozích hlášení o incidentech za jednotlivé měsíce v roce 2016



Graf 6: počet řešených incidentů za jednotlivé měsíce v roce 2016[13]



Graf 7: klasifikace řešených incidentů za rok 2016

[13] Graf má osu „Y“ (počet incidentů) uvedenou v logaritmickém měřítku

Popis kategorií vychází z formuláře pro hlášení incidentů[14]:

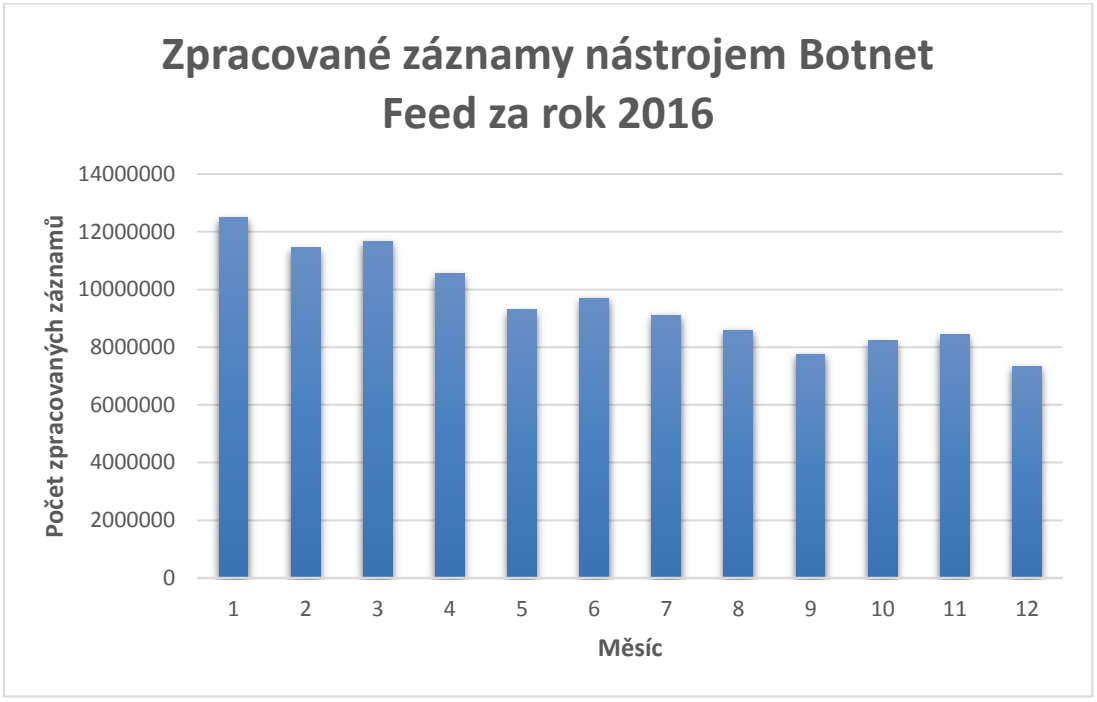
- Urážlivý obsah (např. spam, kyberšikana, nevhodný obsah)
- Škodlivý obsah (např. virus, červ, trojský kůň, dialer, spyware)
- Sběr informací (např. skenování, sniffing, sociální inženýrství)
- Pokus o průnik do systému (např. pokus zneužití zranitelnosti, kompromitace aktiva, "0-day" útok)
- Průnik (např. úspěšná kompromitace aplikace nebo uživatelského účtu)
- Dostupnost (např. narušení dostupnosti způsobené DoS/DDoS útokem nebo sabotáží)
- Narušení informační bezpečnosti (např. neautorizovaný přístup nebo neautorizovaná změna informace, atd.)
- Podvod (např. phishing, neoprávněné využití ICT - porušení licenčních práv, krádež identity, aj.)
- Administrativní = tato kategorie se liší od kybernetických incidentů. Příkladem může být soudní rozhodnutí o vypnutí systému, který je součástí KII / VIS

7.3 Projekt Botnet Feed

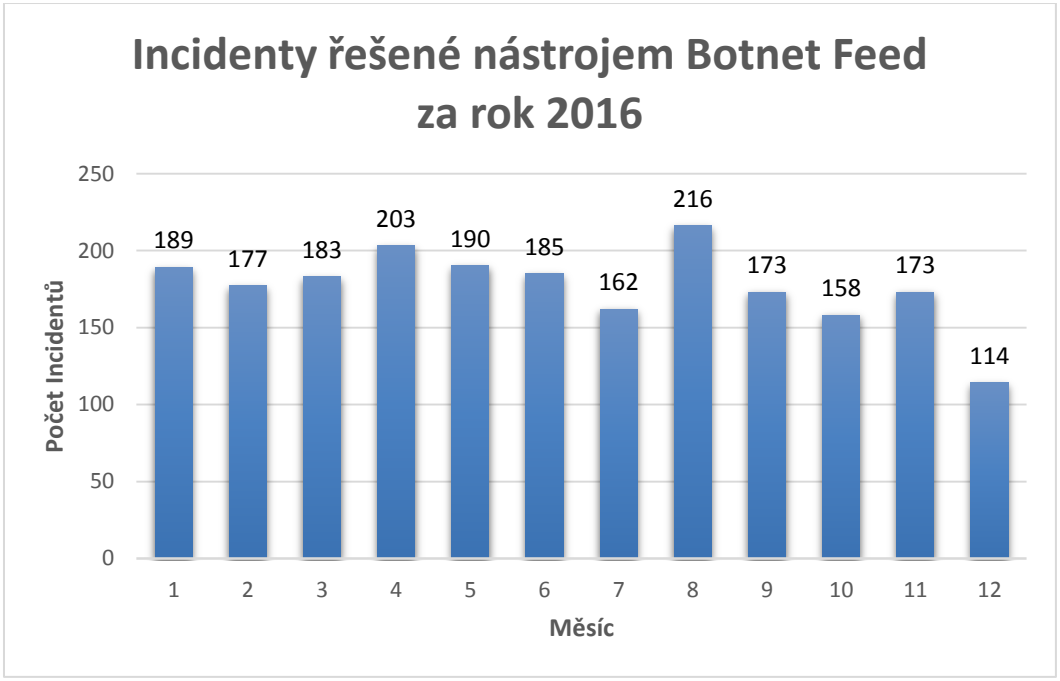
V rámci svých proaktivních činností GovCERT.CZ pomocí několika nástrojů analyzuje data z uzavřených i veřejně dostupných zdrojů, jež obsahují indikátory o kompromitaci systémů. Nejdůležitějším nástrojem je Botnet Feed, který je vyvíjen týmem GovCERT.CZ za účelem sběru a zpracování dat o koncových stanicích zapojených do sítí botnetů. Data jsou získávána ze zajištěných řídících serverů (C&C). Původcem dat je společnost Microsoft.[15] V roce 2016 probíhal proces navazování spolupráce s dvěma novými bezpečnostními CERT/CSIRT týmy, které by mohly rozšířit množinu odběratelů dat z projektu. Se současným rostoucím počtem vznikajících bezpečnostních týmů se předpokládá i zvyšování odběratelů dat v nadcházejícím období. Převážná část reportů je určena komerční sféře (ISP/poskytovatelé hostingových služeb). Denně je exportováno přibližně 10 MB reportů ve strojově čitelném formátu. Od ledna do prosince roku 2016 bylo zpracováno a vyhodnoceno přibližně 114,5 milionů záznamů o potenciálních bezpečnostních hrozbách v České republice. Celkem bylo partnerům a institucím spadajících do působnosti GovCERT.CZ odesláno 2123 reportů.

V následujících grafech je v rámci proaktivního projektu Botnet Feed uveden měsíční přehled počtu zpracovaných záznamů za rok 2016 a počet kybernetických incidentů řešených pracovníky GovCERT.CZ.

[14] K dispozici na: https://www.govcert.cz/cs/vladni-cert/hlaseni-incidentu/
[15] GovCERT.CZ doposud odebírá data týkající se 14 botnetů, mezi kterými jsou např. Bamital, Citadel, Conficker, Kelihos, Zeus, Simda, Ramnit, Dorkbot a další.



Graf 8: počet zpracovaných záznamů za rok 2016



Graf 9: počet incidentů za rok 2016 s rozdělením po měsících

PŘÍLOHY

Příloha č. 1: Nejčastější zjištění z kontrol KII/VIS

Systém řízení bezpečnosti informací (ISMS)

a) Podpora vedení

Podpora vrcholového vedení je pro správné řízení kybernetické bezpečnosti naprosto klíčová.

b) Bezpečnostní politiky

Častým zjištěním kontrolujících bylo, že předložená bezpečnostní politika kontrolovaného subjektu:

- nebyla formálně schválená a účinná – většina těchto případů byla způsobená zdlouhavým procesem schvalování interních dokumentů a týkala se převážně subjektů státní správy,
- nebyla úplná z hlediska požadovaného obsahu,
- nebyla řízená – nejsou stanoveny postupy a pravidla pro řízení dokumentace,
- nereflektovala potřeby organizace – nejčastěji v případech kdy byla dokumentace vytvořena třetí stranou bez přizpůsobení kontextu a potřebám organizace
- nebyla dodržována (nejčastěji se jednalo o nedodržení politikou stanovených pravidel, např. v oblasti klasifikace aktiv a manipulace s aktivy).

Řízení aktiv

Nejčastěji identifikovanými nedostatky v oblasti řízení aktiv byly:

- chybějící požadované metodiky pro řízení aktiv a související dokumentace,
- nedostatečná identifikace a klasifikace aktiv.

Řízení rizik

Nejčastěji identifikovanými nedostatky v oblasti řízení rizik byly:

- chybějící požadované metodiky pro řízení rizik a související dokumentace,

- nejednotný proces řízení rizik v rámci organizace (např. rizika jsou mnohdy řízena pouze v souladu se zákonem o finanční kontrole nebo jsou řízena samostatně na úrovni jednotlivých organizačních útvarů),
- chybějící požadované prohlášení o aplikovatelnosti (SoA) a plánu zvládání rizik (RTP),
- chybějící provázanost analýzy rizik, SoA a RTP.

Organizační bezpečnost

- Nevhodné zařazení bezpečnostních rolí do organizační struktury, nedostatečné rozhodovací pravomoce a kompetence bezpečnostních rolí.
- Osoby zastávající jednotlivé bezpečnostní role nemají dostatečné kompetence.
- Manažer KB bez dostatečné znalosti prostředí organizace.

Aplikační bezpečnost

- Nejsou prováděny bezpečnostní testy zranitelnosti aplikací, které jsou přístupné z vnější sítě (před jejich nasazením a po změnách).

Řízení dodavatelů

Nejčastějšími nedostatky v oblasti řízení dodavatelů jsou:

- smluvní vztahy nerespektující zákonné požadavky vztahující se na poskytovanou službu,
- řízení přístupových oprávnění dodavatelů,
- správa uživatelských účtů dodavatelů služeb s privilegovaným oprávněním.

Audit kybernetické bezpečnosti

- Nejsou prováděny požadované audity kybernetické bezpečnosti.

Ověřování identity uživatelů

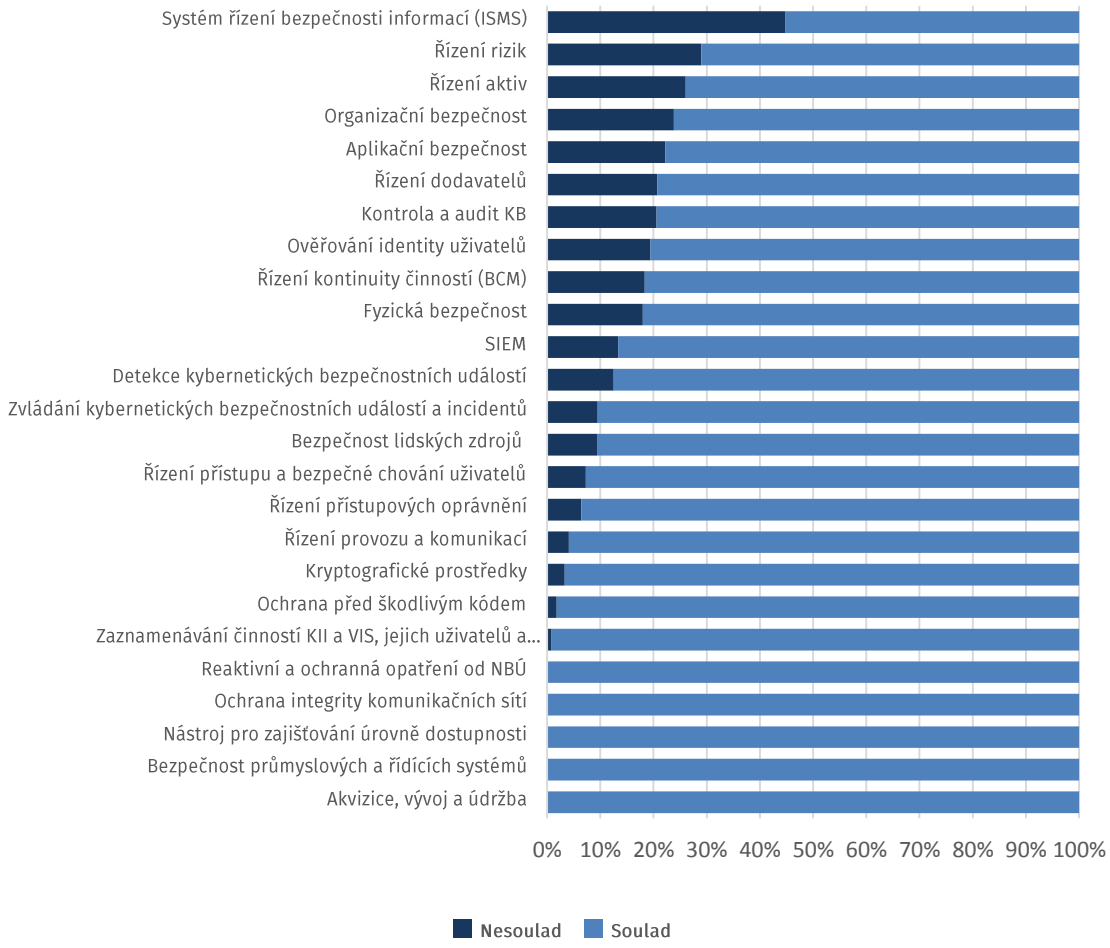
- Nedostatky v procesu správy uživatelských účtů (např. řízení oprávnění v souvislosti s životním cyklem zaměstnanců).
- Řízení identit třetích stran.
- Neplnění požadavků na sílu hesla.

Řízení kontinuity činností

- Neexistující plány řízení kontinuity či jejich neúplnost.
- Chybějící testování havarijních plánů.

Fyzická bezpečnost

- Nedostatečná opatření k zamezení neoprávněnému vstupu do vymezených prostor nebo k zamezení poškození technologií ve vymezených prostorách.



Graf 10: Nesoulad v jednotlivých oblastech

Příloha č. 2: Seznam použitých zkratek a pojmů

APT – Advanced persistent threat

CBMs – Confidence Building Measures (opatření pro zvyšování důvěry mezi státy)

CCDCoE – Cooperative Cyber Defence Centre of Excellence

CECSP – Central European Cyber Security Platform (Středoevropská platforma pro kybernetickou bezpečnost)

CERT – Computer Emergency Response Team

CESNET – sdružení založené roku 1996 českými veřejnými vysokými školami a Akademií věd ČR

CIRC MO – Computer Incident Response Capability, středisko kybernetické ochrany resortu Ministerstva obrany

CSIRT – Computer Security Incident Response Team

CSIRT-MU – bezpečnostní tým pro dohled nad sítí Masarykovy university v Brně

CZ.NIC – zájmové sdružení právnických osob založené v roce 1998 předními poskytovateli internetových služeb, jeho hlavní činností je provozování registru domén

DEFACEMENT – průnik do webového serveru protivníka a nahrazení jeho internetových stránek obsahem, který vytvořil útočník; 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

DoS/DDoS – Odmítnutí služby (Denial of Service) a distribuované odmítnutí služby (Distributed Denial of Service).

EDA – European Defence Agency (Evropská obranná agentura)

ENISA – European Union Agency for Network and Information Security (Evropská agentura pro bezpečnost sítí a informací)

EU – Evropská unie

FIRST – Forum for Incident Response and Security Teams

FSS MU – Fakulta sociálních studií Masarykovy univerzity v Brně

GFCE – Global Forum on Cyber Expertise

GovCERT.CZ – vládní CERT sloužící jako koordinační místo pro okamžitou reakci na kybernetické bezpečnostní incidenty; je organizační složkou Národního bezpečnostního úřadu, respektive specializované pracoviště Národního centra kybernetické bezpečnosti

Honeypot – návnada lákající útočníka. Po zachycení potencionálně nebezpečného software dochází k jeho automatizované analýze

ICS – Industrial Control System je systém pro řízení technologických celků; příkladem může být SCADA

IROP – Integrovaný regionální operační program (10. výzva)

KII – kritická informační infrastruktura

KYBERKRIMINALITA – specifický druh kriminality páchaný prostřednictvím výpočetních a komunikačních technologií

MALWARE – počítačový program určený k proniknutí nebo poškození počítačového systému

MF – Ministerstvo financí

MO – Ministerstvo obrany

MPO – Ministerstvo průmyslu a obchodu

MSp – Ministerstvo spravedlnosti

MŠMT – Ministerstvo školství, mládeže a tělovýchovy

MV – Ministerstvo vnitra

MZV – Ministerstvo zahraničních věcí

NATO – North Atlantic Treaty Organization (NATO)

NBÚ – Národní bezpečnostní úřad

NIS – Directive on security of network and information systems

NCKB – Národní centrum kybernetické bezpečnosti

NSKB – Národní strategie kybernetické bezpečnosti

OECD – Organisation for Economic Co-operation and Development (Organizace pro hospodářskou spolupráci a rozvoj)

OBSE – Organizace pro bezpečnost a spolupráci v Evropě

OKBP – Odbor kybernetických bezpečnostních politik

OTPVV – Oddělení teoretické podpory, vzdělání a výzkumu

PČR – Policie České republiky

PHISHING – podvodná metoda usilující o odcizení citlivých údajů uživatele za účelem jejich zneužití, většinou vytvořením podvodné zprávy, šířené většinou elektronickou poštou, jež se snaží citlivé informace uživatelů vylákat; zprávy mohou být maskovány tak, aby co nejvíce imitovaly důvěryhodného odesílatele

SABU – Sdílení a analýza bezpečnostních událostí SCADA systém (Supervisory Control and Data Acquisition) – 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. výrobě elektrické energie), infrastrukturní (např. rozvod pitné vody) nebo zařízení (např. železniční stanice)

TABLE-TOP – cvičení navrženo k testování teoretických schopností cvičících ve skupině reagovat na krizovou situaci; výhodu tohoto druhu cvičení představuje možnost vyzkoušet si jakoukoliv hypotetickou situaci bez rizika způsobení škody a dalších důsledků

VIS – Významný informační systém

ZKB – zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů

Příloha č. 3: Hlášení o stavu naplňování Akčního plánu k Národní strategii kybernetické bezpečnosti České republiky na období let 2015 až 2020[16]

Umístěno jako příloha v samostatném dokumentu

[16] Toto hlášení reflektuje stav naplňování úkolů Akčního plánu k Národní strategii kybernetické bezpečnosti České republiky na období let 2015 až 2020 s termínem do čtvrtého kvartálu 2016 a úkolů, které mají být plněny průběžně.