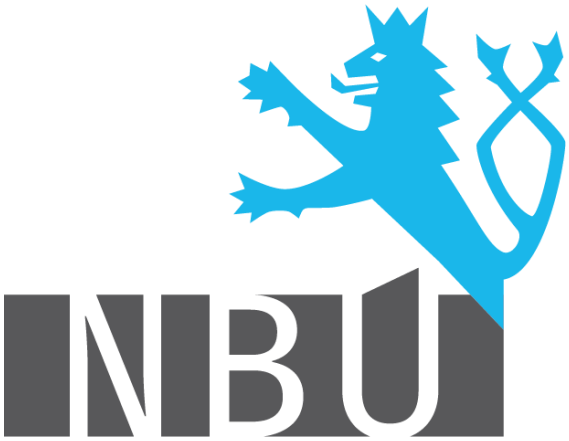
NÁRODNÍ BEZPEČNOSTNÍ ÚŘAD

Národní centrum kybernetické bezpečnosti



ZPRÁVA O STAVU

KYBERNETICKÉ BEZPEČNOSTI

ČESKÉ REPUBLIKY ZA ROK 2015

OBSAH

ÚVOD 4

1. ROZVOJ NCKB 5
2. KRITICKÁ INFORMAČNÍ INFRASTRUKTURA A VÝZNAMNÉ INFORMAČNÍ SYSTÉMY 7
   - 2.1. Technická bezpečnost systémů KII/VIS 7
   - 2.2. Určování prvků KII a posuzování VIS 11
   - 2.3. Přípravy ke kontrole podle zákona o kybernetické bezpečnosti 12
3. VÝVOJ LEGISLATIVY A KONCEPČNÍCH DOKUMENTŮ 13
   - 3.1. Národní strategie kybernetické bezpečnosti a Akční plán 13
   - 3.2. Legislativní vývoj 14
4. MEZINÁRODNÍ SPOLUPRÁCE 16
   - 4.1. Evropská unie 16
   - 4.2. Evropská agentura pro bezpečnost sítí a informací (ENISA) 17
   - 4.3. Severoatlantická aliance (NATO) 17
   - 4.4. Organizace pro bezpečnost a spolupráci v Evropě (OBSE) 18
   - 4.5. Central European Cyber Security Platform (CECSP) 19
   - 4.6. Bilaterální a další spolupráce 19
   - 4.7. GÉANT / Trusted Introducer 21
   - 4.8. Účast na mezinárodních kybernetických cvičeních 21
     - 4.8.1. Crisis Management Exercise 21
     - 4.8.2. Locked Shields 22
     - 4.8.3. Cyber Coalition 22
     - 4.8.4. CECSP 2015 Exercise 23
     - 4.8.5. Cvičení pro US Cyber Command 23
   - 4.9. Projekt Honeynet 24
5. NÁRODNÍ SPOLUPRÁCE 25
   - 5.1. Bezpečnostní tým CSIRT.CZ 25
   - 5.2. Další bezpečnostní týmy CSIRT 26
   - 5.3. Policie České republiky a zpravodajské služby 27
   - 5.4. Ministerstvo obrany 28
   - 5.5. Akademická sféra 28

5.6. Další partneři 30
5.7. Národní cvičení CYBER CZECH 2015 30
5.7.1. Teoretické cvičení 30
5.7.2. Technické cvičení 30
6. ZVYŠOVÁNÍ POVĚDOMÍ A OSVĚTA 32
PŘÍLOHY 35
Příloha č. 1 – Přehled nejvýznamnějších incidentů 35
Příloha č. 2 – Statistiky 38
Příloha č. 3 – Seznam použitých zkratek a pojmů 40
Příloha č. 4 – hlášení o stavu naplňování Akčního plánu k Národní strategii kybernetické bezpečnosti České republiky na období let 2015 až 2020 42

ÚVOD

Rok 2015 znamenal další rozvíjení a prohlubování schopností České republiky v oblasti kybernetické bezpečnosti. S Novým rokem vstoupil v účinnost zákon o kybernetické bezpečnosti a prováděcí předpisy, které rámují činnost Národního bezpečnostního úřadu jako gestora kybernetické bezpečnosti a mimo jiné stanovují bezpečnostní standardy pro důležité sítě a informační systémy s celostátním významem.

V únoru 2015 byla schválena Národní strategie kybernetické bezpečnosti na období let 2015 až 2020, o tři měsíce později na ni navázal Akční plán, který jednotlivým dotčeným subjektům ukládá konkrétní úkoly a termíny jejich plnění.

Po celý rok se Národní bezpečnostní úřad intenzivně věnoval procesu určování prvků kritické informační infrastruktury a významných informačních systémů. Technickou podporu při zajišťování kybernetické bezpečnosti těchto systémů úřad poskytuje prostřednictvím vládního bezpečnostního týmu GovCERT.CZ, jehož cílem je čelit bezpečnostním výzvám, reagovat na incidenty, koordinovat kroky k jejich řešení a účinně jim předcházet. Zaměstnanci úřadu také na řadě jednání a konferencí vysvětlovali práva a povinnosti vyplývající ze zákona o kybernetické bezpečnosti, metodiku určování subjektů, na které se zákon vztahuje, a v neposlední řadě termíny, ve kterých budou zákonem stanovené povinnosti muset být plněny.

Rozvíjely se i další bezpečnostní týmy činné v České republice, v prvé řadě CSIRT.CZ plnící mimo jiné funkci národního CERT týmu, která byla potvrzena podepsáním veřejnoprávní smlouvy s Národním bezpečnostním úřadem v prosinci 2015.

Rok 2015 v oblasti kybernetické bezpečnosti znamenal i rozvoj intenzivní mezinárodní spolupráce na bilaterální i mnohostranné úrovni. Česká republika postupně získává reputaci kvalitního a důvěryhodného partnera nejen při výměně informací, ale i v rámci cvičení kybernetické bezpečnosti. Jako první z členských států NATO podepsala v říjnu novou generaci memoranda o porozumění v oblasti kybernetické bezpečnosti (*cyber defence*). Aktivně jsme se podíleli na přípravě evropské směrnice o bezpečnosti sítí a informačních systémů, kterou po více než dvou letech jednání dovedlo do konce lucemburské předsednictví. Pokračovala spolupráce v rámci Středoevropské platformy pro kybernetickou bezpečnost, jejíž je Česká republika zakládajícím členem. Strategická partnerství byla navázána s Izraelem a Jižní Koreou.

1. ROZVOJ NCKB

Národní bezpečnostní úřad (NBÚ) v roce 2015 pokračoval v budování kapacit Národního centra kybernetické bezpečnosti (NCKB), slavnostně otevřeného v květnu 2014, a v technické i teoretické podpoře svých partnerů.

NCKB se skládá ze dvou oddělení. Prvním je vládní bezpečnostní tým GovCERT.CZ, jehož IT odborníci poskytují pomoc s technickým řešením kybernetických bezpečnostních incidentů, provádí penetrační analýzu, analýzu malware a zajišťují sdílení informací o incidentech a budoucích trendech v této oblasti s IT komunitou i veřejností. Druhým je Oddělení teoretické podpory, výzkumu a vývoje, které 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 předpisů, mezinárodní spolupráci, osvětu a vzdělávání nebo publikační činnost.

S postupně vzrůstající potřebou reakce na kybernetické hrozby v oblasti průmyslových řídicích systémů započal GovCERT.CZ v roce 2015 s budováním takzvané ICS-SCADA laboratoře umožňující hlubší zkoumání této problematiky. Spoluprací s průmyslovými partnery a subjekty spravujícími KII a VIS jsou získávány cenné technické a provozní informace o používaných řídicích systémech a způsobu jejich integrace na síť. Na to navazuje monitorování technologií nejčastěji používaných v České republice a s ním související analýza nových trendů v oblasti kybernetické bezpečnosti těchto systémů. GovCERT.CZ tak bude schopen v případě řešení krizové situace nabídnout konzultace a asistenci i v mezinárodním kontextu. Získané poznatky jsou dále využívány při mezinárodních bezpečnostních cvičeních, která se již začínají i na tuto problematiku zaměřovat.

V roce 2015 rovněž pokračovalo budování laboratoře pro forenzní analýzu kybernetických bezpečnostních incidentů, která s jejich rostoucím počtem nabývá na aktuálnosti. Správa laboratorního prostředí je kontinuální proces zahrnující průběžné vylepšování a přizpůsobování aktuálním potřebám a trendům. Laboratoř bude využívána během cvičení kybernetické bezpečnosti a při spolupráci s národními i mezinárodními partnery, kterou GovCERT.CZ postupně rozvíjí, například s Policií ČR nebo Evropským centrem pro počítačovou kriminalitu EC3 spravovaným Europolem.

Z povahy pracoviště CERT a jeho úkolů vyplývá nezbytnost vysoké odbornosti jeho zaměstnanců a její neustálé prohlubování, aby mohli být rovnocennými partnery svým zahraničním kolegům při spolupráci a řešení stále nových kybernetických hrozeb a útoků. Součástí je vzdělávání formou specializovaných školení, stáží a kurzů. NBÚ na základě veřejné zakázky proto v květnu 2015 uzavřel smlouvu se společností SANS, jedním ze světově nejuznávanějších poskytovatelů technické expertízy v oblasti kybernetické bezpečnosti. V letech 2015-2017 členové vládního CERT podle svého zaměření získají certifikaci v incident handlingu, forenzní analýze a vyšetřování, reverzním inženýrství a analýze malware, Windows security, UNIX security, virtualizaci a cloudové bezpečnosti, penetračním testování nebo ICS/SCADA bezpečnosti. Do konce roku 2015 školení SANS absolvovalo 11 zaměstnanců. Jeden zaměstnanec stihl zakončit školení certifikátem ještě v roce 2015. Další certifikace jsou naplánovány na první čtvrtletí roku 2016, plán školení na 2016 se připravuje.

Své rostoucí technické schopnosti GovCERT.CZ hodlá v roce 2016 stvrdit certifikací v organizaci FIRST, která pracoviště ukotví na mezinárodní scéně, přispěje k vyšší důvěře zahraničních partnerů a umožní přístup k citlivým informacím využitelným při plnění úkolů GovCERT.CZ. Organizace FIRST zejména zprostředkovává kontakt na bezpečnostní týmy z celého světa, podporuje aktivity v oblasti odhalování a vyřazování botnetů, hledání a klasifikace zranitelností či, analýzy malware.

Mezi největší úspěchy OTPVV patřilo v roce 2015 schválení Národní strategie kybernetické bezpečnosti na období let 2015-2020 a Akčního plánu k této strategii, který byl připravován v intenzivní spolupráci se zástupci ministerstev a dalších státních institucí. Členové OTPVV se rovněž intenzivně věnovali určování prvků KII a VIS[1].

Nový právní rámec a koncepční dokumenty, jakož i ad hoc zadání znamenají narůstající agendu pro NCKB. V roce 2015 proto NBÚ pokračoval v rozšiřování personálních i technických kapacit NCKB. Ke konci roku 2015 naplnilo NCKB počet přidělených pracovních míst, zejména, specialisty na informační technologie, krizové řízení, mezinárodní vztahy, právo a bezpečnost. Usnesením č. 520 ze dne 1. července 2015 vláda rozhodla o personálním a finančním posílení NBÚ v průběhu let 2016-2018, které reflektuje potřeby vyplývající ze ZKB a koncepčních dokumentů, jakož i rostoucí objem a požadavky na kvalitu práce při řešení kybernetických bezpečnostních incidentů.

[1] Viz kapitola 3.1

2. KRITICKÁ INFORMAČNÍ INFRASTRUKTURA A VÝZNAMNÉ INFORMAČNÍ SYSTÉMY

Po vstupu ZKB v účinnost NBÚ zahájil proces určování prvků KII. Správci KII a správci VIS od roku 2015 začínají plnit povinnosti podle zákona, technickou podporu jim přitom poskytují odborníci GovCERT.CZ. Ke dni 31. prosince 2015 bylo opatřením obecné povahy nebo usnesením vlády určeno 76 prvků KII. Průběžně byly jednotlivými správci, kteří jsou organem veřejné moci, nahlašovány systémy, které naplňují kritéria pro VIS. Dále byl připraven systém kontroly podle ZKB a zkušenosti získané v prvním roce pomohly k identifikaci možných budoucích legislativních změn.

2.1. Technická bezpečnost systémů KII/VIS

Technickou podporu při zajišťování kybernetické bezpečnosti u systémů KII a VIS zajišťuje GovCERT.CZ, který disponuje odborníky na klíčové oblasti kybernetické bezpečnosti. Cílem je účinně čelit bezpečnostním výzvám, reagovat na incidenty, koordinovat kroky k jejich řešení a účinně jim předcházet.

Z tohoto důvodu GovCERT.CZ vypracoval metodiku pro zvládání kybernetických bezpečnostních incidentů, kde je definován

- pracovní postup,
- jakým způsobem a jakou formou je možné incidenty hlásit,
- co má hlášení obsahovat,
- jak je dále s hlášením nakládáno.

Kybernetický bezpečnostní incident je možné hlásit e-mailem, telefonicky, skrze PDF formulář a nově i automatizovaně pomocí XML dokumentu. Při řešení citlivých informací lze použít šifrování PGP, kdy veřejný klíč pro e-mailovou adresu určenou pro hlášení incidentů je dostupný na stránkách www.govcert.cz. Prověření komunikující osoby lze provést skrze sítě důvěryhodných spolupracujících CERT/CSIRT týmů (například Trusted Introducer, FIRST), zpětným voláním, zpětnou e-mailovou zprávou nebo v případě potřeby osobním kontaktem.

Po přijetí hlášení je důležité posoudit, zda je incident věrohodný, určit jeho rozsah a stanovit priority. GovCERT.CZ k prošetření incidentu kontaktuje zúčastněné strany, usnadňuje kontakt s dalšími subjekty a v případě potřeby informuje ostatní CERT/CSIRT týmy. GovCERT.CZ také shromažďuje statistické údaje o událostech a incidentech v rámci v rámci jeho působnosti. Přehled nejvýznamnějších incidentů za rok 2015 je uveden v příloze č. 1, počty přijatých hlášení, řešených incidentů a jejich klasifikací pak v příloze č. 2.

Jedním z projektů GovCERT.CZ, ceněných pro svůj přínos jejich adresáty, byla v roce 2015 preventivní analýza veřejně dostupných informací ze serverů státních institucí spadajících do kompetence GovCERT.CZ, které by mohly sloužit a v reálných případech být použity pro přípravu sofistikovaného cíleného kybernetického útoku na dané subjekty. Data byla shromažďována na základě na míru vytvořené metodologie prostřednictvím vybraných open-source nástrojů a specializovaného software pro získávání metadat z dokumentů a jednotlivých webů. Výstupem analýzy byly poskytnuté zprávy, kde se objevily informace o jménech jednotlivých zaměstnanců, e-mailových adresách, používaných operačních systémech nebo o používaných softwarových nástrojích. Na základě následné důkladné analýzy rizik byl vypracován soubor doporučení pro správce dotyčných systémů k zajištění bezpečnějšího zacházení se zveřejňovanými informacemi. Projekt bude v následujícím roce pokračovat i pro další orgány státní správy v působnosti GovCERT.CZ.

GovCERT.CZ dále začal s realizací dvou projektů týkajících se externího penetračního testování a skenování zranitelností podle OWASP. V rámci prvního projektu bude NBÚ externím subjektům nabízet penetrační testování jejich systémů z pohledu potenciálního útočníka. V roce 2015 probíhala příprava pilotního testování na vybrané státní instituci včetně formulace rozsahu činností a zodpovědnosti zúčastněných stran, které budou upraveny smluvně. Druhý projekt, zaměřený na testování webových aplikací s využitím testovací struktury Open Web Application Security Project (OWASP), umožní GovCERT.CZ otestovat vyšší počet subjektů a tím zvýšit úroveň kybernetické bezpečnosti napříč státní správou. V roce 2015 proběhly pilotní testy v rámci NBÚ.

O rostoucím významu kybernetické bezpečnosti svědčí i skutečnost, že v rámci Integrovaného regionálního operačního programu byla v říjnu 2015 vypsána výzva č. 10 Kybernetická bezpečnost, kde je alokováno 1 411 764 706 Kč. Tato výzva se týká zvýšení odolnosti KII veřejné správy a VIS vůči kybernetickým hrozbám. V rámci této výzvy GovCERT.CZ spustil projekt k zajištění monitorování provozu systémů KII a VIS. Cílem je zprostředkovat rezortům monitoring a detekci událostí v síťovém provozu, díky kterým, současně s detekcí bezpečnostních událostí, získají přehled o provozu ve vlastních sítích. Přidanou hodnotou je globální přehled GovCERT.CZ nad detekovanými událostmi napříč rezorty, který umožní předcházet některým cíleným útokům. Získané informace budou následně předávány rezortům zpět ve formě varování před nebezpečnými IP adresami, doménami nebo útoky na jejich sítě. Pilotního projektu se zúčastnil jeden z klíčových rezortů státní správy, kterému NBÚ zapůjčil síťovou sondu, která je plně spravována jejich administrátory. Na oplátku bude rezort sdílet s GovCERT.CZ

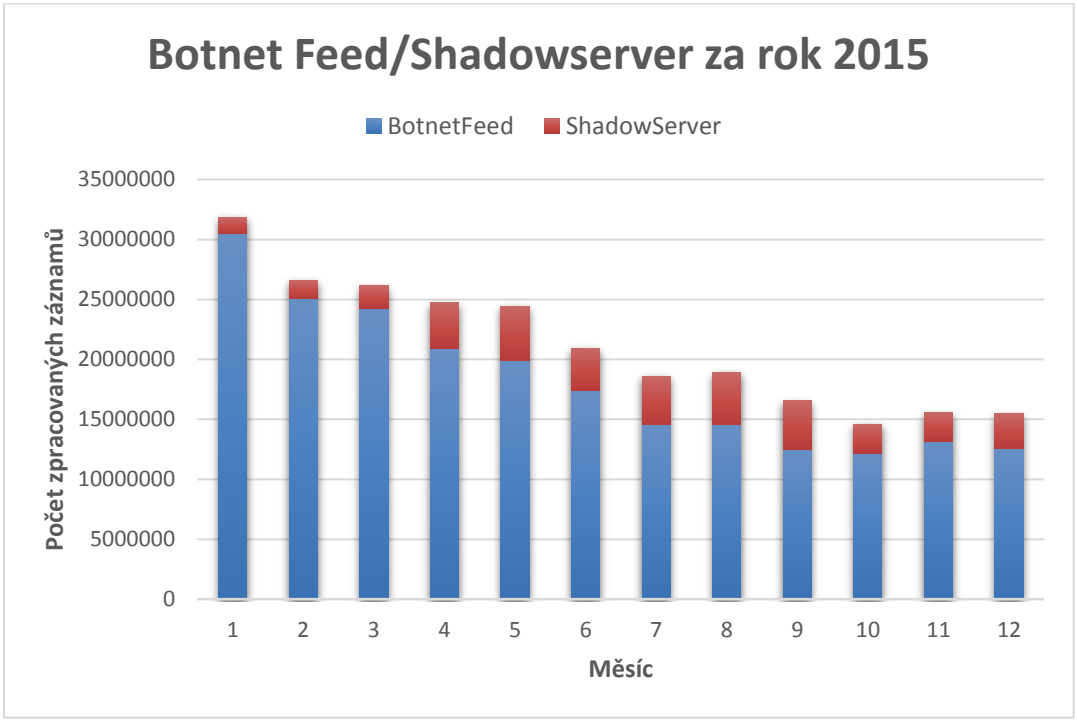
informace o některých událostech, které sonda nahlásí jako podezřelé. Na pilotním rezortu proběhlo seznámení a zaškolení příslušných pracovníků a v současnosti by již měla být sonda odladěna a schopna zobrazovat relevantní data. Od října 2015 NBÚ jednal s dalšími rezorty a začalo mapování jejich sítí s cílem určit co nejpřínosnější nasazení sond v rezortních sítích.

V rámci svých proaktivních činností GovCERT.CZ rovněž pomocí několika nástrojů analyzuje data z uzavřených a veřejně dostupných zdrojů, jež obsahují indikátory o kompromitaci systémů. Prvním nástrojem je Incident Handling Automation Project (IHAP) shromažďující informace o phishingových útocích, útocích hrubou silou, průnicích do sítí, spamu, exploit kitech a o skenování zranitelností.[2] Druhým 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 z převzatých řídících serverů (C&C). Zdrojem dat je společnost Microsoft.[3] V roce 2015 se podařilo rozšířit množinu odběratelů dat z projektu o další čtyři bezpečnostní CERT/CSIRT týmy z komerční sféry a o subjekty KII a VIS. Převážná část reportů je určena komerční sféře (ISP/poskytovatelé hostingových služeb). Denně je exportováno přibližně 10 MB reportů ve strojově čitelném formátu. Z pohledu státní správy, KII a VIS se jedná o cca 248 reportů od začátku roku. Třetím nástrojem je Shadowserver poskytující informace o malware, botnet sítích a dalších elektronických podvodných aktivitách. Zdrojem dat je dobrovolnická mezinárodní skupina profesionálních bezpečnostních pracovníků Shadowserver Foundation. GovCERT.CZ je do projektu zapojen od konce roku 2014, v současnosti odebírá a zpracovává informace o zhruba 30 druzích hrozeb. Tato data jsou následně automaticky analyzována a jsou identifikovány hrozby spadající do působnosti GovCERT.CZ. Od začátku roku 2015 do listopadu 2015 bylo zpracováno a vyhodnoceno přibližně 29,3 milionů záznamů o bezpečnostních hrozbách v České republice.

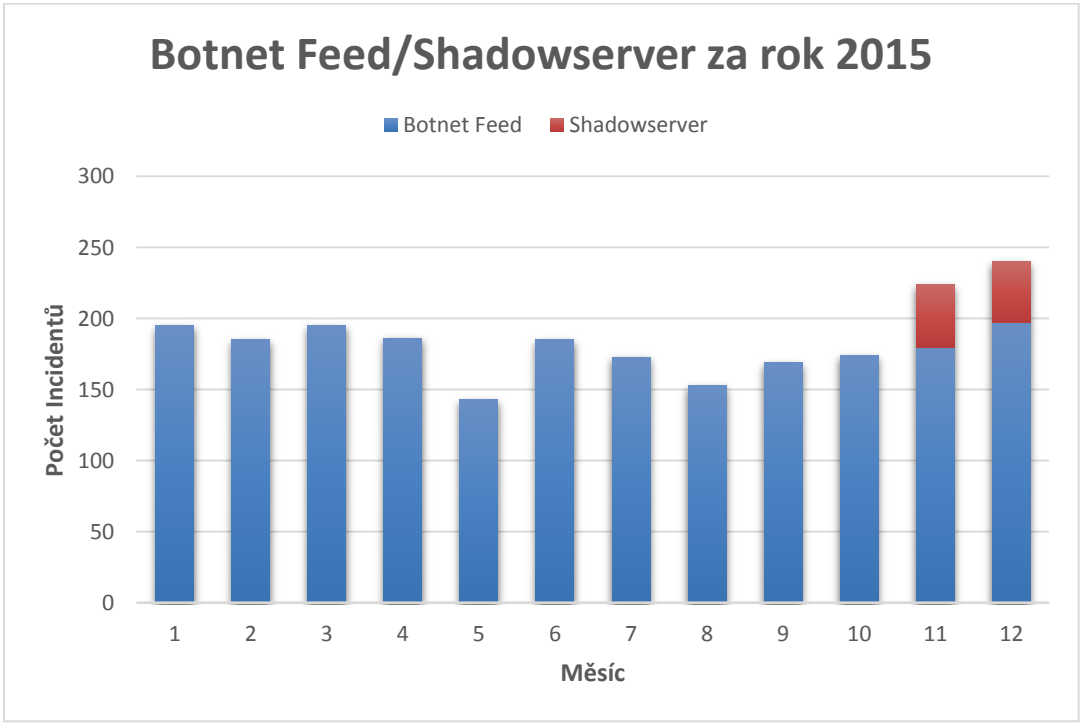
V následujících grafech je uveden počet zpracovaných záznamů za rok 2015 v rámci proaktivních projektů Botnet Feed a Shadowserver a počet kybernetických incidentů řešených pracovníky GovCERT.CZ spadajících do jeho působnosti.

[2] Pro Českou republiku se měsíčně jedná o stovky tisíc indikátorů kompromitace, ale jen malá část z nich spadá do působnosti GovCERT.CZ.

[3] GovCERT.CZ doposud odebírá data týkající se přibližně 14 botnetů, mezi kterými jsou např. Bamital, Citadel, Conficker, Kelihos, Zeus a další. V průběhu letošního roku byla přidána data o botnetech Simda, Ramnit a Dorkbot.



Graf 01 – počet zpracovaných záznamů za rok 2015



Graf 02 – počet incidentů za rok 2015 s rozdělením po měsících

2.2. Určování prvků KII a posuzování VIS

Proces určování KII probíhá prozatím ve třech vlnách. V první vlně se NBÚ zaměřil na informační nebo komunikační systémy ve správě organizačních složek státu - ústředních orgánů státní správy. Určování v této vlně bylo spuštěno neprodleně po vstupu ZKB v účinnost a bylo završeno dne 15. února 2015, kdy NBÚ k zařazení do KII navrhl 45 informačních a komunikačních systémů. Usnesením vlády č. 390 ze dne 25. května 2015 byl tento seznam schválen.

V druhé vlně se NBÚ zaměřil na zbývající organizační složky státu a dne 15. září 2015 předložil podle krizového zákona Ministerstvu vnitra další seznam prvků KII navržených k určení. Usnesením vlády č. 981 ze dne 2. prosince 2015 byl seznam schválen. Tato skupina nicméně může být ještě rozšířena, nepředpokládá se však takové množství prvků KII jako ve vlně první.

Ve třetí vlně jsou identifikovány prvky KII, jejichž správcem nejsou organizační složky státu. Jedná se o strategické informační a komunikační systémy jak ve správě soukromých společností, tak ve správě státních podniků a obdobných subjektů. Tato fáze není doposud ukončena. Zatímco určení KII u organizačních složek státu je prováděno usnesením vlády ČR na návrh NBÚ, u ostatních subjektů se tak stane opatřením obecné povahy vydaným NBÚ. Ke dni 31. prosince 2015 bylo opatřením obecné povahy určeno 28 prvků KII.

Počty určených prvků KII shrnuje následující tabulka:

Tabulka 1: Počty prvků KII a správců v soukromé/veřejné sféře

Správce	Počet prvků	Počet správců
Organizační složky státu (1. a 2. vlna)	48	14
Ostatní	28	15
Celkem	76	29

Pozn.: Údaje uvedené v tabulce reflektují situaci ke dni 31. prosince 2015

Proces určování KII je vzhledem k dynamickému prostředí informačních a komunikačních technologií průběžnou činností. NBÚ nepředpokládá výrazný nárůst počtu prvků KII u organizačních složek státu. Naproti tomu u ostatních subjektů je nárůst očekáván a dle odhadů budou mít tyto subjekty ve správě více než polovinu všech určených prvků KII.

Na rozdíl od kritické informační infrastruktury je za posouzení naplnění kritérií pro významné informační systémy odpovědný sám správce systému. Seznam těchto systémů je uveden v příloze vyhlášky č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích, která ke dni 31. prosince 2015 obsahovala 92 VIS spravovaných celkem 35 subjekty. Podobně jako proces určování KII je však i posuzování VIS kontinuální činností a stav se proto již v průběhu roku 2015 měnil; některé systémy byly přeřazeny do KII a mnoho jiných systémů bylo jednotlivými správci nově posouzeno a nahlášeno. Ke dni 31. prosince 2015 NBÚ evidoval cca 105 VIS a začal připravovat aktualizaci předmětné přílohy.

2.3. Přípravy ke kontrole podle zákona o kybernetické bezpečnosti

Zákon o kybernetické bezpečnosti ukládá správcům KII a správcům VIS množství povinností. Kromě obecných povinností, jako jsou například hlášení kontaktních údajů a hlášení kybernetických bezpečnostních incidentů NBÚ, jde o povinnosti spojené se zavedením řady organizačních a technických bezpečnostních opatření podle vyhlášky č. 316/2014 Sb. Správci KII a VIS mají pro naplnění většiny povinností roční přechodnou lhůtu. U KII se tato lhůta počítá od okamžiku určení, u VIS od posouzení.

V průběhu roku 2015 probíhaly přípravy na kontrolu dodržování zákonných povinností, kterou bude od r. 2016 NBÚ provádět. Jeho kompetence v tomto směru jsou upraveny zákonem č. 255/2012 Sb., o kontrole, a vnitřními předpisy NBÚ.

Podle předběžných informací lze obecně říci, že jednotliví správci KII a VIS k plnění povinností vyplývajících ze zákona o kybernetické bezpečnosti přistupují s odpovědností. Existují však rozdíly mezi úrovní zabezpečení informačních a komunikačních systémů u jednotlivých správců. Nejvýraznější odlišnosti byly evidovány mezi správci v soukromé a veřejné sféře, kdy ve veřejné sféře bývá kybernetická bezpečnost a informační bezpečnost podceňována nebo strádá, kromě nedostatku expertů, také nedostatkem financí či administrativními a regulatorními bariérami, byť toto hodnocení samozřejmě nelze na veřejnou sféru uplatnit paušálně.

3. VÝVOJ LEGISLATIVY A KONCEPČNÍCH DOKUMENTŮ

Rok 2015 zaznamenal několik milníků v oblasti právně-strategické úpravy kybernetické bezpečnosti v České republice. S novým rokem vešel v účinnost zákon č. 181/2014 Sb., o kybernetické bezpečnosti, společně s prováděcími předpisy, o měsíc později vláda přijala Národní strategii kybernetické bezpečnosti na období let 2015 až 2020, na kterou v květnu navázal Akční plán.

3.1. Národní strategie kybernetické bezpečnosti a Akční plán

Nová Národní strategie kybernetické bezpečnosti na období let 2015-2020, schválená vládou dne 16. února 2015, navázala na předchozí strategii pro období 2012 až 2015, jejíž hlavní úkoly byly úspěšně splněny či průběžně realizovány. Od budování základních kapacit se tím Česká republika posouvá k pokročilejšímu a hlubšímu zajišťování kybernetické bezpečnosti.

Strategie představuje ucelený soubor opatření, který definuje vizi České republiky v oblasti kybernetické bezpečnosti a pojmenovává sledovaný cílový stav. Formuluje rovněž základní principy, které bude ČR při zajišťování kybernetické bezpečnosti následovat a dodržovat. Dále definuje konkrétní výzvy a problémy na poli kybernetické bezpečnosti jak v domácím, tak mezinárodním prostředí. Stěžejní část Strategie tvoří hlavní cíle v osmi definovaných prioritních oblastech:

I. Zajištění efektivity a posilování všech struktur, procesů a spolupráce při zajišťování kybernetické bezpečnosti,
II. Aktivní mezinárodní spolupráce,
III. Ochrana národní KII a VIS,
IV. Spolupráce se soukromým sektorem,
V. Výzkum a vývoj / Spotřebitelská důvěra,
VI. Podpora vzdělávání, osvěta a rozvoj informační společnosti,
VII. Podpora rozvoje schopností Policie České republiky vyšetřovat a postihovat informační kriminalitu,
VIII. Právní úprava pro kybernetickou bezpečnost (vytváření právního rámce). Účast na tvorbě a implementaci evropských a mezinárodních pravidel.

Na únorové přijetí Strategie navázal Akční plán, který vláda přijala dne 25. května 2015. Akční plán vychází z hlavních cílů Strategie a na příštích pět let definuje konkrétní úkoly k jejímu naplnění. U každého ze 141 úkolů je uveden jeden či více subjektů, které za splnění odpovídají, a termín, do kdy se tak má stát. V září 2015 se uskutečnilo první setkání zástupců jednotlivých subjektů odpovědných za plnění úkolů Akčního plánu, na které budou navazovat další setkání minimálně dvakrát ročně, ve formátu pracovní skupiny pro harmonizaci národních pozic zřízené v listopadu usnesením Rady pro kybernetickou bezpečnost, poradního orgánu předsedy vlády. Hlavní cílem je především diskutovat o jednotlivých bodech Akčního plánu, u kterých se blíží termín plnění či se plní průběžně, s cílem identifikovat výzvy a řešit problematické oblasti.

Na implementaci Akčního plánu a Strategie kromě NBÚ pracují zejména rezorty vnitra, obrany, zahraničních věcí, průmyslu a obchodu a financí. Nezastupitelnou úlohu hrají zpravodajské služby, na osvětové činnosti budou důležitý podíl mít Ministerstvo školství, mládeže a tělovýchovy a Ministerstvo práce a sociálních věcí. Ve vybraných úkolech se dále zapojí Technologická agentura České republiky nebo Český telekomunikační úřad.

Informace o plnění Akčního plánu, respektive Strategie, zpracovaná na základě vstupů jednotlivých subjektů, tvoří v souladu s příslušným usnesením vlády přílohu této Zprávy[4].

3.2. Legislativní vývoj

Nový právní rámec kybernetické bezpečnosti v České republice tvoří zejména zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů, vyhláška č. 316/2014 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti, vyhláška č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích, a nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury ve znění nařízení vlády č. 315/2014 Sb.

S účinností ZKB a prováděcích předpisů zahájil NBÚ proces určování prvků kritické informační infrastruktury, jejichž správcům, stejně jako správcům významných informačních systémů vznikly zákonné povinnosti ve vztahu k bezpečnostním opatřením a specifické povinnosti vůči NBÚ a GovCERT.CZ.

[4] Viz příloha č. 4

Prvky KII určuje NBÚ podle kritérií stanovených nařízením vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury. Proces určování je pak upraven zákonem č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon), přičemž k posouzení, zda daný systém kritéria naplňuje či nikoli, dochází na základě oboustranných jednání s jejich správci.[5] Do KII obecně patří takové informační a komunikační systémy, jejichž narušení by mohlo mít závažný dopad na bezpečnost státu, zabezpečení základních životních potřeb obyvatelstva, zdraví osob nebo ekonomiku státu. Jsou to zejména ty systémy, na kterých jsou zcela nebo významně závislé další prvky kritické infrastruktury (například elektrárny, přenosové soustavy, některé banky apod.).

Druhou skupinou povinných subjektů jsou správci VIS. Správcem VIS může být pouze orgán veřejné moci, v současnosti však významným informačním systémem není informační systém ve správě obce.[6] Významné informační systémy musí naplnit kritéria stanovená vyhláškou č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích. Obecně lze říci, že narušení bezpečnosti informací v těchto informačních systémech by mohlo omezit nebo výrazně ohrozit výkon působnosti orgánu veřejné moci. Posouzení naplnění kritérií pro VIS provádí sám správce systému, který v případě jejich naplnění nahlásí kontaktní údaje NBÚ pomocí formuláře z přílohy č. 7 k vyhlášce č. 316/2014 Sb., o kybernetické bezpečnosti.[7]

S přibývajícími zkušenostmi z určování KII/VIS je možné identifikovat případné mezery či nedostatky legislativy, aby časem mohla být právní úprava novelizována. V prosinci 2015 Rada EU schválila návrh směrnice o bezpečnosti sítí a informačních systémů, která se po své transpozici v příštích letech rovněž významně odrazí na úpravě kybernetické bezpečnosti v ČR.

[5] V roce 2015 zástupci NBÚ uskutečnili více než 150 jednání s potenciálními povinnými osobami.
[6] § 3 odst. 2 vyhlášky 317/2014 Sb.
[7] Ačkoli je posouzení, zda určitý systém naplňuje kritéria stanovená pro VIS ponecháno na správci, NBÚ je se subjekty v kontaktu a poskytuje jim při posuzování podporu.

4. MEZINÁRODNÍ SPOLUPRÁCE

Tradičními partnery NBÚ jsou v oblasti mezinárodní spolupráce orgány a agentury Evropské unie, Severoatlantická aliance a další mezinárodní organizace. Rok 2015 nebyl výjimkou, přičemž rozvoj zaznamenala také Středoevropská platforma pro kybernetickou bezpečnost – Central European Cyber Security Platform (CECSP) a oblast bilaterálních vztahů. Na mezinárodním poli v souvisejících oblastech aktivně působí i další instituce, zejména Ministerstvo obrany (MO), Ministerstvo průmyslu a obchodu, Ministerstvo zahraničních věcí či Český telekomunikační úřad. K lepší koordinaci práce a informovanosti jednotlivých rezortů o mezinárodních aktivitách v kybernetické bezpečnosti a souvisejících oblastech v budoucnu přispěje i pracovní skupina pro harmonizaci mezinárodních pozic zřízená v listopadu 2015 v rámci Rady pro kybernetickou bezpečnost, poradního orgánu předsedy vlády.

4.1. Evropská unie

Česká republika v roce 2015 pokračovala v práci na vyjednávání směrnice o bezpečnosti sítí a informačních systémů, představené Evropskou komisí v únoru 2013. Konečný návrh byl na úrovni COREPER členskými státy schválen dne 18. prosince 2015. Po překladu do národních jazyků a konečném schválení Radou EU a Evropským parlamentem, očekávaném na jaře 2016, musí směrnice být ve lhůtě 21 měsíců transponována do vnitrostátního právního řádu.

Česká republika dlouhodobě usilovala o maximální možné zúžení okruhu dotčených subjektů a minimalizaci povinností jim ukládaných. V tomto úsilí byla ve spolupráci s některými členskými státy částečně úspěšná; ačkoli se zařazení poskytovatelů digitálních služeb nepodařilo vyhnout úplně, jejich okruh byl omezen na polovinu z původně navrhovaného počtu kategorií a byla zavedena zásada maximální harmonizace, díky které členské státy nebudou moci těmto operátorům uložit přísnější povinnosti, než předvídá směrnice.

Práce pokračovala i ve skupině Přátel předsednictví pro kybernetické otázky (Friends of Presidency on Cyber Issues), kde jsou diskutována horizontální témata od kybernetické obrany po správu internetu a která sleduje implementaci Strategie kybernetické bezpečnosti Evropské unie, nebo s Evropskou obrannou agenturou, kde se angažuje zejména MO.

4.2. Evropská agentura pro bezpečnost sítí a informací (ENISA)

ENISA i v roce 2015 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. V neposlední řadě ENISA provozuje celosvětovou databázi národních strategií kybernetické bezpečnosti a v roce 2015 publikovala tradičně kvalitní rozbor kybernetických hrozeb za rok 2014 *„ENISA Threat Landscape 2014“*.

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.

Na každoročním jednání představenstva konaném v říjnu 2015 byl schválen pracovní program ENISA pro rok 2016. V nadcházejícím roce tak byly potvrzeny priority ENISA z roku 2015, zejména:

i. pořádání celoevropského cvičení kybernetické bezpečnosti *„Cyber Europe“* a Evropského měsíce kybernetické bezpečnosti,

ii. ochrana kritické informační infrastruktury,

iii. podpora CERT komunity v členských státech EU.

Pro rok 2016 se ENISA zaměří i na nové oblasti, u nichž narůstá kritičnost selhání ICT, jako jsou inteligentní automobily, systémy řízení letišť a nemocnic a obecně bezpečnost internetu věcí.

4.3. Severoatlantická aliance (NATO)

V roce 2015 docházelo k dalšímu prohlubování a upevňování vztahů se Severoatlantickou aliancí. NBÚ se jako gestor aktivně podílel na přípravě nového formátu memoranda o porozumění s NATO o spolupráci v oblasti kybernetické obrany a dne 12. října 2015 se ČR stala prvním členským státem NATO, který toto memorandum podepsal.

Zástupkyně NCKB se zúčastnila zářijové konference NIAS2015 Cyber Security Symposium, kde na pozvání NCI Agency představila priority ČR v rámci kulatého stolu na téma Cyber Security Leadership.

V neposlední řadě NBÚ pokračoval v aktivní účasti na projektu Multinational Cyber Defence Education and Training, jednom ze tří Smart Defence projektů, které Severoatlantická aliance v rámci problematiky kybernetického prostoru zaštiťuje. V projektu ČR dále rozvíjela své dřívější zapojení do pracovní skupiny zabývající se vytvářením společné taxonomie, nově pak usilovala o členství v pracovní skupině, jejímž cílem je vznik magisterského programu zaměřeného na mezinárodní právo v kybernetickém prostoru. Jedná se o jednu ze vzdělávacích iniciativ, jejichž vznik je hlavním cílem celého projektu. Ke spolupráci na vytváření osnov tohoto magisterského programu byla přizvána Masarykova univerzita v Brně, konkrétně Ústav práva a technologií Právnické fakulty. Své zapojení do projektu na přelomu roku zvažovaly i další součásti Masarykovy univerzity, zájem projevily například některé technicky zaměřené vědecké týmy.

Na spolupráci s NATO se v rámci aliančí politiky v oblasti kybernetické obrany podílí i Ministerstvo obrany. NBÚ spolupracuje s MO na přípravě pozic na jednání Cyber Defence Committee a podle potřeby i jiných formátů NATO zabývajících se kybernetickou bezpečností a obranou. Společně se tyto rezorty v roce 2015 opět zúčastnily aliančních cvičení Cyber Coalition a Locked Shields[8]. Požadavky NATO v oblasti kybernetické obrany realizuje MO na základě závazků k plnění cílů výstavby schopností NATO CT 2013/E 5308 N „Information Assurance and Cyber Defence“.

Česká republika se aktivně podílela rovněž na činnosti NATO Cooperative Cyber Defence Centre of Excellence (CCDCoE) v estonském Tallinnu, jehož posláním je výzkumná a vědecká činnost v oblasti kybernetické bezpečnosti a obrany, a zlepšování spolupráce a sdílení informací mezi členskými státy a NATO. V právní a politické divizi CCDCoE i nadále působil pracovník NBÚ vyslaný v lednu 2014 jako tzv. voluntary national contribution, který se autorsky podílel na analytických publikacích CCDCoE, poskytoval odbornou asistenci při cvičeních kybernetické bezpečnosti a podílel se na organizaci tematicky zaměřených seminářů a konferencí pořádaných CCDCoE. NBÚ centru rovněž poskytl součinnost v několika techničtěji zaměřených projektech.

4.4. Organizace pro bezpečnost a spolupráci v Evropě (OBSE)

V roce 2015 pokračovala činnost neformální pracovní skupiny založené Stálou radou OBSE pro vypracování a implementaci opatření pro budování důvěry v kyberprostoru mezi účastnickými státy, tzv. kybernetických CBMs *(„Confidence Building Measures“)*.

[8] Viz kapitola 4.8

V roce 2013 byl přijat první soubor CBMs, navzdory intenzivním jednáním se druhou sadu CBMs v roce 2015 nepodařilo dokončit a schválit.

Kontinuální a pravidelně aktualizované informace ke všem přijatým kybernetickým CBMs, která ČR plně podporuje, jsou s ostatními účastnickými státy sdíleny prostřednictvím systému POLIS OSCE. Zástupce NBÚ na jednáních pracovní skupiny v roce 2015 navíc seznámil účastnické státy s českou Strategií a Akčním plánem, prezentoval stav implementace kybernetických CBMs v ČR a sdílel zkušenosti získané v rámci procesu vytváření a přijímání Strategie v ČR.

4.5. Central European Cyber Security Platform (CECSP)

Platforma CECSP má poměrně krátkou historii – první oficiální setkání proběhlo v květnu 2013 v Praze. Jejími členy jsou Česká republika, Maďarsko, Polsko, Rakousko a Slovensko. Platforma má vhodně doplňovat jiné evropské nebo mezinárodní organizace a jejím hlavním cílem je především sdílení know-how a příkladů dobré praxe mezi sousedními zeměmi, kde panuje vysoká míra důvěry a spolupráce.

Na posledním technickém setkání v prosinci 2015 zástupci GovCERT.CZ představili partnerům některé své projekty, například záměr tvorby koordinačního centra pro české bezpečnostní týmy, webového portálu pro sdílení informací nebo ICS-SCADA laboratoře. Dále sdíleli počty incidentů zpracovaných za měsíc a další české reálie. Informovali také o podobě a průběhu národního cvičení Cyber Czech 2015. Následně GovCERT-Hungary prezentoval zpracování Big Data a uspořádal workshop s forenzní analýzou paměti.

4.6. Bilaterální a další spolupráce

Česká republika také navázala a prohloubila strategická partnerství s Izraelem, Spojenými státy a Korejskou republikou. Mezi další zahraniční partnery s vysokou mírou bilaterální spolupráce patří Estonsko, Itálie, Německo, Lucembursko, Rumunsko a Kanada.

Na základě společné deklarace, podepsané během společného zasedání české a izraelské vlády v Jeruzalémě dne 25. listopadu 2014, navrhnul ředitel partnerského úřadu *Israeli National Cyber Bureau* Dr. Eviatar Matania uspořádat seminář ke kybernetické bezpečnosti pro seniorní představitele státní správy České republiky. Seminář se uskutečnil ve dnech 8. – 10. září 2015 v Tel Avivu za účasti 31 představitelů ministerstev, Parlamentu ČR, zpravodajských služeb, Policie ČR, Armády ČR a Nejvyššího státního zastupitelství na úrovni náměstků ministrů a ředitelů. Delegace byla vedena místopředsedou Poslanecké

sněmovny Janem Bartoškem. Izraelské straně se podařilo shromáždit vynikající přednášející jak z vládní, tak ze soukromé sféry. Seminář zahrnul veškeré aspekty kybernetické bezpečnosti a účastníci získali hodnotné informace, které jim usnadní přijímat rozhodnutí tykající této oblasti. Uvedený seminář posílil dobré vztahy mezi Českou republikou a Státem Izrael.

Na strategickou úroveň se v roce 2015 podařilo posunout i spolupráci s Korejskou republikou. Dne 26. února 2015 předseda vlády Bohuslav Sobotka během své návštěvy podepsal s korejskou prezidentkou Park Geun-hye Společnou deklaraci o strategickém partnerství obsahující i pasáž o spolupráci v oblasti kybernetické bezpečnosti.

Ve vztahu k USA byla posílena spolupráce zejména s *Federal Bureau of Investigation* a *Department of Homeland Security.* V oblasti právní úpravy pak zástupci NBÚ předávali zkušenosti zástupcům Kongresu a koordinátorovi Bílého domu pro otázky kybernetické bezpečnosti[9].

V roce 2015 NBÚ také pokračoval v rámci několika evropských projektů v poskytování asistence státům, které budují systém kybernetické bezpečnosti. Za tím účelem se uskutečnily workshopy o institucionálním, právním a technickém rámci kybernetické bezpečnosti pro Jordánsko, Srbsko a pro Bosnu a Herzegovinu.

Zástupci NBÚ také v rámci instrumentu TAIEX Evropské komise prezentovali na žádost ukrajinské vlády v Kyjevě.

V rámci projektu Enhancing Cyber Security pak zástupce NBÚ pravidelně přednáší vládním bezpečnostním týmům v Makedonii, Moldávii a Kosovu. V roce 2015 proběhly dva workshopy pro členy jejich CERT/CSIRT týmů, první zaměřený na budování CERT/CSIRT týmu z hlediska technického a organizačního (působnost, typy útoků, nabízené služby, techniky shromažďování informací, personální náročnost), druhý na forenzní analýzu a table-top cvičení simulující útoky na součásti státní infrastruktury a phishingovou kampaň z interního pohledu CERT/CSIRT týmu.

Na bilaterální úrovni se v oblasti kybernetické bezpečnosti angažuje i Ministerstvo obrany, které spolupracuje s ozbrojenými silami USA v rámci programu Mil-to-Mil, s Izraelem a dalšími státy.

[9] Viz kapitola 4.8.5

4.7. GÉANT / Trusted Introducer

GovCERT.CZ je již druhým rokem akreditovaným členem evropského sdružení Trusted Introducer. Tato instituce, působící v rámci evropské organizace GÉANT (dříve TERENA), sdružuje bezpečnostní týmy vládní, národní, akademické a komerční sféry z celého světa. V rámci svého členství se GovCERT.CZ účastní pravidelných neveřejných setkání komunity, která slouží ke sdílení know-how, vyvíjených aplikací, zkušeností a informací o řešených incidentech apod. Dalším přínosem je výměna dat a informací o nakažených stanicích, webových stránkách, zranitelnostech, kampaních a dalších informací užitečných pro CERT/CSIRT komunitu. V neposlední řadě GovCERT.CZ těží rovněž z přístupu k uzavřenému, šifrovanému mailing listu a kontaktům, které v případě problému závažného svou povahou či geografickým dopadem slouží k časnému varování členů.

4.8. Účast na mezinárodních kybernetických cvičeních

NBÚ dlouhodobě vnímá cvičení kybernetické bezpečnosti jako optimální nástroj nejen pro procvičování technických schopností a znalostí, ale rovněž i pro testování a ověřování komunikačních kanálů, rozhodovacích pravomocí a interních postupů v případech řešení kybernetických bezpečnostních incidentů. Pravidelně se proto účastní jak technicky orientovaných cvičení, tak table-topů[10] spočívajících v odborných diskuzích souvisejících s řešením hypotetické krizové situace. V roce 2015 NBÚ participoval na celkem šesti cvičeních, z nichž čtyři byla mezinárodní. U zbývajících dvou národních cvičení NBÚ vystupoval přímo jako organizátor a hostitel.[11]

4.8.1. Crisis Management Exercise

Mezinárodní cvičení orgánů krizového řízení NATO Crisis Management Exercise proběhlo ve dnech 4. – 10. března 2015. Hlavním koordinátorem cvičení na národní úrovni byla Sekce obranné politiky a strategie MO. NBÚ měl svého zástupce v ředitelství cvičení, které bylo odpovědné za monitoring celkového vývoje cvičení a hodnocení splnění cílů a úkolů. Současně GovCERT.CZ vystupoval jako cvičící v připraveném scénáři týkající se kompromitace řídicích systémů SCADA v sítích zajišťujících přenos elektrické energie. Tato kybernetická část tvořila pouze jednu z dějových linek celého scénáře, který byl

[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.

[11] NBÚ se podílel na organizaci dvou národních cvičeních, o kterých bude blíže pojednáno v kap. 6.7.

zaměřen na komplexní řešení krizové situace ve fiktivní oblasti Indického oceánu s následným ohrožením bezpečnosti některých členských států NATO a partnerských zemí. Cílem cvičení na národní úrovni z pohledu gesce NBÚ bylo procvičit si bilaterální spolupráci mezi Českou republikou a Polskem a paralelně mezi GovCERT.CZ a českým operátorem elektroenergetické přenosové sítě při řešení kybernetického bezpečnostního incidentu.

4.8.2. Locked Shields

Česká republika se v roce 2015 opět zapojila také do největšího mezinárodního technického cvičení kybernetické bezpečnosti Locked Shields (LS15). Toto cvičení je každoročně pořádáno prostřednictvím CCDCoE v Tallinnu v Estonsku.

Cvičení je z mnoha pohledu unikátní. Odehrává se v simulovaném prostředí s desítkami počítačů a serverů, kde proti sobě stojí zástupci jednotlivých zemí v roli modrých týmů, jejichž úkolem je bránit vlastní infrastrukturu, a červený tým tvořený útočníky. Cvičení navíc probíhá v reálném čase, využívá reálné technologie, sítě a metody a rovněž je pravidelně obohacováno o aktuální trendy z oblasti kybernetické bezpečnosti. Cílem cvičení je otestovat technické dovednosti zúčastněných týmů, a navíc také schopnost reagovat a přizpůsobovat se nečekaným okolnostem z hlediska práva a komunikace s médii v případě krize. Zároveň je to jediné bodované cvičení, kterého se NBÚ pravidelně zúčastňuje. V roce 2015 se do cvičení zapojil rekordní počet více jak 400 odborníků z 16 zemí.

Konečným vítězem LS'15 se stal tým NATO Computer Incident Response Capability. Česká republika skončila na celkovém sedmém místě, získala však prvenství ve dvou ze tří samostatných kategorií, právní a mediální. Česká republika byla v roce 2015 zastoupena nejen vlastním modrým týmem; dva pracovníci NCKB podpořili také bílý tým, jenž se podílí na celkové organizaci, tvorbě scénářů a hodnocení.

4.8.3. Cyber Coalition

Na základě Memoranda o porozumění a spolupráci v oblasti kybernetické obrany mezi NATO a Českou republikou se NBÚ a MO v roce 2015 již popáté společně zapojili do každoročního aliančního cvičení kybernetické bezpečnosti Cyber Coalition. Mezinárodní cvičení Cyber Coalition 2015 (CC15), které proběhlo ve dnech 16. – 20. listopadu 2015 pod řízením Velitelství NATO pro transformaci (Allied Command Transformation) a dohledem Vojenského výboru NATO, se účastnilo více než 700 odborníků na kybernetickou bezpečnost z členských a partnerských zemí Aliance.

Na národní úrovni bylo cvičení organizováno zástupci NBÚ, kteří nesli odpovědnost za koordinaci cvičení na vládní úrovni, a MO, odpovědné za přípravu za vojenskou část. Centrálně bylo CC'15 moderováno z estonského Tartu. Hlavní cvičící operační složky v České republice byly GovCERT.CZ a Centrum CIRC MO. Stejně jako v minulém roce cvičily oba týmy odděleně – Centrum CIRC MO ve svých prostorách na půdě Univerzity obrany v Brně a GovCERT.CZ v prostorách NCKB rovněž v Brně. Na obou lokalitách byly přítomny tzv. společné týmy složené ze zástupců státní správy (MO, NBÚ, ÚZSI, BIS, MZV, PČR), soukromého sektoru (CSIRT.CZ, AVAST) a akademické sféry (Masarykova univerzita).

Scénáře CC'15 byly koncipovány tak, aby umožnily procvičit si rozhodovací procesy, technickou i netechnickou koordinaci při řešení kybernetických bezpečnostních incidentů, zlepšit sdílení informací o situaci včetně výměny klasifikovaných technických informací během kybernetické krize a s tím spojenými právními otázkami. Česká republika byla hojně zastoupena v rámci všech scénářů, které byly zaměřené jak na řešení technických problémů a právních otázek, tak i na koordinaci mezi jednotlivými orgány a rezorty.

4.8.4. CECSP 2015 Exercise

Dne 25. listopadu 2015 proběhlo komunikační cvičení v rámci Středoevropské platformy pro kybernetickou bezpečnost. Jednalo se o několikahodinové cvičení, kterého se zúčastnili zástupci CERT týmů České republiky, Maďarska, Polska, Slovenska a Rakouska. Jeho cílem bylo otestovat nastavené komunikační kanály a výměnu informací mezi kontaktními osobami v případě detekování podezřelé aktivity na stránkách operátorů kritické informační infrastruktury.

4.8.5. Cvičení pro US Cyber Command

V roce 2015 NBÚ uskutečnil první cvičení na klíč pro zahraničního partnera. Jednalo se o americké Ministerstvo obrany a velitelství kybernetických sil USA (US CYBERCOM). Na jejich žádost NBÚ vyslal dva experty a připravil modul do vzdělávacího programu budoucích členů velitelství kybernetických sil a dalších složek. Zaměstnanci NBÚ připravili specializované školení a návazné strategické table-top cvičení reflektující aktuální dění ve světě. Událost měla kladný ohlas a představitelé Pentagonu projevili zájem o opakování i v roce 2016.

4.9. Projekt Honeynet

Od června 2015 jsou dva pracovníci GovCERT.CZ členy české pobočky mezinárodní neziskové 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 také plánováno zveřejňování nově získaných poznatků ze síťových pastí (honeypotů) v rámci komunity zapojené do projektu.

V rámci přípravy na zpracování většího množství sledovaných lokalit a v nich nasazených honeypotů GovCERT.CZ přizpůsobil svou strategii sběru a analýzy získaných dat. V průběhu roku 2015 bylo vytvořeno s pomocí ELK (Elasticsearch, Logstash a Kibana) rozhraní pro sběr, předzpracování, uložení a vizualizaci dat zachycených honeypoty GovCERT.CZ. Rozhraní je stále ve vývoji a probíhá jeho optimalizace pro možnost nasazení v produkčním prostředí. Cílem je vytvoření různých pohledů nad uloženými daty, aby bylo možné snadněji zpracovávat a vizualizovat velké objemy dat. Údaje tak bude možné zobrazovat například podle honeypotu, který tyto informace vygeneroval, podle instituce, ve které je nasazen, nebo zobrazit celkový pohled na sumarizovaná data ze všech honeypotů.

Dále probíhá experimentální nasazování jednotlivých typů honeypotů s cílem identifikovat množinu těch nejužitečnějších a připravit je k nasazení v takové kombinaci, aby nebyly rozeznatelné od skutečných produkčních systémů, a verzích vhodných pro hromadné nasazení a správu. Průběžné výstupy jsou publikovány na GitHubu GovCERT.CZ (https://github.com/GovCERT-CZ) a informace sdíleny jak v rámci české kapitoly, tak mezinárodně.

5. NÁRODNÍ SPOLUPRÁCE

Vedle vládního týmu GovCERT.CZ pokračovalo v roce 2015 budování dalších bezpečnostních týmů CERT/CSIRT ve veřejném i soukromém sektoru. Počet českých týmů u Trusted Introducer se zvýšil v roce 2015 o šest na 22, z nichž pět je akreditovaných a jeden se připravuje na certifikaci v roce 2016; celkem v ČR operuje již 24 týmů CERT/CSIRT. Významnou úlohu hrál tradičně národní tým CSIRT.CZ provozovaný sdružením CZ.NIC, které své postavení stvrdilo ve výběrovém řízení a bude v této činnosti nadále pokračovat podle veřejnoprávní smlouvy s NBÚ předvídané zákonem o kybernetické bezpečnosti.

Kromě technické úrovně se národní spolupráce rozvíjela i v oblasti institucionální a vzdělávací, byly navázány kontakty mezi jednotlivými aktéry kybernetické bezpečnosti z řad policie, justice, armády či zpravodajských služeb, ale i akademické obce. Jejich zástupci se rovněž zúčastnili národních cvičení kybernetické bezpečnosti zorganizovaných NBÚ samostatně či ve spolupráci s Masarykovou univerzitou v Brně.

5.1. Bezpečnostní tým CSIRT.CZ

Dosavadní technická spolupráce CSIRT.CZ s GovCERT.CZ při řešení bezpečnostních incidentů byla v roce 2015 rozšířena o krátkodobé stáže pracovníků GovCERT.CZ. GovCERT.CZ a CSIRT.CZ začaly připravovat sdílení informací z honeypotů, sdílení know-how a zkušeností týkajících se skenování zranitelnosti webových stránek. Týmy spolupracovaly i na mezinárodních cvičeních kybernetické bezpečnosti[12].

V roce 2015 se CSIRT.CZ stal prvním českým členem v mezinárodní organizaci FIRST sdružující bezpečnostní týmy z vládního, komerčního a akademického sektoru.

V oblasti své působnosti CSIRT.CZ v roce 2015 pokračoval v realizaci či nově zahájil několik projektů. Projekt TURRIS sdružení CZ.NIC v roce 2015 zahrnoval již téměř 2000 zapojených routerů, přičemž získané výstupy o potenciálně škodlivých IP adresách byly integrovány také do projektu IntelMQ s cílem jiným CSIRT/CERT týmům usnadnit využívání výsledků projektu TURRIS. Prostřednictvím služby Skener webu otestoval v roce 2015 zdarma 118 českých webů na bezpečnostní zranitelnosti a vydal přes 900 doporučení k možným vylepšením konkrétních webových aplikací. V rámci Programu bezpečnostního výzkumu ČR pak v roce 2015 zahájil v pilotním provozu pětiletý projekt PROKI - Predikce a ochrana před kybernetickými incidenty, jehož cílem je automatizace sběru a hlášení bezpečnostních

[12] Viz kapitola 4.8

incidentů. V dubnu 2015 CSIRT.CZ a CZ.NIC rovněž zahájily Evropskou unií financovaný projekt CS Danube (Cyber Security Danube) zaměřený na posílení důvěry a spolupráce mezi bezpečnostními týmy CERT/CSIRT z Rakouska, Slovenska, Chorvatska, Srbska a Moldavska, školení, sdílení jejich know-how a nástrojů.

CSIRT.CZ samozřejmě pokračoval v informování veřejnosti o bezpečnostním dění a o nákaze v doméně .CZ a školení IT odborníků, osvětě běžných uživatelů a publikační činnosti. V roce 2015 mimo jiné vydal přes 400 zpráv o aktualitách, každý měsíc řešil přes sto škodlivých URL a členové týmu proškolili přes 340 lidí v tématech jako praktické stránky počítačové bezpečnosti, technická opatření Zákona o kybernetické bezpečnosti a zakládání CSIRT/CERT týmu.

5.2. Další bezpečnostní týmy CSIRT

GovCERT.CZ udržuje úzké vztahy i s dalšími bezpečnostními týmy v ČR, v prvé řadě s CSIRT Masarykovy univerzity (CSIRT-MU) při Ústavu výpočetní techniky (ÚVT-MU), který svou odbornost evropské úrovně plánuje v roce 2016 potvrdit získáním certifikace sdružení Trusted Introducer. Spolupráce s GovCERT.CZ probíhala i v roce 2015 zejména na technické úrovni při národním cvičení Cyber Czech a při mezinárodních cvičeních[13]. NBÚ se dále podílel na projektu Kybernetického polygonu poskytujícího virtuální prostředí pro simulaci kybernetických útoků využitelné pro cvičení kybernetické bezpečnosti slavnostně otevřeného v dubnu 2015. Spolupráce byla i v roce 2015 posilována krátkodobými stážemi zaměstnanců GovCERT.CZ u CSIRT-MU, kde se seznámili s jejich pracovními postupy a vyměnili si zkušenosti ze zvládání incidentů.

Dalším bezpečnostním týmem úzce spolupracujícím s GovCERT.CZ je Centrum CIRC v rezortu MO (C-CIRC MO), jehož pracovníci se aktivně zapojují do mezinárodních kybernetických cvičení a podílejí se na výměně informací o bezpečnostních událostech[14].

Z ostatních bezpečnostních týmů je namístě zmínit zejména tým sdružení CESNET (CESNET-CERTS) podílející se na sdílení dat o stanicích zapojených do botnetu získávaných na základě spolupráce se společností Microsoft[15] a v budoucnu snad i sdílení know-how a dat z honeypotů, jež CESNET-CERTS provozuje. Obdobně nelze pominout CERT tým operátora O2 Czech Republic, s nímž NBÚ v roce 2015 realizoval finální fázi projektu automatického

[13] Viz kapitola 4.8 & 5.7
[14] Viz kapitola 4.8 & 5.4
[15] Viz kapitola 3.3

rozhraní pro hlášení kybernetických bezpečnostních incidentů týkajících se významných informačních systémů v operátorově síti.

Spolupráci mezi bezpečnostními týmy činnými v ČR podporuje například pracovní skupina CSIRT.CZ, která se schází dvakrát či třikrát ročně k diskusi o tématech jako aktuální trendy v oblasti bezpečnosti a bezpečnostních hrozeb, rozvoj další spolupráce mezi bezpečnostními týmy či výměna zkušeností z řešení bezpečnostních incidentů a jejich předcházení. V roce 2015 proběhly dvě pracovní skupiny; v lednu Pracovní skupina CSIRT.CZ s otevřenou částí pro širší bezpečnostní komunitu a uzavřenou pro CSIRT/CERT týmy, v červnu pak pracovní skupina pro CSIRT týmy a členy stále rostoucího projektu FENIX sdružení NIX.CZ, kteří se nadále budou setkávat společně v rámci Pracovní skupiny CSIRT.CZ.

V rámci koordinační úlohy NCKB při řešení kybernetických bezpečnostních incidentů, a s cílem posílit komunikační kanály s ostatními bezpečnostními týmy a dalšími případnými partnery z řad KII/VIS v roce 2015 NBÚ rovněž pracoval na elektronické komunikační a kolaborační platformě. Prakticky se jedná o videokonferenční systém, který kromě teleprezenčních a komunikačních služeb může nabídnout možnost online kolaborace zapojených účastníků nad zpracovávaným obsahem. Celá platforma poběží v zabezpečeném režimu a bude pod výlučnou správou a kontrolou NCKB. Systém pracuje samostatně, nezávisle na službách třetích stran nebo podpůrných technologií typu cloud. Veškerá komunikace mezi účastníky bude probíhat šifrovaně. Dostupnost platformy je zajištěna prostřednictvím internetového připojení, s minimálními nároky na stanice zapojených účastníků. Přístupová práva budou distribuována mezi kooperující subjekty a jednotlivé uživatele prostřednictvím NBÚ. Vysoký potenciál kolaborační platformy lze dále využít v průběhu příprav kybernetických cvičení nebo v neposlední řadě pro pořádání online jednání, školení a jinou vzdělávací činnost.

5.3. Policie České republiky a zpravodajské služby

Z Národní strategie kybernetické bezpečnosti na období let 2015-2020 vyplývají specifické úkoly i pro Policii ČR a zpravodajské služby, zejména ve vztahu k budování kapacit pro boj s počítačovou kriminalitou a zajišťování národní bezpečnosti. V roce 2015 Policie ČR dále pracovala na strukturálních a organizačních změnách tak, aby specializovaný celorepublikový útvar, o jehož zřízení rozhodl policejní prezident již v roce 2014, měl dostatečné personální a materiální zajištění. Zástupci policie své schopnosti testovali i během cvičení kybernetické bezpečnosti, jichž se účastnili, a rozvíjeli technickou spolupráci s GovCERT.CZ a zahraničními partnery včetně Europolu.

Zpravodajské služby se rovněž účastnily cvičení kybernetické bezpečnosti a pracovaly na plnění úkolů, které jim ukládá Akční plán.

5.4. Ministerstvo obrany

Ministerstvo obrany úzce spolupracuje s NBÚ na strategické i technické úrovni. K zajištění rychlé a operativní vzájemné spolupráce bylo dne 9. května 2015 uzavřeno „Prováděcí ujednání o vzájemné podpoře v oblasti kybernetické bezpečnosti a kybernetické obrany“ na základě „Rámcové dohody o vzájemné podpoře vybraných činností mezi MO a NBÚ“.

Poradním a koordinačním orgánem v rámci MO je Rada pro kybernetickou bezpečnost Ministerstva obrany (RKB MO), které předsedá bezpečnostní ředitel MO, jenž byl rozhodnutím ministra určen gestorem kybernetické bezpečnosti na úrovni MO. V podřízenosti bezpečnostního ředitele bylo ke dni 1. června 2015 zřízeno oddělení kybernetické bezpečnosti (OKB), které zabezpečuje odborné a metodické řízení a koordinaci činností v oblasti kybernetické bezpečnosti. OKB mělo ke konci roku 2015 tři zaměstnance z plánovaných devíti. Pro realizaci konkrétních úkolů a opatření RKB MO byly vytvořeny dvě pracovní skupiny, a to pro zajištění implementace požadavků ZKB a pro zpracování Strategie kybernetické bezpečnosti MO a Akčního plánu KB MO na období let 2016 až 2020.

5.5. Akademická sféra

Akademická obec patří mezi důležité partnery v kybernetické bezpečnosti. Spolupráce začala přípravou ZKB, pokračuje při realizaci národních i mezinárodních cvičení kybernetické bezpečnosti a sdílení informací a zkušeností z řešení kybernetických bezpečnostních incidentů, a v roce 2015 se rozšířila i do oblasti vzdělávání.

Ve spolupráci s Ministerstvem školství, mládeže a tělovýchovy ČR, Ministerstvem práce a sociálních věcí ČR, odborníky z dalších orgánů veřejné správy, neziskových organizací a partnery ze soukromého sektoru byl v roce 2015 vypracován první „Návrh koncepce vzdělávání v oblasti kybernetické bezpečnosti“. Jedná se o ucelený materiál, zdůvodňující potřebu modernizace a systematizace procesu vzdělávání v ČR, který je rozdělen do tří kapitol. Na rok 2016 je plánováno připomínkové řízení a následně její předložení vládě. Koncepce vzdělávání je rozdělena do tří kapitol; první je věnována obecnému vzdělávání především široké veřejnosti a subjektů, které toto vzdělávání zajišťují či v jeho rámci jakkoli působí, a dále dělena podle konkrétních cílových skupin, u nichž se zaměřuje na získání základního povědomí o kybernetické bezpečnosti, rizicích vyplývajících z užívání technologií

ICT, dodržování bezpečnostních pravidel a osvojení si digitální hygieny. Druhá kapitola se věnuje specifickým skupinám, které již určitou úroveň znalostí mají, a cílí na jejich prohlubování a získávání nových zkušeností. Tato kapitola zahrnuje například správce KII a VIS, akademickou sféru, bezpečnostní složky ČR a orgány činné v trestním řízení, veřejnou správu, soukromý sektor a pracoviště typu CERT/CSIRT. Poslední kapitola se týká vzdělávání zaměstnanců NBÚ.

Tradičně intenzivní spolupráce NBÚ probíhala s Masarykovou univerzitou v Brně. Kromě technické spolupráce týmů CSIRT-MU při Fakultě informatiky, ÚVT-MU, a GovCERT.CZ[16] se zástupci NBÚ podíleli i na výuce na Fakultě sociálních studií, kde v zimním semestru 2015/2016 zajišťovali výuku ve čtyřech předmětech bakalářského a magisterského programu o tématech spojených s kybernetickou bezpečností. Právnická fakulta, jmenovitě Ústav práva a technologii, v tomtéž semestru iniciovala neformální diskusní platformu pro pravidelná setkávání právníků zabývajících sekybernetickou bezpečností a souvisejícími obory v akademii, NBÚ, justici a dalších složkách státní správy, tzv. CyberCake. V roce 2015 NBÚ navíc spustil program studentských stáží v NCKB, který do konce roku v rozsahu 1-3 měsíce absolvovalo 8 studentů z Fakulty sociálních studií a Pedagogické fakulty MU a z Fakulty podnikatelské Vysokého učení technického v Brně (VUT). Program je otevřen i studentům jiných relevantních oborů a všem vysokým školám v ČR.

O kybernetické bezpečnosti zástupci NBÚ v zimním semestru 2015/2016 přednášeli i na Palackého univerzitě v Olomouci. V průběhu roku NBÚ uzavřel rámcové smlouvy o spolupráci s Vysokou školou báňskou – Technickou univerzitou Ostrava, Univerzitou Tomáše Bati ve Zlíně, Jihočeskou univerzitou v Českých Budějovicích a Karlovou univerzitou v Praze. Vzdělávání v kybernetické bezpečnosti i společné výzkumné či jiné projekty tedy budou mít v budoucnosti příležitost rozvíjet se i na dalších veřejných vysokých školách.

V té souvislosti bylo v roce 2015 v rámci plnění Akčního plánu provedeno mapování vysokoškolských programů, oborů a předmětů s cílem zjistit možnosti výuky, kterou nabízí české akademické prostředí. Mapování zahrnovalo technické i humanitní směry, bylo osloveno celkem 38 vysokých škol, z čehož výsledný počet technických oborů dosud činil 102 a dosavadní počet humanitních byl 18. Součástí mapování bylo vytvoření jmenného seznamu kontaktních osob pro problematiku kybernetické bezpečnosti za jednotlivé vysoké školy. Odkazy na tyto programy, obory a předměty je v plánu zpřístupnit veřejnosti prostřednictvím vlastního osvětového portálu, který NBÚ připravuje spustit v roce 2016.

[16] Viz kapitola 4.8

5.6. Další partneři

Mezi další partnery, se kterými v průběhu roku 2015 rozvíjel NBÚ spolupráci, patří například peeringové sdružení NIX.CZ, projekt FENIX, Asociace krajů a její jednotliví členové jako Kraj Vysočina, AFCEA, nebo nevládní sdružení Národní centrum bezpečnějšího internetu. Prostřednictvím České bankovní asociace spolupracuje NBÚ s bankami, které mají zájem na zvyšování ochrany své počítačové infrastruktury.

5.7. Národní cvičení CYBER CZECH 2015

5.7.1. Teoretické cvičení

Ve dnech 16. – 18. června 2015 uspořádal NBÚ ve spolupráci s European Cyber Security Initiative a European Defence Agency cvičení kybernetické bezpečnosti s názvem Strategic Decision Making Course & Exercise on Cyber Crisis Management.

Cvičení se uskutečnilo v prostorách NBÚ v Praze a jeho cílem bylo formou table-top prověřit schopnosti státu činit rozhodnutí a účinně používat dostupné prostředky při řešení krize v kybernetickém prostoru. Hlavní důraz cvičení byl kladen na procvičení komunikačních kanálů a spolupráce při řešení kybernetických bezpečnostních incidentů mezi čtyřmi základními složkami: i) zástupci vlády a dalších exekutivních složek, ii) zástupci armády a zpravodajských služeb, iii) zástupci policejních složek a státních zástupců, iv) reprezentanti soukromého sektoru. NBÚ zastával roli hostitele a současně posílil vládní a právní cvičící tým dvěma svými pracovníky.

5.7.2. Technické cvičení

NBÚ ve spolupráci s Ústavem výpočetní techniky Masarykovy univerzity uspořádal ve dnech 6. a 7. října 2015 první ročník národního technického cvičení kybernetické bezpečnosti CYBER CZECH 2015. Toto cvičení se uskutečnilo ve speciálním prostředí Kybernetického polygonu v Brně. V tomto prostředí je možné simulovat komplexní scénáře útoků vedených proti prvkům kritické informační infrastruktury a vyhodnocovat jejich průběh.

Hlavním cílem bylo ověřit praktické znalosti zvládání kybernetických incidentů v souvislosti s ochranou prvků kritické informační infrastruktury České republiky a procvičit postupy podle zákona č. 181/2014 Sb., o kybernetické bezpečnosti včetně komunikace s médii při zvládání nastalé krize. Cvičení se v roli obránců, tzv. modrých týmů, zúčastnilo dvacet zástupců z řad ministerstev a dalších subjektů kritické informační infrastruktury.

Jejich úkolem bylo bránit informační infrastrukturu fiktivní jaderné elektrárny, na kterou útočil tým hackerů, tzv. červený tým, složený ze zaměstnanců NBÚ a Masarykovy univerzity. Cvičení bylo celkově hodnoceno jako přínosné, propracované a po technické i příběhové stránce velmi dobře zorganizované.

6. ZVYŠOVÁNÍ POVĚDOMÍ A OSVĚTA

S ohledem na vstup zákon o kybernetické bezpečnosti v účinnost se NBÚ v uplynulém roce zaměřil především na vysvětlování práv a povinností v zákoně obsažených. Odborné i široké veřejnosti méně i více podrobně vysvětloval jednotlivá ustanovení zákona a z nich vyplývající práva a povinnosti, zejména pro správce prvků KII a VIS. NBÚ k tomu využil především různé konference a semináře, kde účastníky zajímaly zejména konkrétní dopady zákona na jejich činnost, kritéria a způsob, jakým budou jednotlivé prvky KII a VIS určovány, a v neposlední řadě termíny, ve kterých budou muset plnit zákonem stanovené povinnosti.

Konkrétní informační akcí k zákonu o kybernetické bezpečnosti byl například květnový celodenní seminář, který NCKB uspořádalo na půdě Fakulty podnikatelské VUT. Na něm byla objasněna ustanovení ZKB především těm, na které přímo dopadá, tedy například ICT manažerům, ICT administrátorům, právníkům, bezpečnostním ředitelům a zástupcům povinných osob podle ZKB.

Pro pomoc a usnadnění orientace v problematice zákona o kybernetické bezpečnosti NBÚ pravidelně vydává a aktualizuje množství podpůrných materiálů, které průběžně zveřejňuje na webových stránkách NCKB www.govcert.cz. Obdobnou osvětovou činnost vyvíjí i CSIRT.CZ a další české bezpečnostní týmy.

V květnu byl pod záštitou NBÚ, Masarykovy univerzity v Brně a odborného časopisu Global Politics uspořádán 2. ročník konference *„CyberCon Brno 2015“.* Konference byla primárně určena pro odbornou veřejnost a akademickou sféru. Hlavní témata příspěvků byla „kybernetické bojiště“, „právní aspekty kybernetické bezpečnosti“ či „kybernetické hrozby a společnost“.

Zástupci NBÚ vysvětlovali důležitost kybernetické bezpečnosti včetně problematiky zákona o kybernetické bezpečnosti rovněž médiím. Odborníci z NCKB komentovali v médiích různé události, které byly způsobeny hackery nebo nestandardním chováním některých informačních systémů, vyjadřovali se k preventivním krokům a k eliminaci následků těchto událostí. Díky zájmu některých odborných médií byly prezentovány podstatné parametry zákona a příslušných vyhlášek. Velmi atraktivní bylo pro média první technické kybernetické cvičení Cyber Czech 2015[17].

[17] Viz kapitola 5.7

Ve spolupráci se stážisty z Pedagogické fakulty Masarykovy univerzity v Brně připravuje NBÚ pilotní e-learningový kurz *„Digitální stopa“* určený pro žáky II. stupně ZŠ. Kurz je pojat zábavnou interaktivně-detektivní formou, kdy musí žáci postupně rozplétat složitý příběh. Kurz bude doprovázet i metodika pro učitele a bude zkušebně testován na několika základních školách. S nevládním sdružením Národní centrum bezpečnějšího internetu bylo v průběhu roku 2015 připraveno memorandum o spolupráci zejména v oblasti osvěty a metodických a výukových materiálů.

NBÚ dále vypracoval Návrh koncepce vzdělávání v oblasti kybernetické bezpečnosti, který vychází z aktuálních domácích i zahraničních zkušeností[18]. Materiál vznikal především ve spolupráci s Ministerstvem školství, mládeže a tělovýchovy a jeho Národním ústavem pro vzdělávání, dále s Ministerstvem práce a sociálních věcí a za podpory dalších odborníků, kteří se vzděláváním v ICT a zvyšováním digitální gramotnosti dlouhodobě zabývají. Materiál především určuje podobu bezpečnostního vzdělávání pro jednotlivé cílové skupiny a doporučuje vhodné nástroje. Úloha NBÚ spočívá vedle poskytnutí vlastní expertízy v koordinaci vzdělávacích kapacit národních i zahraničních partnerských organizací.

Ve spolupráci s českou pobočkou AFCEA byl v září 2015 uskutečněn na Policejní akademii ČR seminář o kybernetické bezpečnosti. Zástupci NBÚ rovněž prezentovali na stánku AFCEA v rámci Mezinárodního veletrhu obranné a bezpečnostní techniky IDET. Sdružení AFCEA také ve spolupráci s NBÚ a Policejní akademií ČR vydalo 3. edici slovníku kybernetické bezpečnosti, který je zdarma k dispozici široké veřejnosti na našich internetových stránkách.

Odborníci NBÚ přednášeli o kybernetické bezpečnosti i na dalších fórech, pořádaných například Parlamentem České republiky.

NBÚ dále záštitou podpořil vybrané významné osvětové akce, například mezinárodní kampaň *„Evropský měsíc kybernetické bezpečnosti 2015“* vyhlašovanou každoročně Evropskou agenturou pro síťovou a informační bezpečnost (ENISA) a organizovanou neziskovým sdružením Národní centrum bezpečnějšího internetu, nebo řadu odborných konferencí organizovaných společností IDG, které byly zaměřené na problematiku bezpečnosti pro IT profesionály z různých oborů.

[18] Viz kapitola 5.5

V neposlední řadě odborníci NBÚ mnohokrát vystoupili na odborných konferencích, seminářích a diskutovali u kulatých stolů nad aktuálními tématy z oblasti kybernetické bezpečnosti a to jak na národní, tak na mezinárodní úrovni.

V osvětě se NBÚ mimo jiné angažoval také formou podpory Školního diáře 2015/2016. Tento diář vydává nadnárodní občanské sdružení Generation Europe a vychází ze vzdělávacího modelu, který kombinuje zábavu a vzdělání. Diář byl distribuován do škol po celé České republice a některými školami je pravidelně využívám při výuce.

PŘÍLOHY

Příloha č. 1 – Přehled nejvýznamnějších incidentů

První čtvrtletí roku 2015 se vyznačovalo četnými útoky na principu sociálního inženýrství, kdy útočníci na své oběti cílili pomocí sofistikovaných podvodných zpráv. Tyto podvodné zprávy ve většině případů obsahovaly škodlivou přílohu nebo odkaz směřující na podvodné webové stránky. Útočníci těmito zprávami v nejvíce případech cílili na zákazníky e-shopů, bank, zaměstnance státní správy a další skupiny.

V lednu byl nejvážnějším řešeným incidentem DDoS útok směřující na instituci státní správy, kde GovCERT.CZ na základě obdržených síťových logů zjistil, že zahlcení serveru pravděpodobně způsobil špatně nastavený čínský DNS server. Chybné nastavení následně způsobilo chybný překlad některých domén (torrenty, facebook, twitter, …) na náhodné IP adresy a tyto dotazy následně zahltily server instituce.

K nejzávažnějšímu útoku za měsíc únor patřila další vlna špionážního malware Turla, kdy docházelo k útoku na návštěvníka kompromitovaných IP adres a domén. Konkrétně se mezi nakaženými servery nacházela i jedna česká doména hostovaná v Rusku. Doména měla podle nám známých informací obsahovat škodlivý PHP skript neznámého účelu. Jelikož se jedná o špionážní kampaň, lze se domnívat, že skript měl za účel infikovat návštěvníka stránek, případně provést jinou činnost vedoucí k odcizení dat. Na základě nastavené spolupráce s institucemi státní správy a kritické informační infrastruktury se GovCERT.CZ týmu podařilo zjistit, že mezi návštěvníky těchto nakažených serverů bylo i několik počítačových stanic státní správy. Vzhledem k neúplnosti některých informací nebylo možné zjistit účel webového skriptu. V dotčených institucích proto došlo k reinstalaci počítačových stanic a ke změně hesel požívaných dotčenými uživateli.

Březen byl z hlediska incidentů zajímavý zranitelností v protokolu SSL/TLS známou pod označení FREAK. Touto zranitelností bylo ohroženo přibližně 70 serverů státních a jiných významných institucí. GovCERT.CZ s institucemi postupně navázal komunikaci a doporučil jim aktualizaci používaného systému, nebo jeho deaktivaci v případě, že SSL/TLS protokol nevyužívají.

V druhém čtvrtletí roku se GovCERT.CZ setkával zejména s incidenty typu podvodných zpráv, DDoS útoků nebo ransomware. Ve všech případech se jednalo o ransomware využívající v současnosti bezpečné šifry, které bez znalosti hesla nelze dešifrovat.

V květnu byl nejzávažnějším incidentem útok na webové stránky státní instituce, kdy se útočníkům z albánské skupiny AnonCoders podařilo neznámým způsobem napadnout server poskytovatele, na kterém běžely mimo jiných i webové stránky zmíněné instituce. Útočníkům se během útoku podařilo pozměnit obsah webových stránek, kde zanechali informace upozorňující, že došlo k napadení stránky.

Začátek léta se nesl v podání šifrovacích malware, kdy nezávisle na sobě došlo ke kompromitaci několika počítačových stanic na různých státních institucích a zašifrování uživatelského obsahu. Uživatelské obsahy stanic byly zašifrovány pomocí algoritmu AES-256, který je v současnosti bez znalosti hesla nedešifrovatelný. Administrátoři dotčených institucí byli i tak požádáni o zaslání vzorku zašifrovaných dat, která jsme se pokusili dešifrovat pomocí nástrojů, které využívají nalezené klíče na zabavených řídících (C&C) serverech.

Za období měsíce června lze zmínit ještě jeden řešený incident, kdy neznámí útočníci napadli webové stránky státní instituce. Na ně následně umístili škodlivý kód a pozměnili jejich obsah. Dále se útočníkům podařilo získat přístup k e-mailové schránce zaměstnance dotčené instituce. Útočníci z této adresy následně rozesílali smyšlené zprávy, ve kterých se vydávali za pracovníka instituce. Z dalších dostupných informací je zřejmé, že útok mohl být součástí rozsáhlejší Advanced Persistent Threat (APT) mezinárodní kampaně.

Za následující měsíce červenec a srpen se bezpečnostní incidenty týkaly převážně podvodných zpráv a jednoho severokorejského botnetu, do kterého byly zapojeni i uživatelé z České republiky. Významnou událostí z tohoto období pak je zjištění podezření na infikaci několika počítačů instituce státní právy malwarem Duqu 2. Toto podezření se v průběhu šetření události nepotvrdilo.

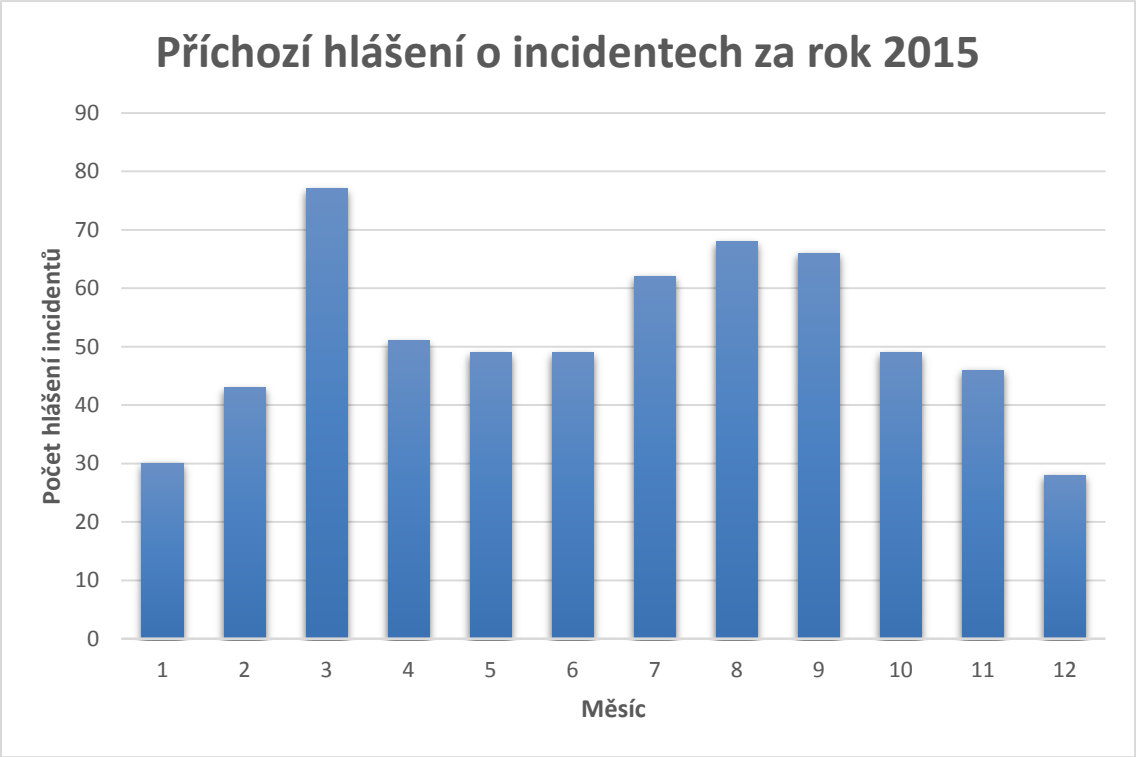
Počátek třetího čtvrtletí se vyznačoval zejména nárůstem infikace počítačů institucí státní správy ransomware. Tak jako v incidentech řešených v předchozím čtvrtletí i v těchto se jednalo šifrovací malware využívající algoritmu AES-256 a stejně jako v předešlých případech se větší část dat podařilo obnovit ze zálohy. V období třetího čtvrtletí byla také zaznamenána další phishingová kampaň, která cílila na státní instituce. Útočníci se v e-mailech vydávali za správce e-mailového serveru instituce a žádali uživatele buď o navýšení limitu e-mailové schránky, nebo o změnu přihlašovacího hesla přes zaslaný odkaz na patřičný formulář.

Za měsíc listopad byl nejvýznamnějším incidentem spear-phishingový útok, kdy se neznámým útočníkům podařilo infikovat pracovní počítač pracovníka státní správy a následně rozesílat podvodné zprávy na další státní instituce zemí Evropské Unie. Tyto zprávy obsahovaly jako přílohu malware, který byl následně identifikován jako špionážní malware Turla/Snake/Uroburos. Zprávy byly rozesílány v anglické a německé mutaci. Na řešení incidentu proto GovCERT.CZ spolupracoval s několika evropskými CERT týmy, včetně evropského CERT týmu CERT-EU.

Počet řešených bezpečnostních incidentů v roce 2015 rostl i ve sféře působnosti CSIRT.CZ, zejména v kategoriích malware a *„jiné“*, kam patří například fast flux, podvodné informace na webových stránkách, incidenty z honeypotů či problémy se SOHO routery.

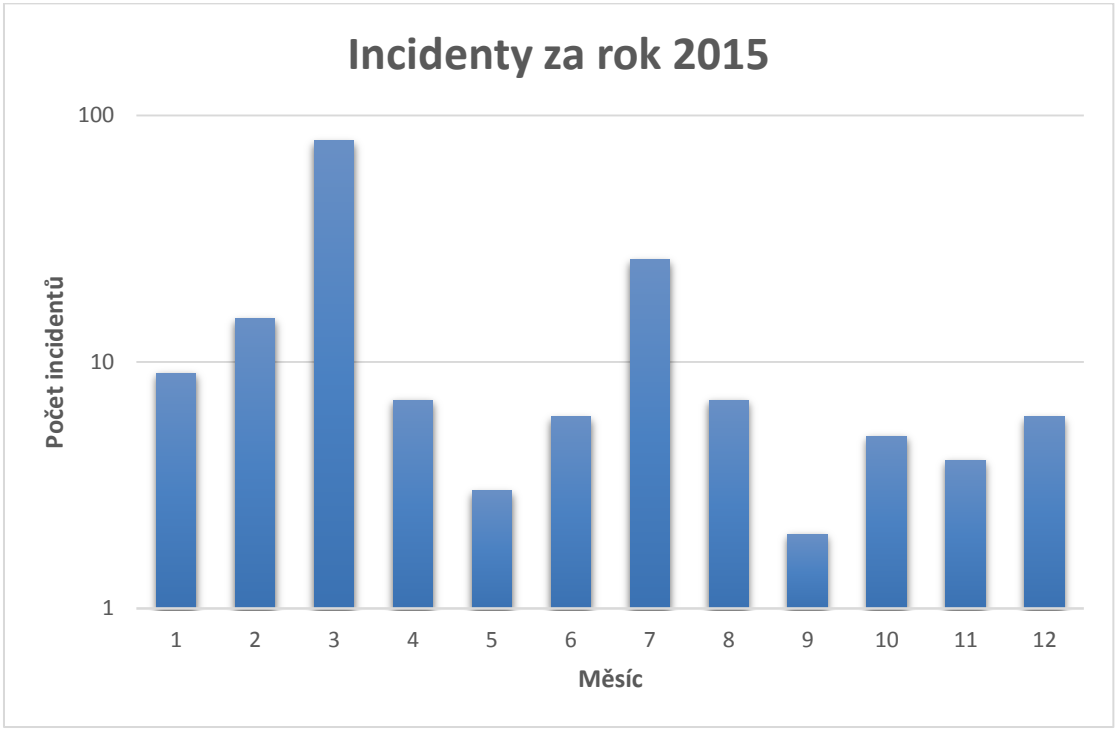
Příloha č. 2 – Statistiky

Kapitola graficky zachycuje počty přijatých hlášení, řešených incidentů a jejich klasifikaci v roce 2015.

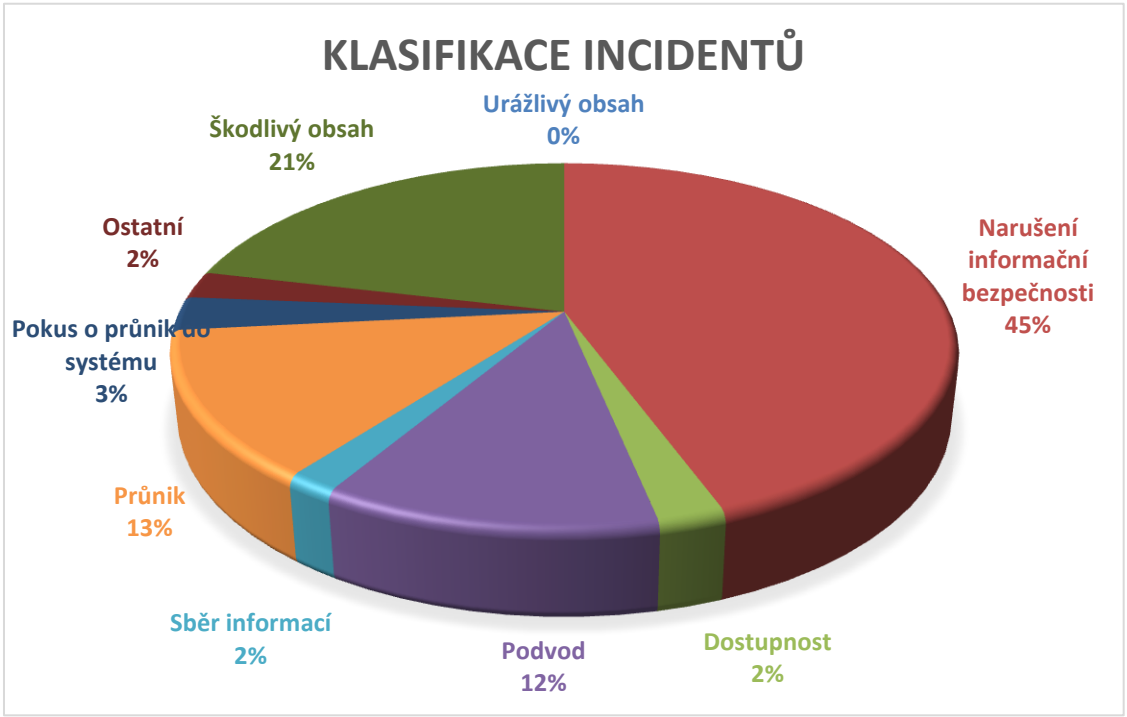


Graf 03 – počet příchozích hlášení o incidentech za jednotlivé měsíce v roce 2015[19]

[19] Jelikož incident mohl být nahlášen více institucemi a ne každý nahlášený incident byl pracovníky GovCERT.CZ ve výsledku označen jako incident, nejsou hodnoty uvedené v tomto grafu shodné s hodnotami v grafu (Graf 02) znázorňujícím počet incidentů.



Graf 04 – počet řešených incidentů za jednotlivé měsíce v roce 2015[20]



Graf 05 – klasifikace řešených incidentů za rok 2015

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

Příloha č. 3 - Seznam použitých zkratek a pojmů

Obsáhlejší výkladový slovník termínů kybernetické bezpečnosti je k nalezení na www.govcert.cz.

AFCEA – Armed Forces Communications and Electronics Association

APT – Advanced Persistent Threat – pokročilá a trvalá hrozba

C&C server – Command and control server – řídící server

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 1996 českými veřejnými vysokými školami a Akademií věd ČR

CSIRT – Computer Security Incident Response Team

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

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

DDoS útok – Distributed Denial of Service – distribuované odmítnutí služby, technika útoku na internetové služby nebo stránky, při níž dochází k přehlcení požadavky a k pádu nebo nefunkčnosti a nedostupnosti systému pro ostatní uživatele a to útokem mnoha koordinovaných útočníků

EC3 – European Cybercrime Centre – Evropské centrum pro boj s kybernetickou kriminalitou

EU – Evropská unie

GovCERT.CZ – vládní koordinační místo pro okamžitou reakci na kybernetické bezpečnostní incidenty (vládní CERT – Computer Emergency Response Team), které je organizační složkou Národního bezpečnostního úřadu, respektive jeho specializovaného pracoviště Národního centra kybernetické bezpečnosti

HONEYPOT – slouží jako návnada lákající útočníka, přičemž po zachycení potenciálně nebezpečného software dochází k jeho automatizované analýze

KII – kritická informační infrastruktura

KYBERKRIMINALITA – specifický druh kriminality páchané prostřednictvím výpočetních a komunikačních technologií

MALWARE – počítačový program určený ke vniknutí nebo poškození počítačového systému

MO – Ministerstvo obrany

MV – Ministerstvo vnitra

NATO – Severoatlantická aliance (North Atlantic Treaty Organization)

NBÚ – Národní bezpečnostní úřad

NCKB – Národní centrum kybernetické bezpečnosti

OBSE – Organizace pro bezpečnost a spolupráci v Evropě

OPEN-SOURCE – Jako open-source jsou označovány programy, jejichž zdrojový kód je dostupný všem uživatelům, kteří za předpokladu dodržení jistých podmínek, mohou tento kód dále využívat, prohlížet a upravovat

OTPVV – Oddělení teoretické podpory, vzdělávání a výzkumu

OWASP – Open Web Application Security Project

PČR – Policie České republiky

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

RANSOMWARE – druh malware, který v prvním kroku zašifruje data na pevném disku, počítač zamkne či jinak znepřístupní; v druhém kroku vyžaduje po uživateli výkupné (anglicky *„ransom“*) za jeho opětovné zpřístupnění

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. výroba elektrické energie), infrastrukturní (např. rozvod pitné vody) nebo zařízení (např. železniční stanice)

SPEAR PHISHING – podvodná technika k získávání citlivých údajů se zaměřením na určitou organizaci

TABLE-TOP – je cvičení navrženo 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

TURLA – pojmenování druhu malwaru

VIS – Významný informační systém

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

Příloha č. 4 – Hlášení o stavu naplňování Akčního plánu k Národní strategii kybernetické bezpečnosti České republiky na období let 2015 až 2020[21]

Umístěno jako příloha v samostatném dokumentu.

[21] 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 2015 a úkolů, které mají být plněny průběžně.