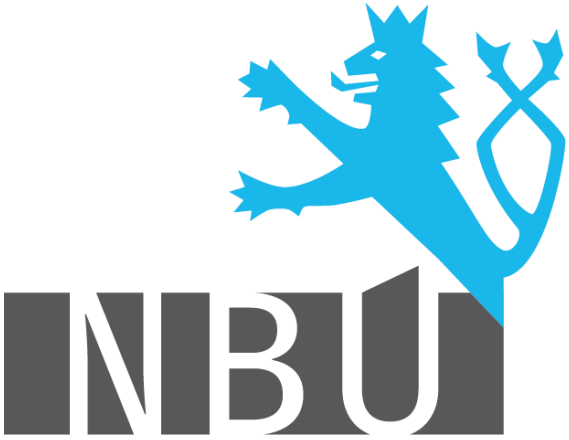
NÁRODNÍ BEZPEČNOSTNÍ ÚŘAD

Národní centrum kybernetické bezpečnosti



ZPRÁVA O STAVU

KYBERNETICKÉ BEZPEČNOSTI

ČESKÉ REPUBLIKY 2014

OBSAH

ÚVOD

Zajištění kybernetické bezpečnosti je jednou z klíčových výzev státu, přičemž její přesah do ostatních bezpečnostních odvětví je nesporný. Se vzrůstající závislostí státu a jeho obyvatel na informačních a komunikačních technologiích musí být stát schopen chránit kyberprostor tak, aby byla zachována bezpečnost České republiky a zároveň práva jedinců na informační sebeurčení.

Rok 2014 byl v oblasti zajištění kybernetické bezpečnosti České republiky velmi dynamický. Česká republika pokračovala v započatém budování kybernetických bezpečnostních kapacit společně s institucionálním a právním zakotvením činnosti gestora kybernetické bezpečnosti. Výsledkem tohoto procesu bylo zejména otevření Národního centra kybernetické bezpečnosti (dále „NCKB“) a přijetí zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně související zákonů (dále „ZKB“), a souvisejících prováděcích právních předpisů. Došlo také k posílení mezinárodní spolupráce v oblasti kybernetické bezpečnosti, kdy se Národní bezpečnostní úřad (dále „NBÚ“) mimo jiné zúčastnil mezinárodních cvičení zaměřených na technické i netechnické aspekty zajišťování kybernetické bezpečnosti. NBÚ v roce 2014 zorganizoval i první národní kybernetické cvičení a podílel se na zvyšování potřebného povědomí a osvěty v této oblasti.

Zpráva o stavu kybernetické bezpečnosti České republiky 2014 (dále „Zpráva“) je předkládána na základě usnesení vlády ze dne 23. května 2012 č. 364 o Strategii pro oblast kybernetické bezpečnosti České republiky na období let 2012 až 2015 a Akčním plánu opatření ke Strategii pro oblast kybernetické bezpečnosti České republiky na období let 2012 až 2015. Zpráva podává přehled plnění cílů v budování kybernetické bezpečnosti České republiky za období roku 2014 v 8 oblastech.

Těmito oblastmi jsou následující:

- Budování NCKB / GovCERT.CZ[1]
- Vývoj legislativy v oblasti kybernetické bezpečnosti
- Tvorba koncepčních dokumentů kybernetické bezpečnostní politiky České republiky

[1] GovCERT.CZ představuje 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.

- Informační systémy důležité pro stát a navázání komunikace se subjekty provozujícími kritickou informační infrastrukturu a významné informační systémy
- Mezinárodní spolupráce
- Národní spolupráce
- Zvyšování povědomí a osvěta
- Činnost GovCERT.CZ a sledování současných trendů v kybernetické bezpečnosti

Cílem této Zprávy je poskytnout ucelené informace o aktivitách státu při zajišťování kybernetické bezpečnosti České republiky.

1. BUDOVÁNÍ NCKB / GOVCERT.CZ

Vznik NCKB lze datovat ke konci roku 2011, kdy byl NBÚ usnesením vlády ze dne 19. října 2011 č. 781 pověřen jeho vybudováním. Od té doby byla provedena celá řada úkonů směřujících k vytvoření jeho operační kapacity. To zahrnovalo značné množství aktivit – od převzetí gesce pro oblast kybernetické bezpečnosti od Ministerstva vnitra (dále „MV"), přes převzetí či navazování nových vztahů s partnerskými úřady v zahraničí, vybudování prostor a zajištění technického zázemí nutného pro fungování NCKB, provedení výběrových řízení a náboru nových pracovníků, po řadu dalších úkonů administrativního charakteru.

Organizačně je NCKB součástí Sekce kybernetické bezpečnosti NBÚ a dělí se na dvě oddělení – GovCERT.CZ a Oddělení teoretické podpory, vzdělávání a výzkumu (dále „OTPVV"). Zatímco GovCERT.CZ je tým zejména IT specialistů zabývající se technickou stránkou kybernetické bezpečnosti zahrnující řešení kybernetických bezpečnostních incidentů subjektů spravujících důležité komunikační a informační systémy pro stát, analýzu malware, sběr a vyhodnocování informací o kybernetických útocích a hrozbách apod., OTPVV je odpovědné za přípravu národních strategií, kybernetických bezpečnostních politik, koordinaci s ostatními gestory bezpečnosti České republiky a zajištění plnění mezinárodních závazků a spolupráce v oblasti kybernetické bezpečnosti. Zároveň je odpovědné za určování kritické informační infrastruktury státu (dále „KII") a komunikaci mezi NBÚ a subjekty KII a správci významných informačních systémů (dále „VIS"). OTPVV také poskytuje nezbytnou právní a administrativní podporu GovCERT.CZ, zabývá se tvorbou vzdělávacích politik a vzděláváním v oblasti kybernetické bezpečnosti a do budoucna i koordinací výzkumu v oblasti kybernetické bezpečnosti na národní úrovni.

Slavnostní otevření nové budovy NCKB, ve které jsou umístěna pracoviště GovCERT.CZ a OTPVV, proběhlo dne 13. května 2014 za účasti předsedy vlády České republiky Bohuslava Sobotky, náměstka generálního tajemníka NATO pro nové bezpečnostní výzvy Sorina Ducaru, ředitele Evropské agentury pro bezpečnost sítí a informací (ENISA) Udo Helmbrechta, představitelů české bezpečnostní komunity a dalších významných hostů nejen z oblasti kybernetické bezpečnosti.

2. VÝVOJ LEGISLATIVY V OBLASTI KYBERNETICKÉ BEZPEČNOSTI

V roce 2014 došlo k několika podstatným událostem na poli kybernetické legislativy. Nejzásadnější bylo přijetí zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů. Příprava tohoto zákona byla uložena NBÚ usnesením vlády ze dne 19. října 2011 č. 781. Absence podobných předpisů v právním řádu České republiky nebo u zahraničních partnerů vedla k vytvoření v současné době ojedinělé koncepce zaměřující se na nastavení systému koordinace a kooperace mezi nejdůležitějšími subjekty kybernetické bezpečnosti a na zavedení bezpečnostních opatření k ochraně informačních a komunikačních systémů důležitých pro stát.

Vedle zákona o kybernetické bezpečnosti byly v roce 2014 vypracovány a schváleny také jeho prováděcí právní předpisy, tj. 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, která byla vypracována společně NBÚ a MV, a novela nařízení vlády ze dne 22. prosince 2010 č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury, kterou mělo v gesci MV.

2.1. Zákon č. 181/2014 Sb., o kybernetické bezpečnosti

Návrh zákona vypracovaný ve spolupráci s akademickou sférou, soukromým sektorem a dalšími státními institucemi byl schválen vládou dne 2. ledna 2014 a do konce června 2014 pak prošel všemi čteními v Poslanecké sněmovně Parlamentu České republiky. Při projednávání zákona došlo na základě připomínek poslanců k několika úpravám návrhu, nicméně původní koncept byl zachován. Následně byl zákon dne 23. července 2014 schválen Senátem Parlamentu České republiky a dne 13. srpna 2014 jej podepsal Prezident České republiky. ZKB vešel v účinnost k 1. lednu 2015.

Zákon stojí na třech následujících pilířích, zaměřených na:

(i) zavedení preventivních bezpečnostních opatření u KII a VIS,
(ii) vytvoření systému hlášení kybernetických bezpečnostních incidentů a předávání informací mezi hlavními subjekty kybernetické bezpečnosti v České republice a
(iii) zakotvení pravomocí NBÚ v oblasti kybernetické bezpečnosti, včetně možnosti vydávat opatření v reakci na určité kybernetické bezpečnostní incidenty. Zákon zároveň zakotvuje činnost Vládního CERT a Národního CERT.

2.2. Vyhláška č. 316/2014 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti

Vyhláška č. 316/2014 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti je prováděcím právním předpisem zaměřeným zejména na konkrétní povinnosti vyplývající ze ZKB. V rámci vyhlášky jsou zejména stanovena konkrétní technická a organizační bezpečnostní opatření, která mají být zavedena u subjektů KII a VIS.

Návrh vyhlášky byl podroben dvoukolovému připomínkovému řízení s cílem dosáhnout co možná nejširší diskuse o navržené právní úpravě a její optimalizace v dopadech na veřejnoprávní a soukromoprávní subjekty v České republice.

Dne 21. února 2014 byl návrh zveřejněn na internetových stránkách NBÚ s výzvou k jejímu připomínkování odbornou veřejností. Úřad obdržel cca 300 připomínek, které byly jednotlivě vypořádány na veřejném jednání dne 11. dubna 2014. Po zapracování vypořádaných připomínek, byl dále návrh postoupen do meziresortního připomínkového řízení, které bylo ukončeno dne 21. srpna 2014. Připomínky byly opět jednotlivě vypořádány na jednání dne 18. září 2014.

Po zapracování vypořádaných připomínek byl návrh vyhlášky zaslán do Legislativní rady vlády. Dne 24. listopadu 2014 byl návrh vyhlášky projednán v Pracovní komisi Legislativní rady vlády pro správní právo. Připomínky nebyly zásadního charakteru, přičemž převážná část byla legislativně technická.

2.3. Vyhláška č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích

Vyhláška č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích, byla připravována společně MV a NBÚ. Návrh vyhlášky byl vypracován v první polovině roku 2014 a po vypořádání vzájemných připomínek obou resortů byl v září 2014 návrh odeslán do meziresortního připomínkového řízení. V tomto řízení obdržely předkládající resorty připomínky z 26 připomínkových míst. Řešeny byly zejména připomínky k uvedení některých systémů do přílohy č. 1 vyhlášky, ve které jsou stanoveny VIS, popřípadě se zaměřovaly na rozsah stanovení určujících kritérií a jiné legislativně-technické aspekty vyhlášky. Připomínky byly jednotlivě vypořádány na jednáních ve dnech 6. a 7. listopadu 2014. Dne 20. listopadu 2014 byla vyhláška postoupena Pracovní komisi Legislativní rady vlády pro správní právo k projednání. Obě vyhlášky byly dne 15. prosince 2014 schváleny a nabyly účinnosti dnem 1. ledna 2015.

2.4. Nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury

NBÚ se podílel také na tvorbě nařízení vlády č.315/2014 Sb., kterým se mění nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury, konkrétně na stanovení odvětvových kritérií pro určení prvku kritické infrastruktury v oblasti kybernetické bezpečnosti. Tato odvětvová kritéria konkrétně stanovují, které informační či komunikační systémy mohou při splnění průřezových kritérií být určeny za KII. Vypracování návrhu této novely bylo v gesci MV. Novela nařízení nabyla účinnosti také dne 1. ledna 2015.

3. TVORBA KONCEPČNÍCH DOKUMENTŮ KYBERNETICKÉ BEZPEČNOSTNÍ POLITIKY ČESKÉ REPUBLIKY

Zásadními počiny při tvorbě koncepčních dokumentů kybernetické bezpečnostní politiky České republiky bylo zejména vytváření nové národní strategie kybernetické bezpečnosti České republiky a navazujícího akčního plánu, který dotčenou strategii dále rozpracovává a konkretizuje jednotlivé úkoly pro odpovědné subjekty. Na základě podnětu NBÚ došlo k aktualizaci Bezpečnostní strategie České republiky tak, aby reflektovala změny bezpečnostního paradigmatu v blízkém pohraničí, posilování role nestátních aktérů a změnu hrozeb včetně těch kybernetických. V neposlední řadě také NBÚ plnil roli gestora kybernetické bezpečnosti poskytováním stanovisek a komentářů k dalším návrhům politik, které se kybernetické bezpečnosti dotýkají, popřípadě připomínkováním legislativy, která by mohla mít dopady na oblast kybernetické bezpečnosti.

3.1. Aktualizace Bezpečnostní strategie České republiky

V souvislosti se vzrůstajícím počtem kybernetických útoků a zvyšující se závislostí společnosti na informačních a komunikačních technologiích roste také hrozba narušení bezpečnostních zájmů České republiky. Z tohoto důvodu byla po dohodě s ostatními partnery a státními institucemi otevřena debata nad aktualizací Bezpečnostní strategie České republiky. NBÚ jako gestor kybernetické bezpečnosti navrhl doplnění příslušných pasáží reflektující současné změny v bezpečnostním prostředí a zdůrazňující potřebnost vytvoření pevného systému kybernetické bezpečnosti. Bezpečnostní strategie České republiky byla dne 21. listopadu 2014 projednána ve Výboru pro koordinaci zahraniční a bezpečnostní politiky Bezpečnostní rady státu a Bezpečnostní radou státu byla schválena dne 22. prosince 2014.

3.2. Národní strategie kybernetické bezpečnosti České republiky a Akční plán

V roce 2011 navázal NBÚ na svého předchůdce (MV) a drobnými úpravami aktualizoval tehdejší strategii kybernetické bezpečnosti. Výsledkem těchto úprav byla Strategie pro oblast kybernetické bezpečnosti České republiky na období 2012 – 2015. Od té doby se podařilo dosáhnout mimo jiné i dvou důležitých milníků, které byly v této strategii stanoveny, a to:

- přijetí Zákona o kybernetické bezpečnosti
- otevření Národního centra kybernetické bezpečnosti, jehož součástí je i plně funkční GovCERT.CZ pro zvládání kybernetických bezpečnostních incidentů.

Ostatní cíle stanovené v dané strategii bylo také možné považovat za splněné či průběžně naplňované, proto bylo rozhodnuto o vytvoření nové strategie kybernetické bezpečnosti v dřívějším termínu.[2]

S blížícím se ukončením platnosti této strategie a splněním v ní stanovených zásadních cílů a úkolů tak začal v roce 2013 NBÚ v souladu se svou úlohou národní autority v oblasti kybernetické bezpečnosti vytvářet ve spolupráci se svými partnery zcela novou Národní strategii kybernetické bezpečnosti na období let 2015 až 2020 (dále „Strategie“). Návrh prošel meziresortním připomínkovým řízením v průběhu srpna a září 2014. Veškeré tyto připomínky byly úspěšně vypořádány a Strategie byla dne 22. prosince 2014 schválena Bezpečnostní radou státu. Tato nová Strategie představuje pro Českou republiku zásadní předěl ve vnímání kybernetické bezpečnosti. Oproti minulé strategii se totiž kvalitativně přesouvá od budování základních kapacit nezbytných pro zajištění základní míry kybernetické bezpečnosti směrem k jejímu dalšímu hlubšímu a pokročilému zajišťování.

Z hlediska struktury a členění textu je ve Strategii nejprve představena vize České republiky pro oblast kybernetické bezpečnosti přesahující časový rámec Strategie (2015 – 2020) a následně jsou definovány základní principy, které stát následuje při zajišťování kybernetické bezpečnosti v České republice. Na tuto první obecnější část pak navazuje kapitola o konkrétních výzvách na poli kybernetické bezpečnosti jak pro Českou republiku, tak i pro mezinárodní prostředí, v jehož rámci se Česká republika nachází.

---

[2] Vyhodnocení Národní strategie kybernetické bezpečnosti pro období let 2012 až 2015 je dostupné na webu Národního centra kybernetické bezpečnosti.
Odkaz: http://www.govcert.cz/cs/informacni-servis/strategie-a-akcni-plan/

Závěrem jsou představeny hlavní strategické cíle, aby bylo možné těmto výzvám čelit:

A. Zajištění efektivity a posilování všech struktur, procesů a spolupráce.
B. Aktivní mezinárodní spolupráce.
C. Zajištění ochrany národní KII a VIS.
D. Spolupráce se soukromým sektorem.
E. Výzkum a vývoj / Budování spotřebitelské důvěry.
F. Podpora vzdělávání, osvěty a rozvoje informační společnosti.
G. Podpora rozvoje schopností Policie České republiky vyšetřovat a postihovat informační kriminalitu.
H. Další rozvoj právní úpravy pro oblast kybernetické bezpečnosti (vytváření právního rámce) - harmonizace s mezinárodní právní úpravou a účast na vývoji evropské a mezinárodní legislativy.

Z těchto cílů vychází i konkrétní Akční plán kybernetické bezpečnosti České republiky na období let 2015 až 2020 (dále „Akční plán“), který bude definovat konkrétní úkoly, stanoví u nich zodpovědnost, termíny jejich plnění a kontrolu. V době přípravy této Zprávy již probíhaly konzultace s partnerskými resorty, institucemi a odbornou veřejností ohledně finální podoby Akčního plánu, jehož přijetí vládou je plánováno na druhé čtvrtletí roku 2015.

Po přijetí Akčního plánu budou NBÚ a jeho specializované pracoviště NCKB průběžně sledovat, diskutovat a hodnotit plnění jednotlivých cílů ve spolupráci s ostatními zainteresovanými subjekty. O stavu naplňování Akčního plánu bude vláda České republiky informována prostřednictvím zpráv o stavu kybernetické bezpečnosti v České republice.

4. INFORMAČNÍ SYSTÉMY DŮLEŽITÉ PRO STÁT A NAVAZÁNÍ KOMUNIKACE SE SUBJEKTY PROVOZUJÍCÍMI KII A VIS

V roce 2014 bylo dokončeno mapování informačních a komunikačních systémů důležitých pro stát, a to jak u veřejnoprávních, tak soukromoprávních subjektů. Mapování sloužilo zejména jako podklad pro tvorbu legislativy kybernetické bezpečnosti, přičemž jeho výsledky v posledních fázích posloužily k řádnému vymezení určujících kritérií KII a VIS. V rámci celého mapování bylo osloveno více než 90 subjektů a identifikováno více než 800 informačních systémů, které byly dále hodnoceny z hlediska důležitosti pro chod státu.

V rámci mapování byly započaty také bezpečnostní projekty s některými subjekty, které měly za cíl zlepšit úroveň zabezpečení daných informačních systémů. Tyto projekty probíhaly i v průběhu roku 2014.

Na základě výsledků provedeného mapování započala komunikace se subjekty, které by se měly stát správci KII nebo VIS dle ZKB. Cílem této komunikace je zejména vymezení činností daných subjektů a jejich jednotlivých informačních systémů k případnému určení jako součásti KII, popřípadě jako VIS, a příprava na plnění povinností dle ZKB.

Značné úsilí bylo také věnováno poskytování informací o dopadech přijaté právní úpravy včetně důsledků, které bude standardizovaná spolupráce v oblasti kybernetické bezpečnosti přinášet. Za tím účelem členové NCKB organizovali a aktivně se účastnili konferencí k ZKB a prováděcím právním předpisům, konferencí ke kybernetické bezpečnosti, odborných seminářů apod.[3] V neposlední řadě byla tato osvěta prováděna i vzájemnými jednáními s mnoha jednotlivými subjekty, které spravují informační nebo komunikační technologie důležité pro stát.

[3] Viz kapitola 7.

5. MEZINÁRODNÍ SPOLUPRÁCE

Stejně jako tomu bylo v předchozích letech, i v roce 2014 pokračoval NBÚ v navazování a budování bilaterální a multilaterální mezinárodní spolupráce.

5.1. Evropská unie

Hlavním tématem pro NBÚ na evropské úrovni byla i v roce 2014 bezpečnost sítí a informací. Směrnice o bezpečnosti sítí a informací[4] (dále „Směrnice NIS“) byla Evropskou komisí představena dne 7. února 2013 v souvislosti se společným sdělením Evropské komise a vysoké představitelky Evropské unie (dále „EU“) pro zahraniční věci a bezpečnostní politiku o evropské strategii pro kybernetickou bezpečnost.

NBÚ od počátku aktivně vysílá své experty na jednání na půdě Rady EU, která probíhají v rámci Pracovní skupiny pro telekomunikace a informační společnost. Tato směrnice byla v roce 2014 intenzivně projednávána, jejího dokončení však nebylo dosaženo, a proto byla další jednání přesunuta na rok 2015. Za tímto účelem byly od poloviny října 2014 zahájeny rovněž tzv. neformální trialogy s Evropským parlamentem, jejichž cílem je sjednotit stanovisko Evropského parlamentu a Rady EU[5]. Cílem NBÚ je prosazení pozice České republiky, která se soustředí zejména na ochranu KII a zabránění významnému rozšiřování oblasti působnosti Směrnice NIS na soukromoprávní subjekty.

Za účelem zpracovávání instrukcí na jednání výše zmíněné pracovní skupiny byla na konci roku 2013 rovněž zřízena resortní koordinační skupina NBÚ, která umožňuje spolupráci NBÚ s dalšími relevantními resorty. Tato resortní koordinační skupina byla aktivně využívána k projednávání Směrnice NIS, stejně jako k projednávání dalších dokumentů a předpisů v rámci EU. Tím tak přispěla k nastavení komunikačních kanálů mezi NBÚ a dalšími orgány státní správy.

[4] Návrh směrnice Evropského parlamentu a Rady o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informací v Unii.

[5] Evropský parlament přijal své stanovisko v 1. čtení dne 13. března 2014. Rada EU se dosud neshodla na společném stanovisku k tomuto čtení.

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

Úlohou Evropské agentury pro bezpečnost sítí a informací (dále „ENISA“) je poskytovat poradenství Evropské komisi a členským státům EU při tvorbě a implementaci politik týkajících se kybernetické bezpečnosti, koordinovat opatření vydávaná pro zabezpečení jejich sítí a informačních systémů, prostřednictvím poskytování kurzů a školení podporovat budování kapacit CERT v jednotlivých členských státech a provozovat celosvětovou databázi národních strategií kybernetické bezpečnosti. V neposlední řadě je ENISA organizátorem jednoho z největších celoevropských cvičení v oblasti kybernetické bezpečnosti Cyber Europe[6].

Česká republika má v ENISA své zastoupení formou účasti na pořádaných formálních a neformálních jednáních. Dva zástupci NBÚ jsou členy představenstva ENISA[7], kde jsou zodpovědní za schvalování programu a plánu prací a rozpočtu ENISA. Na podzim roku 2014 byl pracovník NCKB osloven, aby se stal členem užší pracovní skupiny ENISA vytvořené na podporu tvorby a implementace národních strategií kybernetické bezpečnosti. Přizvaný zástupce se tak bude od příštího roku ve spolupráci s dalšími odborníky podílet na konzultacích a přípravě metodických a podpůrných materiálů pro tvorbu strategických dokumentů.

Česká republika aktivně využívá podpory ENISA při budování svých kapacit a aktivně s agenturou spolupracuje. Kromě účasti na zmíněném cvičení kybernetické bezpečnosti Cyber Europe se zástupci českého týmu GovCERT.CZ spolu se zástupci Policie České republiky (dále „PČR“) zúčastnili kurzu ENISA konaného v sídle NCKB ohledně zvládání kybernetických útoků mířených na KII a zvládání kybernetických bezpečnostních incidentů cílených na mobilní zařízení.

5.3. Severoatlantická aliance (NATO)

Ředitel NBÚ podepsal dne 14. března 2012 Memorandum o porozumění (Memorandum of Understanding) s NATO ve věci kybernetické obrany. S ohledem na měnící se bezpečnostní paradigma započala v roce 2014 práce na sjednoceném znění tohoto Memoranda, které upravuje podmínky spolupráce v rámci alianční kybernetické obrany.

[6] Viz příloha č. 1
[7] Jedná se o pozice Management Board Member a Alternate Management Board Member.

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

Otázky kybernetické bezpečnosti jsou diskutovány také na půdě Organizace pro bezpečnost a spolupráci v Evropě (dále „OBSE“). Konkrétně se členské státy OBSE rozhodnutím Stálé rady č. 1039 ze dne 26. dubna 2012 rozhodly posílit úsilí při řešení bezpečnosti a využívání informačních a komunikačních technologií, a to v souladu se všemi závazky OBSE a ve spolupráci s příslušnými mezinárodními organizacemi. Došlo proto k vypracování prvního souboru opatření pro budování důvěry v kyberprostoru (tzv. Confidence Building Measures, dále „CBMs“), která mají za cíl vést k posílení mezistátní spolupráce, navýšení transparentnosti, předvídatelnosti a stability v kyberprostoru a ke snižování rizika nedorozumění, eskalace a vzniku konfliktu, který by mohl pramenit z využívání informačních a komunikačních technologií.

Česká republika podporuje proces vytváření kybernetických CBMs jako předpoklad pro formalizaci vztahů mezi státy, a to zejména prostřednictvím aktivní implementace první sady kybernetických CBMs a účast v diskuzi ohledně druhé sady těchto opatření. S ohledem na kooperativní charakter druhé sady CBMs Česká republika preferuje opatření na dobrovolné bázi založené na společné důvěře a spolupráci mezi státy.

Česká republika jako jedna z prvních zemí v OBSE již sdílí prostřednictvím systému POLIS OSCE relevantní informace ke všem jednotlivým kybernetickým CBMs a pravidelně je aktualizuje. Zástupce NBÚ (tzv. expert z ústředí) vystoupil s příspěvkem na dvou ze tří jednání Informal Working group 1039 k implementaci kybernetických CBMs, kde prezentoval jak současný stav implementace kybernetických CBMs v České republice, tak i stav kybernetické bezpečnosti v České republice spolu s relevantními dokumenty vztahujícími se k strategickému, legislativnímu a organizačnímu rámci kybernetické bezpečnosti.

5.5. Central European Cyber Security Platform (CECSP)

Česká republika dosáhla významného úspěchu v oblasti na zvyšování zabezpečení a odolnosti KII prostřednictvím regionální spolupráce mezi pracovišti CERT, když byla z její a rakouské iniciativy založena v květnu 2013 Středoevropská platforma kybernetické bezpečnosti (Central European Cyber Security Platform, dále „CECSP“).

Za rakouského předsednictví se v dubnu 2014 uskutečnilo již třetí zasedání na strategické úrovni, kde se hodnotil pokrok v dosavadní spolupráci na poli kybernetické bezpečnosti. Prioritou tohoto jednání bylo i přijetí pracovního programu CECSP pro období nadcházejících tří let a dohody o pravidlech a principech spolupráce v rámci této platformy. V prosinci 2014 se pak uskutečnilo jednání CECSP na technické úrovni a Maďarsku bylo předáno předsednictví na rok 2015. V rámci tohoto zatím posledního zasedání byl zřízen tzv. mailing list[8], zajištěn přístup k společnému úložišti dokumentů a rozpracován tzv. „CECSP contact list“. Zároveň byla potvrzena snaha o hledání společných pozic ke kybernetickým otázkám a diskutovaly se výsledky a přínos prvního společného kybernetického cvičení, které pod vedením Maďarska proběhlo v červnu 2014. V neposlední řadě byl diskutován charakter a termín příštího cvičení CECSP[9].

5.6. Bilaterální a další spolupráce

V červnu navázal NBÚ spolupráci s příslušným italským úřadem Dipartimento delle Informazioni per la Sicurezza, v říjnu s EC3 Unit Europolu a dále v listopadu s rumunským národním dohledovým pracovištěm CERT-RO. V roce 2014 byla rovněž prohlubována spolupráce se stávajícími partnerskými úřady, zejména ze Slovenska, Rakouska, Maďarska, Polska, Německa, Francie, Jižní Koreje, Spojených států a Izraele. Například se slovenským CSIRT.SK došlo k vzájemné výměně bezpečnostních nástrojů vyvíjených jednotlivými týmy.

V případě Spojených států se posílila spolupráce s Department of Homeland Security, jenž NBÚ nabídnul přístup do svého neveřejného portálu a dále možnost účastnit se školení v oblasti průmyslových řídicích systémů. Posílila se i spolupráce s americkým Federálním úřadem pro vyšetřování (Federal Bureau of Investigation), který připravil pro pracovníky NBÚ školení.

Kybernetická bezpečnost se stala jedním z bodů jednání během společného zasedání vlád České republiky a Izraele, které se uskutečnilo v listopadu v Jeruzalémě. Během těchto konzultací byla podepsána společná deklarace o spolupráci v oblasti kybernetické bezpečnosti, kterou za vládu České republiky podepsal náměstek ředitele NBÚ.

[8] Mailing list - sdílený seznam jmen a e-mailových adres na určené kontaktní osoby.
[9] Viz příloha č. 1

Spolupráce se týká:

- sdílení informací, osvědčených postupů a zkušeností týkajících se kybernetických bezpečnostních hrozeb a událostí, jakož i jiných relevantních otázek týkajících se kybernetické bezpečnosti,
- zvýšení celkové kybernetické odolnosti a připravenosti čelit internetovým hrozbám prostřednictvím sdílení informací, výměny zkušeností a spolupráce v odborné přípravě včetně společných kybernetických bezpečnostních cvičení,
- sdílení relevantních informací o projektech výzkumu a vývoje v oblasti kybernetické bezpečnosti,
- vytvoření zabezpečeného komunikačního kanálu za účelem sdílení informací týkajících se kybernetických bezpečnostních hrozeb a událostí[10].

Spolupráce v oblasti kybernetické bezpečnosti byla také předmětem jednání ředitele NBÚ Dušana Navrátila s komisařkou EU pro digitální agendu Neelie Kroes, ministrem britské vlády Francisem Maudem a koordinátorem amerického Department of State Christopherem Painterem.

V rámci spolupráce mezi Českou republikou a NATO Cooperative Cyber Defence Centre of Excellence (dále „CCDCOE"), jehož posláním je přispívat ke zvyšování kybernetické obrany a zlepšovat spolupráci a sdílení informací mezi účastnickými státy a NATO, vyslal NBÚ v lednu 2014 jednoho pracovníka do právní a politické divize CCDCOE jako tzv. voluntary national contribution.

Později se v květnu, resp. červnu 2014 Česká republika prostřednictvím NBÚ oficiálně připojila k činnosti CCDCOE podepsáním tzv. Notices of Joining. Zapojením do činnosti této instituce sídlící v estonském Tallinnu je České republice umožněno podílet se na výzkumných a vzdělávacích projektech CCDCOE a těžit z jejich výsledků. Příkladem za všechny může být bezplatné školení expertů, kterých se v roce 2014 zúčastnilo celkem 6 pracovníků GovCERT.CZ. Školení bylo zaměřeno na analýzu malware, bezpečnostní monitoring, forenzní činnost a analýzu pokročilých síťových hrozeb.

[10] Odkaz: http://www.govcert.cz/cs/informacni-servis/akce-a-udalosti/cr-a-izrael-podepsaly-prohlaseni-o-spolupraci-v-oblasti-kyberneticke-bezpecnosti/.

Vedle toho se dva pracovníci OTPVV účastnili týdenního kurzu zabývajícího se aplikací mezinárodního práva v oblasti kybernetické bezpečnosti.

5.7. Trusted Introducer

V srpnu 2014 se GovCERT.CZ stal akreditovaným členem evropského sdružení Trusted Introducer[11] (dále „TI“). Toto sdružení působí v rámci evropské organizace TERENA a sdružuje evropské bezpečnostní týmy vládní, národní, komerční sféry (např. bank, provozovatelů internetového připojení, výrobců hardware atd.) nebo univerzit. Vstup GovCERT.CZ mezi akreditované týmy TI znamená další krok k užší spolupráci se světovou infrastrukturou bezpečnostních týmů CERT nebo CSIRT a zvýšení prestiže na mezinárodní scéně. Jedná se o placené členství, z něhož mj. vyplývá přístup na uzavřená jednání TF-CSIRT (Task Force), k uzavřenému a šifrovanému mailing listu a k celé řadě informací a kontaktů v partnerských evropských zemích. Za další výhody tohoto členství lze považovat tzv. out-of-band varování[12] v případě závažnějšího či globálního problému, vstup na odborné fórum a obecně serióznější přístup ze strany ostatních týmů.

Pracovníci NCKB se zúčastnili také řady zahraničních konferencí a školení[13].

5.8. Účast na mezinárodních kybernetických cvičeních

NBÚ se během roku 2014 zúčastnil celkem šesti cvičení - Cyber Europe, Locked Shields, CECSP 2014 Exercise, Cyber Czech[14], EU-Multi Layer a Cyber Coalition. Měl se zúčastnit i cvičení Crisis Management Exercise 2014, které však bylo na základě rozhodnutí Severoatlantické rady NATO přesunuto na rok 2015. Česká republika pravidelně dosahuje velmi nadprůměrných výsledků v rámci těchto cvičení. Bližší informace o konkrétních cvičeních jsou součástí přílohy této Zprávy.

[11] Odkaz: http://www.govcert.cz/cs/informacni-servis/akce-a-udalosti/govcertcz-se-stal-akreditovanym-clenem-evropskeho-sdruzeni-trusted-introducer/.
[12] Způsob výměny informací mezi členy prostřednictvím systémů nezávislých na internetu, např. použitím klasických telefonních linek či mobilní komunikace.
[13] Viz kapitola 7.2.
[14] Viz kapitola 6.7.

6. NÁRODNÍ SPOLUPRÁCE

Pro zajišťování kybernetické bezpečnosti je důležitá i široká spolupráce na národní úrovni, přičemž slovo národní zde zahrnuje aktivní kooperaci mezi veřejnou a soukromou sférou a s občanskou společností.

6.1. Bezpečnostní tým CSIRT.CZ/CZ.NIC

V roce 2014 pokračovala spolupráce mezi bezpečnostním týmem CSIRT.CZ a GovCERT.CZ, která z původní konzultační roviny přešla do roviny praktického řešení kybernetických incidentů. CSIRT.CZ nejenže spolupracoval na řešení útoků na informační infrastrukturu, ale současně se podílel na konzultacích k zákonu o kybernetické bezpečnosti a prováděcím právním předpisům. GovCERT.CZ se rovněž v součinnosti s laboratořemi CZ.NIC zapojil do skenování českých webů na zranitelnost HeartBleed. Spolupráce se osvědčila i v rámci letošního cvičení Cyber Europe, kde oba týmy společně řešily množství technických úkolů. Nelze nezmínit také první národní kybernetické cvičení[15] pořádané NBÚ, na jehož scénářích se významnou měrou podíleli právě pracovníci CSIRT.CZ.

6.2. Bezpečnostní týmy CSIRT

Mezi další CSIRT týmy, se kterými GovCERT.CZ udržuje úzké vztahy, patří CSIRT Masarykovy univerzity (dále „CSIRT-MU“). Ten se řadí ke špičkovým pracovištím evropského formátu. Spolupráce s CSIRT-MU probíhá převážně v technické oblasti. Teoretická podpora je stejně jako v loňském roce doplněna stážemi v CSIRT-MU. Tu v roce 2014 absolvovali dva zaměstnanci GovCERT.CZ. Neméně zajímavé je i zapojení členů GovCERT.CZ do projektu Kybernetický polygon, jež se zabývá výzkumem, vývojem a sestavením unikátního prostředí pro analýzu hrozeb ohrožujících bezpečnost KII a výzkum a vývoj metod ochrany KII proti kybernetickým útokům či projektu Czech Cyber Crime Centre of Excellence, jehož cílem je vytvořit kvalitní centrum pro školení a vzdělávání v oblasti prevence a represe kybernetické kriminality.

6.3. Policie České republiky a zpravodajské služby

Relevantními partnery v oblasti řešení kybernetických bezpečnostních incidentů jsou také zpravodajské služby a PČR. Měřitelem této spolupráce je především výměna

[15] Viz kapitola 6.7.

informací o aktuálních či řešených kybernetických bezpečnostních incidentech, zkušeností s jejich zvládáním a vzájemného know-how.

Jedním z významných počinů PČR v roce 2014 bylo rozhodnutí policejního prezidenta zřídit specializovaný celorepublikový útvar pro boj s informační kriminalitou. NBÚ tento krok podporuje a přislíbil pomoc se zřízením tohoto nového útvaru a další spolupráci při budování schopností PČR pro boj s informační kriminalitou.

Vzájemné vztahy prohlubují také kybernetická cvičení, kterých se zástupci PČR i zpravodajských služeb pravidelně účastní.

6.4. Ministerstvo obrany

GovCERT.CZ nadále úzce kooperuje s Centrem CIRC neboli hlavní složkou kybernetické bezpečnosti Ministerstva obrany (dále „MO“) České republiky. Kromě výměny informací a sdílení zkušeností a informací o kybernetických bezpečnostních incidentech se společně účastní také kybernetických cvičení, především cvičení Cyber Coalition, kde jsou v rámci společné reprezentace České republiky v NATO partnery při řešení scénářů[16].

Na základě zkušeností získaných při komunikaci a koordinaci činnosti obou zmíněných týmů se v roce 2014 začalo připravovat Prováděcí ujednání o vzájemné podpoře v oblasti kybernetické bezpečnosti a kybernetické obrany mezi NBÚ a MO, které zajistí rychlou a operativní spolupráci technických týmů při řešení kybernetických bezpečnostních událostí a incidentů.

Spolupráce mezi NBÚ a MO je nastavena také v rovině strategické. NBÚ z pozice národní autority kybernetické bezpečnosti projednává s MO technické, právní a koncepční možnosti kybernetické obrany a diskutuje o možnostech budování kybernetických kapacit Armády České republiky.

6.5. Akademická sféra

NBÚ/NCKB dříve navázal a nadále udržuje vztahy s akademickou sférou v České republice formou smluv o spolupráci. Ke konci roku 2014 byly podepsány smlouvy s následujícími akademickými institucemi: Masarykova univerzita, Vysoké učení technické v Brně, Univerzita obrany, České vysoké učení technické v Praze, Univerzita Palackého v Olomouci a Vysoká škola CEVRO Institut.

[16] Viz příloha č. 1

Úzká spolupráce probíhá zejména s Masarykovou univerzitou v Brně. Dle ujednání v roce 2014 se budou pracovníci NCKB podílet na přednáškové činnosti Fakulty sociálních studií v rámci oboru Bezpečnostní a strategická studia. Se studenty budou také konzultovat jejich diplomové práce dotýkající se tématu kybernetické bezpečnosti.

V roce 2014 se rovněž NBÚ dohodl s Univerzitou Palackého v Olomouci na zapojení do přípravy a následné výuky v celouniverzitním předmětu, jenž má sloužit jako úvod do kybernetické bezpečnosti. Za tímto účelem měli na podzim roku 2014 pracovníci NCKB možnost podílet se na tvorbě kompletního sylabu přednášek.

6.6. Další partneři

Klíčovým partnerem pro NCKB, a to zejména v oblasti analýzy botnetů a poskytování informací o IP adresách a napadených počítačích malware, je společnost Microsoft. NCKB od společnosti získává unikátní data, se kterými dále pracuje. Díky jejich analýze a vyhodnocování dochází ke zvyšování kybernetické bezpečnosti České republiky.

Prostřednictvím České bankovní asociace spolupracuje NCKB také s bankami, které mají zájem na zvyšování ochrany své počítačové infrastruktury. Právě banky se stávají častým terčem kybernetických útoků.

GovCERT.CZ také úzce kooperuje s členy tzv. Bezpečné VLAN, nyní FENIX. Tento projekt by měl v budoucnu výrazně mírnit následky masivních DDoS útoků obdobných těm, jaké Česká republika zaznamenala v březnu 2013. Projekt je zaštítěn národním internetovým uzlem NIX.CZ a v současné době jsou do něj zapojeny významné telekomunikační společnosti.

Mimo zmíněných partnerů na národní úrovni NCKB aktivně spolupracuje s Asociací krajů České republiky, Krajem Vysočina, AFCEA a Národním centrem pro bezpečnější internet[17].

[17] Viz kapitola 7.

6.7. Národní cvičení CYBER CZECH 2014

V měsíci říjnu uspořádalo NCKB první národní cvičení v oblasti kybernetické bezpečnosti CYBER CZECH 2014. Jednalo se o netechnické, tzv. table-top[18] cvičení, jehož záměrem bylo formou skupinové diskuze procvičit schopnost spolupráce při zvládání kybernetických bezpečnostních incidentů a ověřit komunikační kanály, které se při řešení používají. Celodenního cvičení se zúčastnili zástupci ministerstev dopravy, financí, obrany, průmyslu a obchodu, vnitra, zahraničních věcí, práce a sociálních věcí, spravedlnosti, životního prostředí, školství, mládeže a tělovýchovy, dále Úřadu na ochranu osobních údajů, Českého telekomunikačního úřadu, České národní banky, Úřadu vlády a Správy základních registrů. V rámci dvou simulovaných scénářů byli všichni sezvaní cvičící coby bezpečnostní ředitelé a manažeři bezpečnosti informačních technologií fiktivního ministerstva vystaveni otázkám, jak by postupovali v případě rozsáhlých DDoS útoků namířených na webové stránky tohoto ministerstva a cílených phishingových zpráv zaslaných jeho zaměstnancům.

Skupinu šestnácti cvičících doplňovala dvanáctičlenná odborná porota, v níž usedli zástupci bezpečnostního týmu CSIRT.CZ, CSIRT-MU, poskytovatele internetových služeb ACTIVE 24, Nejvyššího státního zastupitelství, PČR, zpravodajských služeb, dále odborníci na právo informačních a komunikačních technologií z Masarykovy univerzity a zástupci NBÚ. Jejich úkolem bylo hodnotit a doplňovat návrhy a odpovědi cvičících.

Cvičení bylo samotnými cvičícími i odbornou porotou hodnoceno kladně. Unikátnost celé akce spočívala ve skutečnosti, že se na jednom místě sešlo a společně diskutovalo velké množství odborníků s pracovníky, kteří řeší a zodpovídají za bezpečnost informačních a komunikačních technologií na svých pracovištích. Přínosnost takového cvičení se ukázala být ve všech ohledech značná, proto i v příštích letech bude NCKB v organizaci národních cvičení pokračovat.

[18] 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.

7. ZVYŠOVÁNÍ POVĚDOMÍ A OSVĚTA

NCKB stejně jako v předchozích letech v souladu se svým posláním informuje veřejnost o svém zaměření a činnostech. Mezi tyto aktivity spadá zejména přednášková a osvětová činnost, poskytování rozhovorů do médií či správa internetových stránek www.govcert.cz, na kterých je mimo jiné možné nalézt aktuální informace o kybernetických bezpečnostních incidentech a zranitelnostech, včetně doporučení k jejich řešení a zavedení preventivních opatřeních, dále informace o legislativě včetně ZKB a s ním souvisejících prováděcích právních předpisů, podpůrné materiály k procesu určování prvků KII a VIS aj. Pracovníci NCKB se rovněž aktivně účastní odborných konferencí, a to jak konaných v České republice, tak v zahraničí.

7.1. Konference u příležitosti otevření NCKB

Při příležitosti otevření NCKB v Brně uspořádal NBÚ ve dnech 13. a 14. května 2014 mezinárodní konferenci Kybernetická bezpečnost - výsledky a výzvy, kde jako hlavní řečníci vystoupili mimo jiné Sorin Ducaru (náměstek generálního tajemníka NATO pro nové bezpečnosti hrozby), Freddy Dezeure (ředitel CERT-EU), Udo Helmbrecht (generální ředitel ENISA), Melissa Hathaway (bývalá poradkyně amerického prezidenta George W. Bushe pro otázky kybernetické bezpečnosti) či Paul Schneider (bývalý náměstek ředitele amerického Department of Homeland Security).

7.2. Vzdělávací a osvětové kampaně a konference

Úlohou NCKB je kromě koordinace spolupráce na národní a mezinárodní úrovni za účelem předcházení a řešení kybernetických bezpečnostních incidentů také osvěta a podpora vzdělávání v oblasti kybernetické bezpečnosti.

Významným partnerem NBÚ pro oblast vzdělávání se v roce 2014 stal Kraj Vysočina. Ten se zapojil do projektu Kraje pro bezpečný internet[19] a v rámci osvěty v oblasti kybernetické bezpečnosti pořádá přednášky, školí studenty, rodiče, pedagogy i příslušníky PČR. Pracovníci NCKB se zúčastnili několika ze zmíněných přednášek. NCKB bylo rovněž přizváno k závěrečnému vyhodnocení projektu i-Bezpečná škola, který vede krajské školské zařízení pro vzdělávání pedagogů Vysočina education. Zmíněný projekt vnímá NBÚ jako pilotní a do budoucna by spolupráci rád rozšířil o další kraje.

[19] Projekt je pořádán Národním centrem pro bezpečnější internet.

Další osvětové aktivity zaměřuje NCKB na zaměstnance státní správy. Příkladem jsou přednášky na MV, MO a NATO Allied Command Transformation Cyber Syndicate, kde pracovníci NCKB prezentovali problematiku kybernetické bezpečnosti z hlediska mezinárodní spolupráce, Národní strategii kybernetické bezpečnosti na období let 2015 až 2020 a profil NCKB coby gestora kybernetické bezpečnosti v České republice. V neposlední řadě proběhl v listopadu seminář k nové strategii kybernetické bezpečnosti České republiky a ochraně KII i na půdě Poslanecké sněmovny České republiky.

Jak již bylo zmíněno, zaměstnanci NCKB se také často v pozici prezentujících účastní zahraničních konferencí, školení, workshopů a přednášek. Namátkou může být uvedena konference Meridian Process 2014, jež se konala v listopadu v Japonsku, kam byl pozván pracovník NCKB, aby představil proces mapování KII v České republice a seznámil mezinárodní publikum s českým konceptem zabezpečení kybernetického prostředí včetně způsobu určování KII. Dále lze zmínit přednášku, se kterou zástupce NCKB vystoupil na konferenci nezávislé neziskové mezinárodní asociace ICS ISAC (Industrial Control Systems Conference) či přednášky na témata kybernetická bezpečnost a národní strategie, se kterými se pracovníci NCKB prezentovali v německém George C. Marshall European Center for Security Studies. V měsíci listopadu pracovníci GovCERT.CZ spoluorganizovali workshop v rámci evropského projektu Enhancing Cyber Security pro Makedonii, Kosovo a Moldavsko. Jeho cílem byla pomoc při budování národních a vládních CERT týmů v těchto zemích. Na tento workshop v Rumunsku navázalo technické školení v Praze zaměřené na obecné hrozby, budování CERT týmů a procesy zvládání kybernetických bezpečnostních incidentů, a dále workshop ve Francii, kde byly sdíleny zkušenosti z předchozích workshopů. V neposlední řadě lze zmínit účast pracovníků na panelových diskuzích a jejich přednášky na půdě ENISA.

Důvodem, proč právě v zahraničí jsou zástupci NCKB žádáni o přednášky s tematikou budování kapacit a systému kybernetické bezpečnosti, tvorby národní strategie či procesu mapování KII, je, že Česká republika patří k malé skupině států, které mají pokročilé zkušenosti s těmito procesy. Jedním z mnoha příkladů rostoucího zájmu o předávání zkušeností v této oblasti je návštěva ředitele NCKB v Jordánsku, kam byl osobně pozván a kde vedl přednášku pro jordánskou armádu.

Účast na mezinárodních konferencích a pomoc dalším státům při budování jejich kybernetických kapacit či systému zajištění kybernetické bezpečnosti staví Českou republiku do pozice váženého člena mezinárodního společenství v této oblasti.

To také přináší i další efekty, zejména ve formě získávání potřebných kontaktů se špičkami v oboru včetně navazování úzké spolupráce s nimi[20], zvýšený zájem o české experty v zahraničí nebo také získávání nejnovějších trendů, poznatků, metod a zajímavých informací a možnost jejich využití při zajišťování kybernetické bezpečnosti v České republice.

V rámci tuzemských konferencí lze zmínit přednášku na mezinárodním policejním kongresu Současné trendy v kyberkriminalitě v Ostravě nebo říjnovou IDG Konferenci, kde proběhla prezentace zkušeností s projektem Botnet Feeds. V měsíci říjnu se konala také třídenní mezinárodní konference Future Crisis, jedno z největších setkání národních i mezinárodních bezpečnostních složek se zástupci obranného průmyslu, kde opět vystoupili pracovníci NCKB s cílem seznámit posluchače s procesem určování KII. Soustavná spolupráce pokračovala s organizací AFCEA a s Policejní akademií České republiky. V měsíci listopadu se naši pracovníci zúčastnili a prezentovali činnost GovCERT.CZ na 1. setkání CSIRT/CERT týmů působících v České republice, které se konalo v Praze. Na této konferenci se představilo všech 16 evidovaných (registrovaných) týmů a dva nově vznikající. V diskuzích byla nastíněna potřeba společné kooperace a podpory jak při řešení jednotlivých kybernetických bezpečnostních incidentů, tak při komunikaci a jednání s úřady a státní správou. Za zmínku stojí také účast na největší konferenci svého druhu ve střední Evropě WebExpo 2014 a prestižní konferenci pořádanou společností AEC poskytující software a služby pro bezpečnost dat s tématem Kybernetická bezpečnost z pohledu státu.

Kromě účasti na konferencích a seminářích národních i mezinárodních organizací navazuje NCKB kontakty s vysokými školami zabývajícími se tématy kybernetické bezpečnosti. NCKB si uvědomuje důležitost vzdělávání studentů, a proto se například v letošním roce někteří zaměstnanci zúčastnili kybernetické konference CyberCon, kterou pořádalo periodikum Global Politics ve spolupráci s webem Sekuriťáci.cz, obojí pod záštitou Fakulty sociálních studií Masarykovy univerzity v Brně. V rámci spolupráce s Univerzitou Palackého a Gymnáziem Jakuba Škody v Přerově byl proveden průzkum mapující úroveň znalostí středoškoláků v problematice kybernetické bezpečnosti, který navazoval na průzkum přímo vedený pracovníky NCKB mapující úroveň vzdělávání na ZŠ a SŠ v této oblasti a dostupnost relevantních vzdělávacích materiálů pro vyučující.

[20] Příkladem může být účast špičkových odborníků na konferenci Kybernetická bezpečnost – výsledky a výzvy uspořádané u příležitosti otevření NCKB v květnu 2014.

NCKB rovněž pracuje na interním vzdělávání svých zaměstnanců. Za tímto účelem plánuje komplexní a vysoce odborné dlouhodobé školení s cílem prohloubit jejich znalosti, aby mohli být i nadále rovnocennými partnery svým zahraničním kolegům.

7.3. Další přednášky a konference

V roce 2014 navázalo NCKB kontakty s několika institucemi zabývajícími se kybernetickou bezpečností. Jednou z aktivních neziskových organizací dlouhodobě se zabývající problematikou kybernetické bezpečnosti je Národní centrum pro bezpečnější internet (dále „NCBI“), jehož nejdůležitějším projektem je Saferinternet.cz, který usiluje o zvyšování povědomí o bezpečnějším užívání internetu. Právě s NCBI byla navázána spolupráce, v jejímž rámci se několik pracovníků NBÚ v čele s ředitelem NCKB jako hosté i jako účinkující zúčastnilo přednášek a workshopů pořádaných právě NCBI. V říjnu 2014 na žádost NCBI převzalo NCKB záštitu nad Evropským měsícem kybernetické bezpečnosti.

8. ČINNOST GOVCERT.CZ A SLEDOVÁNÍ SOUČASNÝCH TRENDŮ V KYBERNETICKÉ BEZPEČNOSTI

8.1. Činnost GovCERT.CZ za 2014

V roce 2014 proběhlo rozdělení činností GovCERT.CZ dle jednotlivých odborností. Zejména bylo potřebné se zaměřit na oblasti industriálních kontrolních systémů, penetračního testování, reverzního inženýrství, analýzy malware a v neposlední řadě i na forenzní činnosti, které jsou pro ochranu systémů státní správy a kritické informační infrastruktury stěžejní. Z důvodu prohlubování odborných znalostí v dané problematice se členové GovCERT.CZ v uplynulém roce účastnili řady mezinárodně uznávaných školení a odborných konferencí[21], z nichž se na některých i aktivně podíleli v roli přednášejících. V rámci nadnárodní spolupráce participovali na kybernetických cvičeních.

V souvislosti s hlavní náplní GovCERT.CZ, kterou bylo v roce 2014 řešení nahlášených incidentů a událostí ze státní a kritické infrastruktury, byla zprostředkovávána mezinárodní komunikace se zahraničními bezpečnostními týmy. Mimo zmíněné činnosti byla subjektům spadajícím do těchto uvedených oblastí nabízena a poskytována technická pomoc. Jednalo se zejména o forenzní a sítové analýzy a analýzy malware.

Jedním z velkých projektů, na který GovCERT.CZ v uplynulém roce navázal, byl rozvoj proaktivních činností a detekce anomálií. V této oblasti bylo dosaženo poměrně velkého posunu zejména díky nástroji BotNet Feed, který byl vytvořen a dále je vyvíjen pro potřeby GovCERT.CZ. Denně tento systém zpracovává přibližně 300 tisíc nových záznamů obsahující desítky tisíc unikátních českých IP adres, které jsou potenciálně nakažené malware. Součástí tohoto projektu bylo a stále je navázání a rozvíjení spolupráce se státními institucemi a bezpečnostními týmy působícími v rámci České republiky. Na základě obdržené zpětné vazby od spolupracujících institucí panuje široká shoda ohledně užitečnosti sdílení těchto informací.

V návaznosti na projekt BotNet Feed byly v uplynulém roce rozpracovány další projekty, jejichž účelem je hromadný sběr dat z veřejně dostupných zdrojů. Takovými zdroji jsou zejména mezinárodní výzkumné organizace, akademický sektor, veřejné

[21] Například Secure 2014, ICS Cyber Security, BRUCON, N4SICS a jiné.

honeypoty[22], systémy pro detekci průniků do sítě a gray a black listy, které mohou obsahovat seznamy IP adres používané pro šíření spamu nebo k dalším škodlivým aktivitám.

Nad takto získanými daty z různých zdrojů je následně prováděna podrobná a sofistikovaná analýza, jejíž součástí je i vzájemná korelace těchto dat. To je doplněno dalšími navazujícími procesy, jejichž účel je vytvářet ucelený obraz zpracovaných informací. Ty jsou následně předávány dál v rámci nastavené spolupráce s ministerstvy, státními organizacemi a komerčními subjekty. Přidanou hodnotou jsou pak i informace obsahující návod na lokalizaci a řešení potenciálně škodlivých událostí.

V rámci národní a mezinárodní komunity GovCERT.CZ přispívá sdílením svých vyvíjených a upravovaných open-source[23] nástrojů. V této oblasti je zejména zájem ze strany mezinárodních CERT týmů o sdílení nástroje BotNet Feed zpracovávajícího informace o botnetech.

Jedním z neméně důležitých prvků proaktivní činnosti je monitorování veřejných a uzavřených zdrojů se zaměřením na odhalování zranitelností potenciálně ohrožující subjekty v naší působnosti. Denně probíhá zpracování více než 300 takovýchto zpráv. Současně probíhá sběr a distribuce informací a analýz týkajících se aktuálních hrozeb postihujících Českou republiku. Takto nashromážděné informace jsou následně vyhodnocovány a dále distribuovány relevantním subjektům. Část těchto informací je zveřejňována na webu GovCERT.CZ formou vydávaných publikací.

V druhé polovině roku 2014 GovCERT.CZ začal s postupným nasazováním odladěných honeypotů a jejich začleňování do testovacího prostředí v laboratorní síti NCKB. Doprovodné procesy zahrnující úpravy konfigurací probíhaly a stále probíhají kontinuálně s ohledem na požadovanou funkcionalitu, reálnost stroje a další klíčové parametry. Cílem projektu je vybudování a následný rozvoj systému včasného varování.

Dalším plánem na rozšíření detekčních schopností je pořízení a následné nasazení síťových sond. To probíhá v součinnosti s dalšími státními institucemi, kterým by toto řešení umožnilo získat širší možnost monitoringu anomálií a škodlivého provozu v jejich sítích. Na tento projekt by GovCERT.CZ chtěl následně navázat nabídkou možností skenování zranitelností a penetračních testů. V současnosti jsou tyto testy prováděny na interních systémech NBÚ a NCKB.

---

[22] Honeypot slouží jako návnada lákající útočníka, přičemž po zachycení potenciálně nebezpečného software dochází k jeho automatizované analýze.

[23] 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.

Na pracovišti GovCERT.CZ vzniká pilotní projekt na oddělené laboratorní prostředí. Důvodem vzniku této laboratorní části je potřeba izolovaného prostoru pro analýzy potenciálně škodlivých dat získaných v rámci jednotlivých incidentů. Dále je toto prostředí využíváno pro účely vývoje vlastních aplikací, testování, ale i pro potřeby simulací systémů v průběhu různých cvičení. Ve spolupráci s odborníky PČR je zde také potenciál k vybudování vysoce kvalifikovaného znaleckého pracoviště, jehož zaměřením může být i forenzní analýza.

Mezi hlavní úkoly GovCERT.CZ patří tzv. koordinační činnost v rámci českých kybernetických bezpečnostních týmů zahrnující videokonferenci s možností okamžitého sdílení dat a informací pro případné řešení rozsáhlých kybernetických útoků. V uplynulém roce probíhala příprava podkladů umožňující vznik tohoto koordinačního centra a zapojení významných aktérů na poli kybernetické bezpečnosti v České republice.

8.2. Přehled nejvýznamnějších incidentů za rok 2014

Začátek roku 2014 byl relativně klidným obdobím doprovázeným pouze několika nejčastějšími typy útoků - DDoS útoky a phishingem – jež však svou intenzitou a průběhem nevybočovaly z dosavadních statistik. Jejich pachatelé útočili jak na subjekty soukromého tak i veřejného sektoru.

Závažnější útoky se odehrály v březnu 2014. Za zmínku stojí především tzv. Pony botnet, jak jej nazvala bezpečnostní společnost Trustwave. Ta vydala analýzu, uvádějící, že útočníci zprovoznili botnet za účelem krádeže přihlašovacích údajů k webovým stránkám, sociálním sítím, e-mailovým účtům a jiným službám. Podle zjištěných údajů byl tento botnet aktivní od září 2013 do ledna 2014. Ve zmíněném období se útočníkům podařilo odcizit více než 700 000 uživatelských pověření. Vyjma kompromitace uživatelských účtů se tento botnet zaměřil i na některé virtuální měny. Analýza získaných dat o útoku, kterou společnost Trustwave provedla, ukázala, že mezi postiženými doménami se nachází i větší zastoupení českých domén, cca 6 253 postižených domén „.cz“ a cca 53 292 přihlašovacích údajů. Na základě spolupráce a výměny informací mezi GovCERT.CZ, bezpečnostním týmem CSIRT.CZ a společnostní Trustwave došlo k informování kontaktních osob postižených domén a následnému řešení incidentu.

V návaznosti na šířící se informace o špionážním malware Turla (nebo také Uroburos, Snake či Carbon) probíhala v měsíci březnu komunikace mezi společností Symantec a GovCERT.CZ za účelem zjistit co nejvíce informací, především zda se mezi zasaženými objekty nenachází také systémy České republiky.

Analytici se v té době domnívali, že bylo nakaženo několik stovek počítačů ve více než 45 zemích po celém světě. Podle tehdejších dostupných informací se Turla v českých systémech neobjevila.

Další březnové útoky se svým charakterem příliš nelišily od těch ostatních. Stejně pak i v dubnu se jednalo především o phishingové kampaně zacílené např. na internetové bankovnictví.

K těm závažnějším patřil zejména útok zahrnující rozesílání upozornění českým uživatelům, že dluží jistou finanční částku, kterou musí uhradit, pokud se chtějí vyhnout soudnímu řízení. Příloha, která vyvolávala dojem, že obsahuje smlouvu mezi obětí a exekutory, obsahovala malware. Při spuštění přílohy došlo k infikování počítačové stanice.

V měsíci květnu se kromě již tradičních phishingových e-mailů objevily také útoky na směrovače (routery) domácích a firemních sítí. Neznámí útočníci využili zranitelnosti špatně zabezpečených nebo neaktualizovaných směrovačů a přinutili jejich uživatele k instalaci malware, který se tvářil jako aktualizace programu Adobe Flash Player. Další řešené květnové incidenty se týkaly mobilního malware zacíleného na klienty českých bank. Virus nabízel uživateli instalaci bezpečnostní aplikace, případně její aktivaci do mobilního telefonu. Nebezpečným rysem těchto útoků zaměřených na vykrádání bankovních kont bylo, že pachatelé takto získané peníze přeposílali na „bílé koně“[24], které nabírali na pracovních portálech. Úkolem bílých koní bylo obdržené peníze zaslat na zahraniční konta. Za tuto službu jim byla poté poskytnuta provize v řádech tisíců korun. Ve stejném období došlo v Belgii k potvrzení, že v informačním systému belgického ministerstva zahraničí a hospodářství byl nalezen špionážní malware Uroburos, který sbíral dokumenty a informace týkající se krize na Ukrajině. GovCERT.CZ byl o této skutečnosti informován CERT-EU. Informace byla ihned distribuována mezi česká ministerstva, která přijala příslušná opatření.

Červnovým statistikám dominoval špionážní malware Havex, který se zaměřoval zejména na průmyslové systémy energetických společností a organizací vyvíjejících průmyslové zařízení (tzv. SCADA systémy). GovCERT.CZ se incidentem začal zabývat poté, co jej bezpečnostní společnost Symantec informovala o důvodném podezření na výskyt

[24] Bílý kůň – slangově označená osoba, která je nastrčena k páchání trestné činnosti s cílem zakrýt skutečného pachatele nebo osobu, která má z této činnosti prospěch.

tohoto škodlivého kódu na 15 českých IP adresách. Na základě varování kontaktoval GovCERT.CZ všechny poskytovatele služeb elektronických komunikací, pod které spadaly postižené IP adresy. Současně jim předal potřebné technické informace a upozornil je na nutnost varovat všechny postižené subjekty.

Období července a srpna 2014 bylo stejně jako v loňském roce doprovázeno zvýšenou intenzitou rozesílání podvodných zpráv. Mezi klasickými exekutorskými zprávami, které měly budit dojem, že e-mail pochází od exekutora a po oběti požaduje uhrazení dlužné částky, se objevil i případ podvodné SMS zprávy. Ta klienta nabádala ke stažení dodatečné aplikace k vylepšení mobilního bankovnictví. Poškozenému byl poté z účtu odcizen větší obnos peněz.

Kromě phishingu patřily k významnějším červencovým incidentům také DoS útoky na informační systémy Kanceláře prezidenta republiky. Útok byl údajně prováděn z čínské IP adresy. V srpnu pak došlo ke znovuotevření incidentu Spyware Turla, neboť se nově objevila podezření, že malware byly nakaženy české státní instituce. Na základě uskutečněné analýzy bylo zjištěno, že se jedná o výstupné body anonymizační sítě TOR provozované na českých serverech.

Zatímco v září se Českou republikou šířila v pořadí několikátá vlna falešných e-mailů vyzývající k zaplacení dlužné částky, říjen byl pozoruhodný další z ruských špionážních kampaní, která získala označení SandWorm. Kampaň cílila na instituce NATO, ukrajinské vládní instituce, západoevropské vládní organizace (MZV, armády a zbrojní dodavatele), energetické společnosti, telekomunikační společnosti a akademické organizace. Díky spolupráci mezi GovCERT.CZ a CERT-EU byla ihned varována ministerstva, u kterých existovala domněnka, že by se mohla stát obětí útoku.

V závěru roku probíhalo dořešení některých incidentů, mezi nimi i těch týkajících se phishingových zpráv rozesílaných zákazníkům České pošty. Díky navázaným vztahům s německým národním týmem CERT a dobře fungující spolupráci s CSIRT.CZ se v této době rovněž podařilo zabránit šíření malware se jménem Asprox/Kuluoz, který útočil na staré redakční systémy. Neméně zajímavý případ ze závěru roku byl také Carbanak – malware útočící na finanční instituce východoevropských zemí. Počet obětí malware navrženého pro špionáž a krádež dat se dle obdržených informací dosud vyšplhal na 25 bankovních institucí. V současné době stále probíhá vyšetřování.

Prosinec byl také měsícem pokračujícího vyšetřování spywaru Red October. Společnost Kaspersky Labs tento malware nazvala Cloude Atlas, neboť jeho infrastruktura byla založená právě na cloudové technologii. Škodlivý kód byl určen pro infikování širokého spektra zařízení včetně Windows OS, domácích routerů, mobilních zařízení s iOS, BlackBerry OS a Android OS. Infikování koncových zařízení probíhalo převážně pomocí spear-phishingových zpráv nebo prostřednictvím škodlivých SMS a MMS.

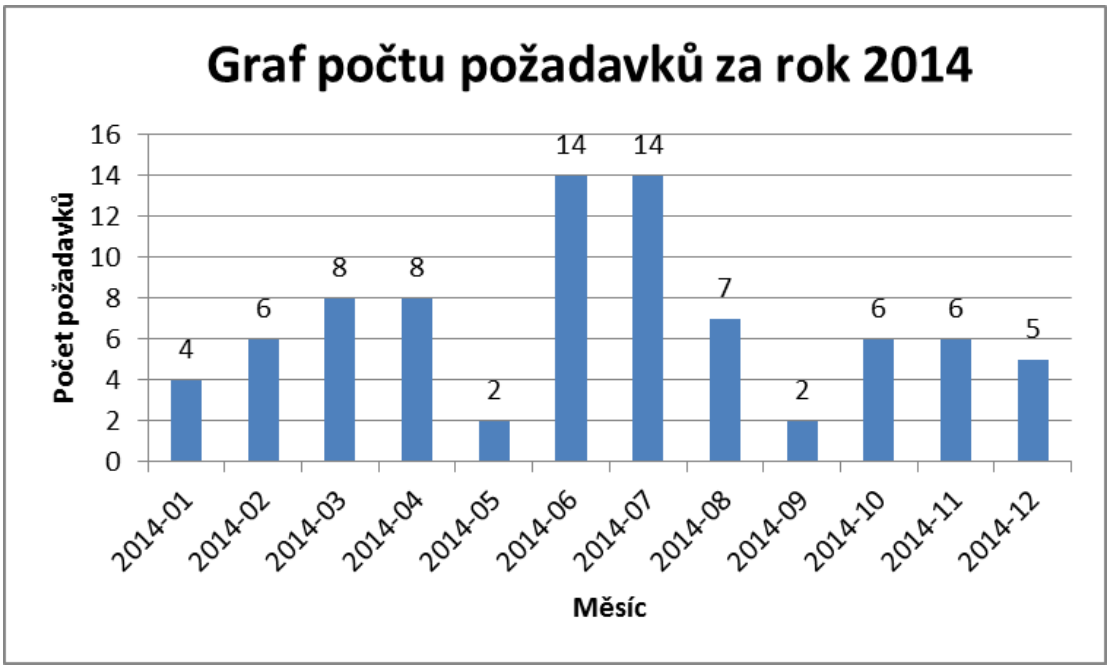
V zásadě lze konstatovat, že se charakter útoků páchaných v roce 2013 a 2014 příliš neliší. Obecně stále platí, že v četnosti útoků jsou nejvýznamnější ty založené na bázi sociálního inženýrství (phishing, spear-phishing). I když se jejich pachatelé snaží používat stále nové a sofistikovanější metody, podstatou útoků zůstává vylákat od uživatelů přístupová hesla, případně distribuovat nebezpečný kód, který útočníkům zajistí přísun užitečných informací. Motivem takových podvodných e-mailů je zpravidla finanční zisk.

Rok 2014 je také dokladem dalšího nebezpečného jevu stále častěji se vyskytujícího v kybernetickém prostoru – použití špionážních malware. Množství takovýchto škodlivých kódů bylo použito jak proti cílům v Rusku, tak proti Spojeným státům nebo i zemím EU. Obvykle se jedná o velmi složité a sofistikované malware navržené ke krádeži důvěrných a citlivých informací státních, vojenských či výzkumných institucí.

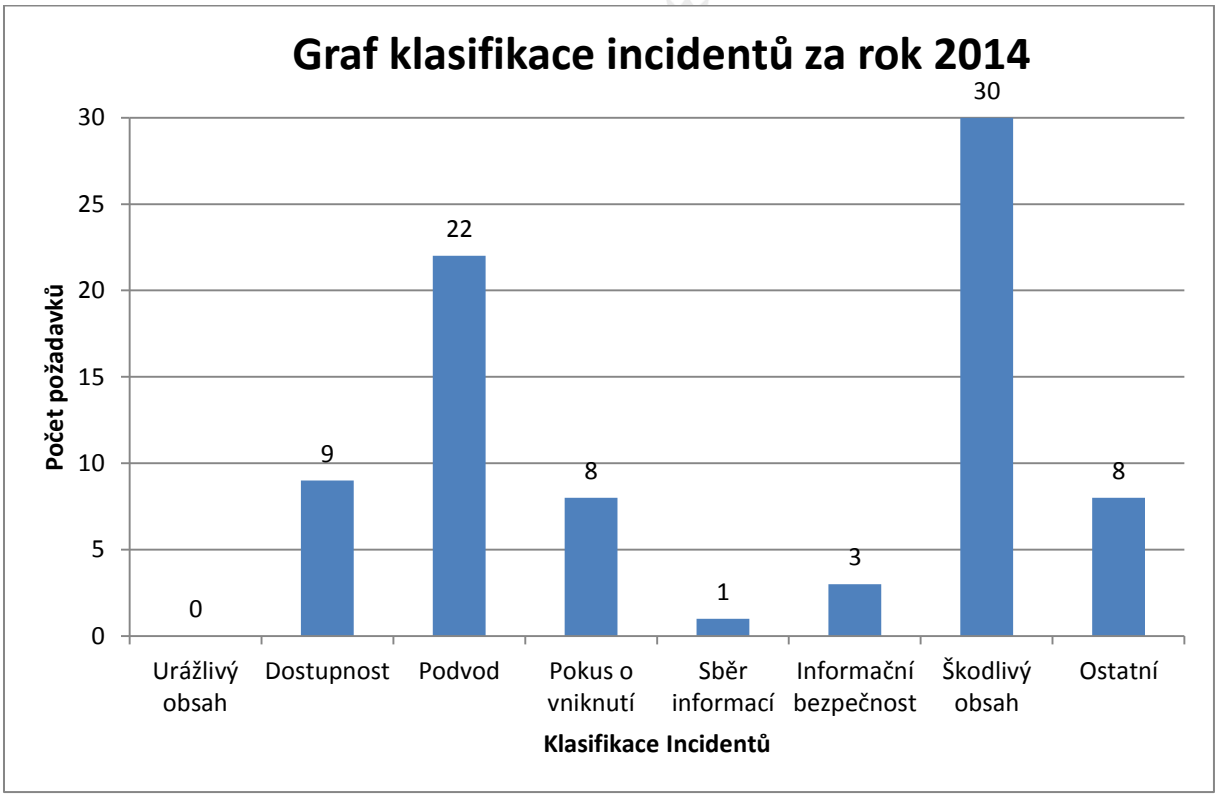
Bližší informace o nejvýznamnějších útocích spáchaných v roce 2014 na české a zahraniční cíle jsou dostupné na stránkách www.govcert.cz v sekci Informační servis. Stručný přehled kybernetických incidentů týkajících se České republiky je pak obsahem následující kapitoly.

8.3. Statistiky kybernetických incidentů

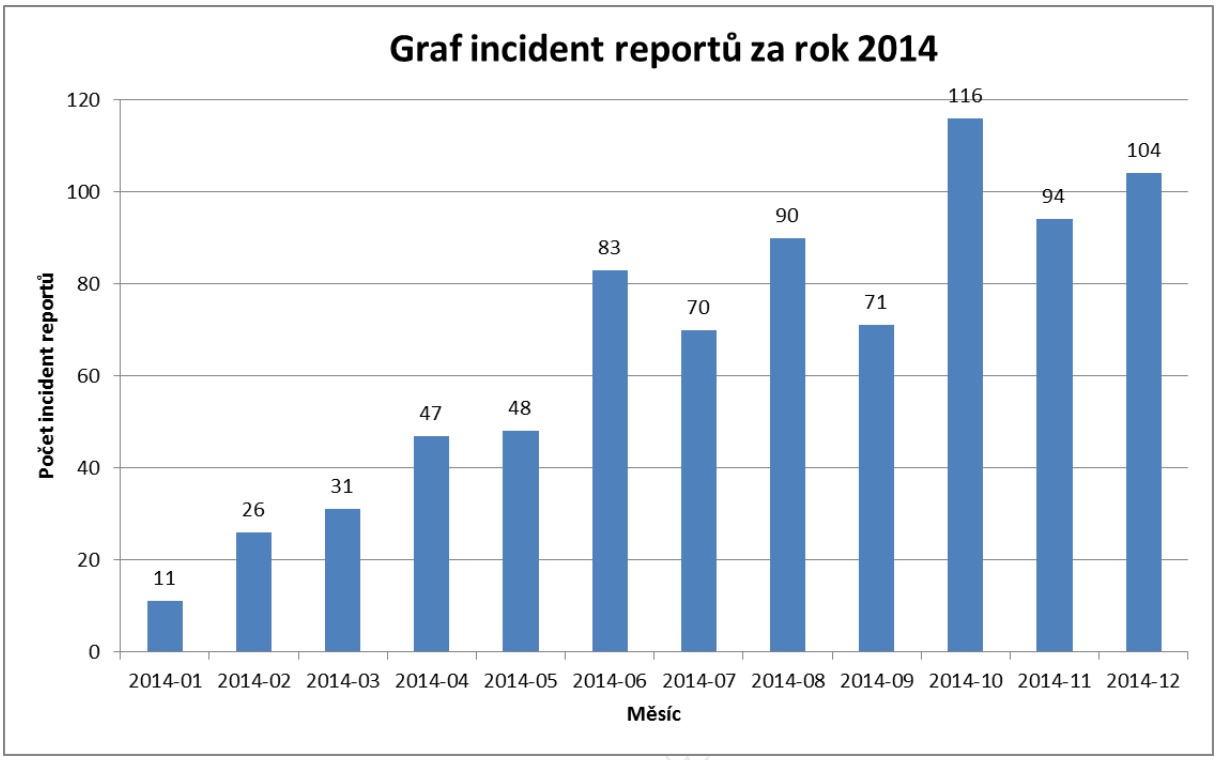
Záměrem této kapitoly je graficky zachytit a znázornit incidenty, které byly v roce 2014 řešeny pracovníky NCKB. Výstupem následných grafů by mělo být poskytnutí informace o jejich počtu, klasifikaci a rozdělení podle tzv. oblastí působnosti.



Graf 01 – množství incidentů přijatých a zpracovaných pracovníky GovCERT.CZ v roce 2014.



Graf 02 – znázornění klasifikace incidentů včetně počtu požadavků.



Graf 03 – počet incident reportů za rok 2014 s rozdělením na každý měsíc.

PŘÍLOHY

Příloha č. 1

Mezinárodní kybernetická cvičení

Cyber Coalition

Na základě Memoranda o porozumění a spolupráci v oblasti kybernetické obrany mezi NATO a Českou republikou se NBÚ a MO v roce 2014 opět zapojili do každoročního aliančního kybernetického cvičení Cyber Coalition. Cvičení Cyber Coalition 2014 proběhlo ve dnech 17. až 21. listopadu 2014 a jeho primárním záměrem bylo na konkrétních scénářích procvičit technickou i netechnickou koordinaci při řešení kybernetických bezpečnostních incidentů, zlepšit vzájemnou informovanost o stávajících obranných schopnostech a upozornit na význam kybernetické obrany v rámci NATO. Mimoto mělo za cíl prověřit rozhodování a spolupráci mezi orgány NATO a národními kybernetickými obrannými kapacitami členských států a partnerských zemí. Do cvičení se zapojilo více než 670 techniků a IT odborníků, vládních zaměstnanců a expertů na kybernetickou bezpečnost z 33 států.

Cvičení bylo na národní úrovni organizováno zástupci MO a NBÚ. Za NBÚ byl do Tartu (Estonsko), odkud bylo celé cvičení řízeno, vyslán jeden zástupce jakožto řídící cvičení. Dále pak byly určeni dva zástupci, kteří působili v Brně jako tzv. rozhodčí cvičení, a kteří koordinovali a dohlíželi na průběh scénářů. Letos poprvé cvičil GovCERT.CZ ve vlastních prostorách v budově NCKB v Brně. Zde byly rovněž přítomny tzv. joint 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, PČR), soukromého sektoru (CSIRT.CZ) a akademické sféry (CSIRT-MU, CESNET). 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 resorty[25] .

[25] Odkaz: https://www.govcert.cz/cs/informacni-servis/akce-a-udalosti/ceska-republika-nacvicovala-kybernetickou-bezpecnost-s-clenskymi-zememi-nato/.

Cyber Europe

Cvičení Cyber Europe je organizováno každé dva roky agenturou ENISA. Letos se jej zúčastnili zástupci z 29 zemí EU a Evropského sdružení volného obchodu. Toto cvičení je koncipováno trojfázově. Fáze technická (Technical-level Exercise) se uskutečnila ve dnech 28. a 29. dubna a fáze operační (Operational-level Exercise) dne 30. října.

Třetí a poslední částí je fáze strategická (Strategic-level Exercixe), která je naplánovaná na leden 2015. Za Českou republiku je primárním zástupcem národní CSIRT, jenž plní koordinační roli. NBÚ/GovCERT.CZ se účastnil obou fází konaných v roce 2014 a přispěl k velmi dobrému hodnocení České republiky v porovnání s ostatními účastnícími se státy.

Locked Shields

Cvičení Locked Shields, pořádané každoročně NATO CCDCOE v Tallinnu, se konalo ve dnech 19. až 23. května 2014 a zapojilo se do něj více než 300 účastníků ze 17 zemí. Cvičení se odehrávalo v simulovaném prostředí s desítkami počítačů a serverů, kde stál tzv. červený tým proti modrým týmům. Úkolem modrých týmů bylo se bránit hacktivistickým kampaním, špionážním, sabotážním a ostatním kybernetickým útokům vedených na jejich sítě členy červeného týmu. Za NBÚ se tohoto cvičení účastnili pracovníci NCKB, kteří společně s Lotyšskem vytvořili společný tým (joint team). Cvičení obsahovalo jak technické, tak právní scénáře, přičemž Česká republika měla zastoupení v obou oblastech. V průběhu cvičení, jež je koncipováno jako konkurenční hra, jsou obranné modré týmy bodově hodnoceny. Dle celkového vyhodnocení dosáhla Česká republika v letošním ročníku nadprůměrných výsledků.

EU – Multi Layer

Cvičení kybernetické bezpečnosti EU – Multi Layer proběhlo v roce 2014 ve dnech 30. září až 23. října. Jedná se o procedurální velitelsko-štábní cvičení orgánů krizového řízení EU s primárním cílem procvičit a zlepšit schopnosti EU zvládat krizové situace a implementovat komplexní přístup EU ke konfliktům. Záměrem tohoto cvičení je procvičit systém krizového řízení EU v různých rovinách, na úrovni strategické a operační, a to jak v prostředí vojenském, tak i civilním. Hlavním cvičícím subjektem za Českou republiku je Stálé zastoupení při EU, jehož podporu zabezpečuje Společná plánovací skupina tvořená na bázi Společného operačního centra MO formou přípravy národních stanovisek na základě analýz přijatých dokumentů a rozhodnutí věcně odpovědných ústředních správních úřadů včetně NBÚ. V rámci scénářů se letos poprvé procvičoval kybernetický bezpečnostní incident, k němuž se musel NBÚ coby gestor kybernetické bezpečnosti České republiky odborně vyjádřit.

Crisis Management Exercise

Crisis Management Exercise (CMX) je cvičení států Severoatlantické aliance a dalších přizvaných států zaměřené na orgány krizového řízení. Jelikož scénáře obsahují zpravidla také kybernetické útoky, zapojuje se do něj pravidelně i NBÚ. Primárně však cvičení spadá pod gesci MO. NBÚ se v rámci CMX podílí nejen na jeho přípravě a tvorbě scénářů, ale zároveň je i jedním z cvičících. Cvičení pro rok 2014 bylo na základě rozhodnutí Severoatlantické rady NATO posunuto na březen 2015.

CECSP 2014 Exercise

Dne 23. června 2014 proběhlo cvičení CECSP 2014 Exercise uspořádané v rámci Středoevropské platformy pro kybernetickou bezpečnost[26]. Jednalo se o jednodenní table-top cvičení, kterého se zúčastnili zástupci České republiky, Maďarska, Polska, Slovenska a Rakouska. Cvičení pod vedením maďarského Národního bezpečnostního úřadu se uskutečnilo v rámci platformy poprvé, do budoucna se však počítá s dalším ročníkem.

[26] Viz kapitola 5.5.

Příloha č. 2

Seznam použitých zkratek a pojmů[27]

AFCEA – Armed Forces Communications and Electronics Association

CBMS – Confidence Building Measures

CCDCOE – Cooperative Cyber Defence Centre of Excellence

CECSP – Central European Cyber Security Platform

CERT – Computer Emergency Response Team

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

CMX – cvičení Crisis Management Exercise

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/DoS útok – Distributed Denial of Service / Denial of Service

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

EU – Evropská unie

FENIX – nové označení projektu Bezpečná VLAN

GovCERT.CZ – představuje 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

ICS ISAC – Industrial Control System Information Sharing and Analysis Center

IDG konference – International Data Group konference

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

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

PČR – Policie České republiky

PHISHING – podvodná technika k získávání citlivých údajů od uživatelů na internetu

RIA – Hodnocení dopadu regulace (Regulatory Impact Assessment)

SCADA systémy – Supervisory Control And Data Acquisition

SIEM – Security Information and Event Management

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.

TF-CSIRT – Task Force Computer Security Incident Response Team

TURLA – pojmenování jednoho druhu malwaru

VIS – Významný informační systém

VLAN – virtual LAN

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