Zpráva o stavu kybernetické bezpečnosti České republiky

Výroční zpráva Národního centra kybernetické bezpečnosti podle usnesení vlády ze dne 19. října 2011 č. 781

2013

NBÚ

Vydáno: březen 2014
Autoři: Národní centrum kybernetické bezpečnosti / Národní bezpečnostní úřad
Elektronická verze: www.govcert.cz

Obsah

Úvod

Zajištění kybernetické bezpečnosti státu je jednou z klíčových výzev současné doby. Absence geografických hranic v kyberprostoru a všudypřítomnost kybernetických hrozeb vyžadují intenzivní mezinárodní spolupráci a budování národních kapacit k zajištění kybernetické bezpečnosti státu.

Oblast kybernetické bezpečnosti je a bude jedním z určujících aspektů bezpečnostního prostředí České republiky. Dynamika vývoje kybernetických hrozeb má rychle rostoucí tendenci. Útoky jsou stále sofistikovanější a komplexnější. Ze sféry přímého ekonomického prospěchu útočníků se útoky přesouvají například do oblasti kybernetické průmyslové špionáže, kybernetického vandalismu a testování kybernetické bezpečnosti prvků kritické infrastruktury. Útočníci se stále více zaměřují na prvky kritické infrastruktury, jako jsou energetické systémy, produktovody a zdravotnické informační systémy.

Zpráva o stavu kybernetické bezpečnosti České republiky je vytvářena na základě usnesení vlády ze dne 19. října 2011 č. 781 o ustavení Národního bezpečnostního úřadu gestorem problematiky kybernetické bezpečnosti a národní autoritou pro tuto oblast. Zpráva hodnotí úroveň dosažených cílů v oblasti budování kybernetické bezpečnosti České republiky za období roku 2013 v šesti prioritních oblastech, kterými jsou:

1. Tvorba legislativy v oblasti kybernetické bezpečnosti (dále také jen „KB“):

Je nezbytné vytvořit právní rámec, který definuje kompetence orgánů veřejné moci a práva a povinnosti fyzických a právnických osob v oblasti kybernetické bezpečnosti.

2. Mezinárodní spolupráce v oblasti KB:

a) Komunikace a spolupráce se zahraničními partnery jsou zcela klíčové pro schopnost vytvářet funkční kybernetickou obranu a posilovat kybernetickou bezpečnost České republiky.

b) Prověřování připravenosti a simulace – z důvodu neustálého vývoje na poli kybernetických hrozeb je nezbytné participovat na mezinárodních cvičeních a pořádat národní cvičení kybernetické bezpečnosti. Technické zázemí a spolupráce odborných prvků jsou jen jednou složkou. Cvičení a simulace krizového řízení a rozhodování je nutné konat i jako službu státnímu sektoru a přizvat soukromý sektor, který je kybernetickými hrozbami taktéž ohrožen.

3. Národní spolupráce v oblasti KB:

Je nezbytná široká meziresortní spolupráce, stejně jako spolupráce mezi veřejnoprávním a soukromoprávním sektorem. Zároveň je potřeba spolupracovat s akademickým a odborným sektorem na rozvíjení schopností nezbytných pro kybernetickou bezpečnost.

4. Řízení rizik v oblasti KB:

Mapování, analýza a vyhodnocení rizik spojených s kybernetickou bezpečností v oblasti kritické informační infrastruktury jsou klíčové. Mapování slouží k pochopení rozsahu neustále narůstajícího množství systémů, které mohou být cílem kybernetického útoku nebo incidentu. Analýza slouží k vyhodnocení důležitosti a významu systému a jeho role při fungování státu. Vyhodnocení rizik slouží k minimalizaci škod při případném incidentu a k nastavení ochrany klíčových systémů pro zachování kybernetické bezpečnosti.

5. Budování NCKB/CERT:

technické a výkonné zázemí – Pro kvalitní a efektivní systém detekce, analýzy, řešení a předpovídání kybernetických útoků je nutné vybudovat specializované pracoviště. V případě České republiky se jedná o Národní centrum kybernetické bezpečnosti (dále také jen „NCKB“). Jeho součástí je vybudování systému včasného vzájemného varování a jeho zapojení do existujících mezinárodních systémů včasného varování o kybernetických hrozbách. Cílem činnosti centra je zabraňovat pokusům o průnik do infrastruktur důležitých pro chod státu, pro jeho bezpečnost a pro jeho ekonomiku. Součástí takového centra je tzv. Vládní CERT (Computer Emergency Response Team, dále také jen „GovCERT.CZ“), jehož úloha spočívá v monitorování kybernetického prostoru a odhalování a řešení kybernetických útoků, jejich prevence apod. Takové pracoviště má špičkovou úroveň expertizy a je plně integrováno v segmentu mezinárodní spolupráce s obdobnými pracovišti jiných států a institucí.

6. Zvyšování povědomí v oblasti KB:

vzdělávání a osvěta – Je nutné trvale zvyšovat úroveň vzdělání vedoucích pracovníků, specialistů a úroveň povědomí veřejnosti o kybernetických hrozbách.

Každá prioritní oblast rozpracovává jednotlivé cíle do konkrétních opatření, která jsou předmětem hodnocení této Zprávy.

1. Vývoj legislativy v oblasti kybernetické bezpečnosti v roce 2013

Národní bezpečnostní úřad (dále také jen „NBÚ“) od počátku roku 2013 vyvíjel intenzivní úsilí na tvorbě právních předpisů v oblasti kybernetické bezpečnosti. Kromě tvorby návrhu paragrafového znění zákona o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti) probíhaly rovněž konzultace k návrhům jeho prováděcích právních předpisů.

1.1 Návrh zákona o kybernetické bezpečnosti

Jak bylo uvedeno výše, NBÚ od počátku roku 2013 pokračoval v tvorbě návrhu paragrafového znění zákona o kybernetické bezpečnosti. V průběhu ledna a února 2013 byl návrh zákona o kybernetické bezpečnosti představen a konzultován se zástupci odborné veřejnosti a současně pokračovaly konzultace s meziresortní pracovní skupinou, tvořenou zástupci Ministerstva vnitra, Ministerstva obrany, Českého telekomunikačního úřadu, Generálního ředitelství hasičského záchranného sboru a zpravodajských služeb. Následně NBÚ rozeslal návrh zákona o kybernetické bezpečnosti do meziresortního připomínkového řízení, které proběhlo v termínu od 15. dubna 2013 do 15. května 2013.

Zásadní připomínky k návrhu zákona uplatnilo celkem 14 připomínkových míst a jejich vypořádání se uskutečnilo dne 27. května 2013. Veškeré zásadní připomínky uplatněné k návrhu zákona o kybernetické bezpečnosti byly vypořádány a NBÚ předložil dne 28. června 2013 návrh předmětného zákona vládě bez rozporů.

Návrh zákona o kybernetické bezpečnosti byl následně projednán pracovními skupinami Legislativní rady vlády: dne 12. července 2013 pracovní komisí pro soukromé právo a pracovní komisí pro hodnocení dopadů regulace, dne 22. července 2013 pak pracovní komisí pro veřejné právo I – správní právo č. 1. Legislativní rada vlády návrh zákona o kybernetické bezpečnosti projednala dne 8. srpna 2013. [1]

1.2 Návrh prováděcích právních předpisů

Na tvorbě vyhlášky o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních protiopatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti (vyhláška o kybernetické bezpečnosti) pracoval příslušný věcný útvar Národního bezpečnostního úřadu ve spolupráci s odborným externím konzultantem od počátku roku 2013.

---

[1] Návrh zákona o kybernetické bezpečnosti byl vládou České republiky schválen dne 2. ledna 2014 a postoupen k dalšímu legislativnímu projednávání v Parlamentu České republiky.

Současně NBÚ spolupracoval s odborným externím konzultantem na tvorbě tezí návrhu vyhlášky o významných informačních systémech a jejich určujících kritériích.

Oba tyto návrhy prováděcích právních předpisů byly dokončeny v červnu 2013 a staly se součástí materiálu předloženého vládě dne 28. června 2013.

V září 2013 NBÚ zahájil spolupráci s meziresortní pracovní skupinou, tvořenou zástupci shora uvedených orgánů veřejné moci, za účelem spolupráce na tvorbě konečného paragrafového znění návrhu vyhlášky o kybernetické bezpečnosti a paragrafového znění návrhu vyhlášky o významných informačních systémech a jejich určujících kritériích.

Od října 2013 NBÚ rovněž pokračuje ve spolupráci se zástupci Generálního ředitelství hasičského záchranného sboru při tvorbě návrhu novely nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury, jež byla zahájena v březnu 2013.

2. Podpora mezinárodní spolupráce v oblasti kybernetické bezpečnosti

NBÚ se zapojil v roce 2013 do mezinárodního kontextu hned ve třech širších oblastech, které lze rozdělit na aktivity v rámci Evropské unie, aktivity v rámci NATO a bilaterální a multilaterální jednání.

2.1 Evropská unie

Otázky spojené s kybernetikou a kybernetickou bezpečností se postupně stávají součástí téměř všech klíčových unijních politik a je logické, že dochází k významným přesahům především u vnitřního trhu a vnějších vztahů a politik, jako jsou justiční spolupráce v trestních věcech, policejní spolupráce, ochrana spotřebitele, transevropské sítě, průmysl či výzkum, technologický rozvoj a společná obchodní politika.

Témata spojená s kybernetikou a kybernetickou bezpečností jsou proto předmětem činnosti několika neformálně ustanovených tematických skupin, které slouží převážně k výměně informací a zkušeností zainteresovaných subjektů, některých agentur EU a také jednotlivých unijních institucí podílejících se na tvorbě legislativy.

Za účelem lepší koordinace činnosti mezi jednotlivými aktéry a vytvořením průřezového náhledu na celou problematiku kybernetiky a kybernetické bezpečnosti byla na popud Německa, Francie, Nizozemí, Švédska a Velké Británie kyperským předsednictvím aktivizována **Skupina přátel předsednictví**, která by se měla scházet cca dvakrát ročně, aby identifikovala priority a zajišťovala soulad mezi aktivitami ostatních pracovních orgánů. První jednání, které se uskutečnilo na počátku prosince 2012, bylo spíše informativního charakteru. Členské státy schválily rozsah působnosti aktivit skupiny a přijaly závazek k pokračování její činnosti. Dále Evropská komise informovala členské státy o stavu příprav Evropské strategie pro kybernetickou bezpečnost (dále také jen „Strategie EU“).

V současné době se aktivity EU na poli kybernetiky a kybernetické bezpečnosti soustředí do tří oblastí, u kterých lze předpokládat, že i do budoucna zůstanou středem zájmu činnosti EU. Konkrétně se jedná o 1) potírání a předcházení kybernetické kriminality, 2) kybernetickou obranu a 3) bezpečnost sítí. Všechny tyto tři elementy jsou společně provázány unijní legislativou, která se aplikuje také při sjednávání mezinárodních smluv EU se třetími zeměmi – což v praxi znamená značný přesah tematiky kybernetiky do zahraničně-politické roviny vnějších vztahů.

Hlavním tématem pro NBÚ na evropské úrovni se stala bezpečnost sítí a informací (NIS). Proto se na první místo v rámci priorit zařadila pracovní skupina Rady EU pro telekomunikace **Working Party on Telecommunications and Information Society**, která projednává návrh směrnice Evropského parlamentu a Rady EU o opatřeních k zajištění vysoké společné úrovně

bezpečnosti sítí a informací v EU (dále jen „Směrnice NIS“). Jedná se o dokument navržený Evropskou komisí pro Evropský parlament a Radu EU.

Při jednáních vychází NBÚ z Rámcové pozice/Stanoviska pro Parlament České republiky, kde jsou stanoveny hlavní problematické body. Během roku docházelo k prvnímu pročítání textu za účasti všech členských států a tyto vznášely prvotní připomínky jak k jednotlivým článkům, tak i k celému textu Směrnice NIS. V oblasti NIS jsou obecně nejaktivnější Spojené království, Francie, Německo, Nizozemsko, Belgie, Finsko a Švédsko; mezi novými členskými státy je to pak Maďarsko či Estonsko.

Související skupinou je již výše zmíněná **Skupina přátel předsednictví pro kybernetickou bezpečnost**, zabývající se Strategií EU. Jedná se o společně navržený dokument Evropské komise a Vysoké představitelky pro zahraniční a bezpečnostní politiku pro Evropský parlament, Radu EU, Evropský hospodářský a sociální výbor a Výbor regionů. Ke Strategii EU byly přijaty tzv. Závěry Rady a v rámci pracovní skupiny se diskutuje o jejich implementaci. Litevské předsednictví navrhlo čtyři různé způsoby implementace a bude nyní na členských státech, ke kterému z nich se přikloní. Česká republika preferuje možnost vytvoření akčního plánu, jenž by jasně identifikoval prioritní oblasti a stanovil jasné termíny a cíle, které by určily postup pro členské státy.

2.2 ENISA

Evropská agentura pro bezpečnost sítí a informací (ENISA) byla zřízena v březnu 2004 s cílem dosáhnout vysokého stupně informační a síťové bezpečnosti mezi členskými státy EU a zvyšovat povědomí o NIS jako přidané hodnoty pro občany, firmy a veřejnou správu, a tudíž přispívat k bezproblémovému fungování vnitřního trhu. ENISA napomáhá Evropské komisi a členským státům chránit informační a síťovou bezpečnost a řešit problémy v této oblasti. Významná je rovněž její role v organizaci cvičení proti kybernetickým útokům či v podpoře týmů CERT včetně jejich koordinace. Správní rada ENISA stanovuje obecné směry činnosti ENISA, dále zajišťuje, aby práce agentury byla v souladu s aktivitami členských států a EU, a také schvaluje pracovní program agentury, roční souhrnnou zprávu o činnosti agentury a rozpočet ENISA.

Česká republika má v ENISA své zastoupení formou účasti na pořádaných jednáních. Dva zástupci ČR jsou členy správní rady ENISA (Management Board Member a Alternate Management Board Member), kde jsou zodpovědní za schvalování programu a rozpočtu ENISA. Vzhledem k aktivní spolupráci s touto agenturou zažádala Česká republika v říjnu 2013 o asistenci v oblasti školení a profesních cvičení v rámci budování Národního centra kybernetické bezpečnosti.

2.3 OBSE

K aktivnímu zapojení České republiky dochází i na půdě OBSE, kde v průběhu roku 2013 probíhala jednání k dokumentu o opatřeních za účelem budování důvěry v oblasti kybernetické bezpečnosti (Confidence Building Measures). Česká republika při těchto jednáních koordinuje své postupy v rámci Evropské unie s dalšími členskými státy, neexistuje zde však „jednotný hlas EU", jelikož k tomu chybí politická vůle některých členských států.

2.4 Bilaterální a multilaterální spolupráce

V průběhu roku 2013 se uskutečnila řada návštěv partnerských úřadů v členských státech NATO a EU zaměřených především na sdílení informací o systému zajištění kybernetické bezpečnosti a na získání zkušeností s provozováním vládních CERTů. V této souvislosti pracovníci NBÚ navštívili Rakousko, USA, Švédsko, Izrael, Francii, Jižní Koreu a CERT Evropské unie.

2.4.1 Rakousko

V lednu 2013 navázal NBÚ spolupráci s vládním a národním CERTem Rakouska. Obě strany se shodly na myšlence regionální spolupráce národních a vládních CERTů v oblasti střední Evropy (státy Visegrádské čtyřky a Rakousko). V květnu 2013 bylo na základě dohody s rakouskými kolegy svoláno ustavující jednání Středoevropské platformy kybernetické bezpečnosti. Jednání se zúčastnili zástupci vládních a národních CERTů z České republiky, Slovenska, Maďarska, Polska a Rakouska. Byla dohodnuta výměna informací a zkušeností v oblasti kybernetické bezpečnosti, konzultace a podpora postojů v rámci EU a NATO a organizace společných cvičení. Ve dnech 18.–19. prosince 2013 pak NBÚ zorganizoval jednání o technických aspektech kybernetické bezpečnosti.

2.4.2 USA

V dubnu 2013 byly při cestě do USA navázány kontakty s Federal Bureau of Investigation (FBI), Department of Homeland Security (DHS) a Department of Defense (DoD). Zároveň proběhly schůzky s CSIRT DHS, zástupci Úřadu prezidenta USA pro kybernetickou bezpečnost, poradcem pro kybernetickou bezpečnost v Kongresu USA a představiteli soukromých subjektů jako je Microsoft, Cisco, AT&T a dalšími.

2.4.3 Švédsko

NBÚ navázal kontakt se Švédskou agenturou pro mimořádné události (MSB/Swedish Civil Contingency Agency), která je národním koordinátorem civilní bezpečnosti v případě stavu nouze a v krizových situacích. Jejím základním úkolem je tvorba a následná podpora krizového managementu v rámci lokálních, regionálních a národních kapacit. Zabývá se celým spektrem krizových scénářů od každodenních drobných nehod přes kybernetickou bezpečnost, ochranu kritické informační infrastruktury až po celonárodní katastrofy zásadního významu, zahrnující například i přírodní katastrofy.

2.4.4 Izrael

V červnu 2013 byla navázána spolupráce s Národní kybernetickou kanceláří státu Izrael. Obě strany se dohodly na oblastech spolupráce (věda a výzkum, výměna informací, stáže expertů, každoroční schůzky hodnotící a usměrňující spolupráci).

2.4.5 Francie

V září se zástupci NBÚ setkali s představiteli francouzského Národního úřadu pro bezpečnost informačních systémů (Agence nationale de la sécurité des systèmes d'information – ANSSI) a dohodli se na spolupráci, výměně informací a konzultacích ohledně směrnice NIS.

2.4.6 Jižní Korea

V říjnu se vedení NCKB zúčastnilo konference „Seoul Conference on Cyberspace 2013" a navázalo spolupráci na bázi výměny expertů s národním CERTem Jižní Korey.

2.4.7 Central European Cyber Security Platform

NBÚ v květnu roku 2013 zorganizoval první setkání vládních, národních a vojenských CERTů zemí Visegrádské skupiny a Rakouska. Po základní prezentaci všech typů CERTů z těchto zemí došlo k dohodě o zorganizování setkání technických expertů. Toto setkání nakonec uspořádal NBÚ ve dnech 18.–19. prosince 2013 v Praze.

2.4.8 CCD COE

NCKB připravilo zapojení České republiky do NATO Cooperative Cyber Defence Centre of Excellence (dále jen „CCD COE") v Tallinnu. Cílem CCD COE je zvyšovat obranné schopnosti a zlepšovat spolupráci a sdílení informací mezi účastnickými státy a NATO, popřípadě mezi účastnickými státy navzájem, a partnery v oblasti kybernetické obrany, a to prostřednictvím zvyšování povědomí o kybernetické bezpečnosti, rozvoje doktrín a koncepcí kybernetické obrany, výzkumu, vývoje a konzultací. V této souvislosti se CCD COE zaměřuje na kybernetickou bezpečnost z hlediska práva, konceptů a strategií, taktického prostředí a ochrany kritické informační infrastruktury. Zájem České republiky o zapojení do CCD COE byl deklarován předsedou vlády České republiky dne 18. dubna 2013. Dne 4. prosince 2013 pak vláda schválila usnesení č. 926/2013 Sb., o zapojení České republiky do NATO Cooperative Cyber Defence Centre of Excellence v Tallinnu.

Zapojení umožní České republice podílet se na výzkumných a vzdělávacích projektech CCD COE a těžit z jejich výsledků, a to například ve formě bezplatného školení expertů Vládního CERTu v oblasti analýzy malwaru, obrany před kyberútoky, forenzních aspektů kybernetické bezpečnosti a obrany před botnety. CCD COE také může poskytnout podporu případných národních cvičení v oblasti kybernetické bezpečnosti.

Účast v CCD COE bude velmi přínosná i z hlediska prosazování zájmů České republiky. CCD COE má totiž významný vliv na vytváření mezinárodního práva v oblasti kybernetických konfliktů a s tím souvisejících bezpečnostních doktrín. V březnu 2013 publikovalo CCD COE tzv. Tallinnský manuál, který aktuálně reprezentuje stanoviska nejkvalifikovanějších právních znalců v oboru. Česká republika bude mít vliv na podobu takových dokumentů již ve fázi jejich vzniku. Česká republika také bude moci ovlivňovat zaměření výzkumné činnosti CCD COE.

2.4.9 TERENA TI

NCKB zrealizovalo kroky k zařazení GovCERT.CZ na seznam Trusted Introducer organizace Trans-European Research and Education Networking Association TI. V současnosti je GovCERT.CZ již zařazen pod status „listed" – registrován; k další certifikaci je zajištěna potřebná podpora partnerů.

2.4.10 Cyber Coalition

Na základě Memoranda o porozumění o spolupráci v oblasti kybernetické obrany mezi NATO a NBÚ se NBÚ poprvé zapojil do cvičení Cyber Coalition 2012 jako primární národní kontaktní místo. Cvičení Cyber Coalition 2013, které proběhlo ve dnech 25.–29. listopadu 2013, mělo za cíl otestovat připravenost států NATO na několik současně probíhajících hrozeb v oblasti kybernetické bezpečnosti. Toto cvičení se soustředí na několik aktuálních oblastí, v nichž je možno očekávat reálný útok. Byly procvičovány jak oblasti čistě technické (analýza škodlivého kódu), tak organizační, právní a public relations.

Cvičení se účastnilo Vrchní velitelství NATO, členské státy NATO, Partnerské státy a orgány EU odpovědné za oblast kybernetické obrany. Za ČR se cvičení účastnilo Ministerstvo obrany a Národní bezpečnostní úřad/NCKB, Policie České republiky, Bezpečnostní informační služba, Ministerstvo zahraničních věcí, CZ.NIC, poskytovatelé internetových služeb (ISP) a dodavatelé technologií. Cvičení Cyber Coalition 13 bylo samotnými cvičícími hodnoceno kladně. Zapojení cvičících na nevojenském úseku obecně a v rámci soukromého sektoru zvláště bylo oproti předchozím ročníkům dosud nejrozsáhlejší. Podařilo se splnit všechny zadané úkoly. Během cvičení bylo zjištěno několik nedostatků. Ty jsou však možná nejcennějším výstupem, protože na jejich základě lze vyslovit doporučení, a to jak k přípravě dalších ročníků Cyber Coalition, tak především k implementaci v reálném světě.

Nejenže se NCKB podílí na přípravě cvičení, vystupuje zároveň jako koordinátor a jeden z účastníků tohoto cvičení.

2.4.11 CMX

Crisis Management Exercise (CMX) je cvičení států NATO a dalších přizvaných států v oblasti krizového řízení. V CMX jsou zahrnuty i tzv. kybernetické scénáře, ve kterých je testována připravenost vojenských i civilních složek reagovat na reálné hrozby v oblasti kybernetické bezpečnosti. NCKB se aktivně podílí na tvorbě těchto scénářů v rámci NATO a provádí konzultace o jejich obsahu a o možnostech zapojení ČR s ostatními orgány veřejné moci a s dotčenými právnickými osobami. NCKB se také bude účastnit samotného cvičení jako cvičící. CMX má i dimenzi národní spolupráce, neboť hlavním cvičícím je Ministerstvo obrany společně s Ministerstvem zahraničních věcí a již zmíněným NCKB. Poslední CMX proběhlo v roce 2012 sloučené s cvičením Cyber Coalition. Další cvičení CMX proběhne v březnu 2014 a NCKB se v roce 2013 podílelo na přípravě cvičných scénářů.

3. Národní spolupráce v oblasti KB

3.1 CZ.NIC

Spolupráce s CZ.NIC se plně projevila během DDoS útoků začátkem roku 2013. Během několika dnů, kdy Česká republika čelila masivním DDoS útokům, byla spolupráce mezi CZ.NIC a NCKB/GovCERT.CZ přenesena z konzultačně-teoretické roviny do praktického řešení útoků na informační infrastrukturu na celonárodní úrovni. Během tohoto období došlo i k vylepšení komunikačních procedur mezi jednotlivými pracovišti. CZ.NIC se zároveň podílí jako člen odborné veřejnosti na konzultacích k zákonu o kybernetické bezpečnosti. Kromě již zmíněné velmi kvalitní spolupráce se CZ.NIC podílí i jako mediátor při komunikaci se soukromými subjekty a pomohl identifikovat mezeru v zákoně o elektronických komunikacích.

3.2 CSIRT.MUNI

CSIRT (Computer Security Incident Response Team) Masarykovy univerzity se řadí mezi špičková akademická pracoviště evropského formátu. Spolupráce s CSIRT.MUNI je založena na vzájemné kooperaci v technické oblasti, spolupráci při řešení DDoS útoků a forenzní analýze. Teoretická podpora je doplněna stážemi pracovníků GovCERT.CZ v CSIRT.MUNI. CSIRT.MUNI je díky své pozici i jedním z garantů pro přistupování GovCERT.CZ do mezinárodních aliancí a organizací v akademické a technické rovině.

3.3 Microsoft

Společnost Microsoft je jedním z klíčových partnerů NCKB. V roce 2013 byla podepsána smlouva mezi NBÚ/NCKB a společností Microsoft upravující spolupráci v problematice botnetů. Česká republika je jednou z prvních zemí na světě, která má takovouto smlouvu podepsanou. Smyslem smlouvy je předávání informací ze strany Microsoftu o napadených počítačích malwarem, které jsou součástí botnetů, české straně, jež pak v rámci svých pravomocí upozorňuje majitele dotčených stanic o napadení jejich počítačů. Jedná se o unikátní data, jejichž zpracování a vyhodnocování přispívá ke zvýšení kybernetické bezpečnosti České republiky.

3.4 Ministerstvo obrany

NBÚ a Ministerstvo obrany připravily Rámcovou smlouvu o spolupráci v oblasti informačních a komunikačních technologií a bezpečnosti. Kromě již připravované Rámcové smlouvy NCKB spolupracuje s armádním CSIRTem za účelem výměny a sdílení zkušeností a informací o kybernetických událostech a incidentech.

3.5 Poradní komise ředitele Národního bezpečnostního úřadu

Poradní komise byla zřízena dne 12. března 2013. Smyslem komise je vytvoření poradního orgánu ředitele NBÚ, ve kterém jsou reprezentovány akademické instituce, soukromé subjekty i orgány veřejné moci. Důvodem je koordinace úsilí a společných postupů pro zajištění kybernetické bezpečnosti při útoku na kybernetickou infrastrukturu, sdílení informací a návrhy řešení a obrany proti kybernetickým útokům. Zřízená komise ředitele má za úkoly mimo jiné:

- shromáždění provozních dat a jejich analýzu nasbíraných během incidentu
- analýzu malwaru
- návrh doporučení, jaká data v budoucnu sbírat
- návrh doporučení pro subjekty, jak postupovat v budoucnu při napadení jejich sítě
- nastavení spolupráce mezi bezpečnostními týmy a administrátory napadených sítí

Členy poradní komise jsou zástupci internetových poskytovatelů, internetových portálů, výzkumných pracovišť univerzit, Policejního prezídia České republiky / Policejní akademie České republiky, tajných služeb, bankovního sektoru a zástupci energetického sektoru. Jednání komise se účastní přizvané instituce dle charakteru kybernetického incidentu.

3.6 Akademická sféra

NBÚ/NCKB navázaly spolupráci s akademickou sférou ČR formou smluv o spolupráci. V současné chvíli jsou podepsány smlouvy s následujícími akademickými institucemi:

- Masarykova univerzita Brno
- Vysoké učení technické Brno
- Univerzita obrany
- České vysoké učení technické Praha

Zároveň se připravují smlouvy o spolupráci s Policejní akademií, Vysokou školou báňskou v Ostravě a CEVRO Institutem.

3.7 Další partneři

Mimo zmíněných partnerů na národní úrovni NCKB aktivně spolupracuje i s Bankovní asociací ČR, Asociací krajů ČR, Policií České republiky v oblasti kybernetické kriminality, Policejním prezidiem a zpravodajskými službami České republiky.

4. Řízení rizik v oblasti KB

V průběhu roku 2012 provedl NBÚ rozsáhlý průzkum zaměřený na stav zabezpečení informačních systémů státní správy a samosprávy. V rámci průzkumu byly osloveny ústřední orgány státní správy a územní samosprávné celky dvěma dotazníky zaměřenými na stav a zabezpečení jejich informačních systémů. Klíčovým parametrem pro vyhodnocení úrovně řízení rizik v oblasti kybernetické bezpečnosti důležitých informačních a komunikačních technologií státu bylo hodnocení úrovně vyspělosti systému řízení bezpečnosti informací. Toto bylo provedeno na základě sedmistupňové hodnotící škály (podrobnosti viz Příloha ke Zprávě o činnosti NBÚ v oblasti KB v roce 2012 – Kvalitativní úrovně řízení bezpečnosti podle ISO/IEC 27001). Nedostatky, které byly zjištěny v průběhu průzkumu, byly s dotčenými subjekty projednány na společných dvoustranných jednáních v průběhu prvního čtvrtletí roku 2013. V průběhu roku 2013 probíhala vícefázová jednání se subjekty z průzkumu za účelem narovnání nedostatků, metodického vedení a nastavení komunikačních vazeb v případě kybernetického incidentu. Poznatky plynoucí z provedeného šetření NBÚ/NCKB dále využijí pro vymezení kritické informační infrastruktury v České republice a pro řízení rizik spojených s jejím provozem a správou.

Dalším úkolem v této oblasti je vytvoření přehledu informačních a komunikačních systémů České republiky, provedení analýzy rizik poskytovaných služeb dodavatelů, kteří nejsou v majetku veřejné správy, a předložení návrhů opatření ke zvládání rizik. Metodika mapování je popsána v Příloze 1 této Zprávy.

Celková databáze důležitých informačních a komunikačních systémů pro fungování státu v českém kyberprostoru je základem pro jejich efektivní zabezpečení. Vzhledem ke skutečnosti, že doposud neexistovala žádná využitelná databáze, se NBÚ rozhodl vytvořit vlastní novou databázi pro potřeby řízení kybernetické informační bezpečnosti a zvládání kybernetických bezpečnostních rizik. Tvorba takové databáze je vzhledem ke své rozsáhlosti a náročnosti zpracování rozdělena na etapy.

Etapy realizace databáze důležitých informačních a komunikačních systémů

Realizace celé databáze je rozdělena do dvou časově navazujících etap.

- Cílem první etapy realizované v roce 2012 je vytvoření databáze důležitých informačních a komunikačních systémů pod **správou veřejnoprávních subjektů**.
- Cílem druhé etapy, která je v plánu na rok 2013, je doplnění databáze o důležité informační a komunikační systémy pod správou **soukromoprávních subjektů**.

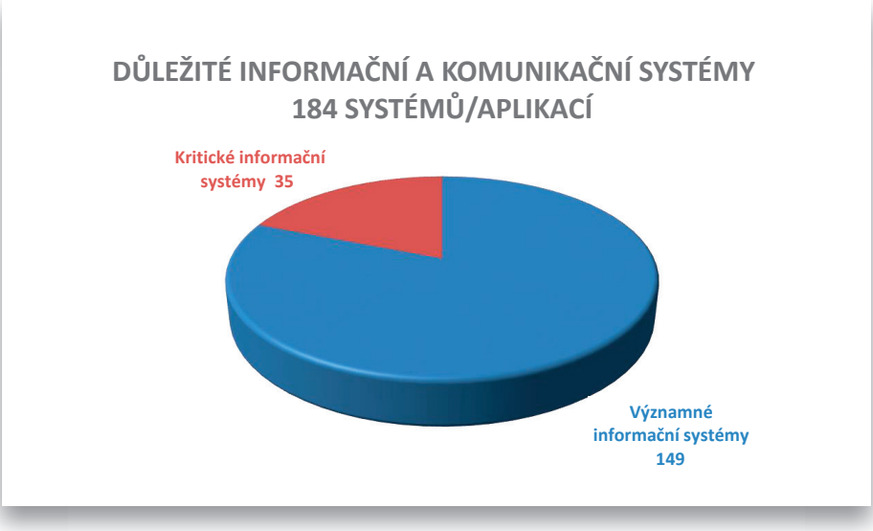
Dopady mapování v první etapě

Přestože zákon o kybernetické bezpečnosti je ve fázi schvalování, NBÚ/NCKB při mapování důležitých informačních a komunikačních systémů spolupracují s budoucími povinnými subjekty. Spolupráce v předstihu je nezbytná pro naplnění podmínek zákona a poskytnutí dostatečného prostoru povinným subjektům připravit se na stav po přijetí zákona. Tato praxe vede k zavádění bezpečnostních politik u povinných subjektů, nastavení komunikačních vazeb a požadavků vyplývajících ze znění zákona o kybernetické bezpečnosti před jeho samotným přijetím. Zároveň tento postup umožní subjektům přípravu bezpečnostních strategií v předstihu, tvorbu analýz rizik a jejich implementaci.

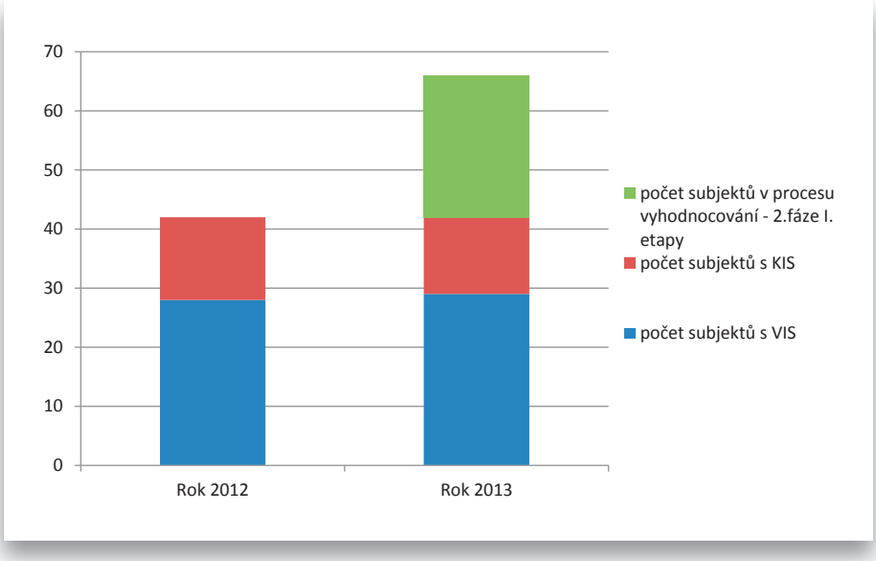
Po vyhodnocení zjištění ze strany NBÚ/NCKB se ukázalo, že subjekty, které mají ve správě důležité informační a komunikační systémy, vnímají důležitost mapování a vyhodnocování. Zároveň dochází ke změně postupů a chování v oblasti zajišťování bezpečnosti. Rovněž bylo vypozorováno, že subjekty se připravují velmi zodpovědně na zavedení zákona, aby zajistily soulad s normami. Byly zaznamenány i změny priorit v bezpečnostních politikách a investicích na základě provedených analýz rizik. Mapování a spolupráce se subjekty tak má přímý a reálný přesah do vnitřního fungování subjektů, což vede ke zvýšení kybernetické bezpečnosti už před přijetím zákona. Tento přesah je jedním z hmatatelných výsledků a vedlejších efektů mapování kritické a významné informační infrastruktury. Kromě již zaznamenaných hmatatelných výsledků a změny v procesech řízení rizik a bezpečnosti je patrné i zvýšené povědomí o kybernetické bezpečnosti v subjektech veřejné správy.

4.1 První etapa

První etapa, zahájená v roce 2012, přinesla poznatky o stavu kybernetické bezpečnosti ve veřejnoprávním sektoru. V průběhu roku 2013 dobíhala první etapa mapování informačních a komunikačních systémů. S ohledem na množství komunikačních a informačních systémů ve správě orgánů veřejné správy je tato činnost řešena dotazníky, které jsou vyhodnocovány pracovníky NCKB. Množství systémů spadajících do kategorie „kritické či významné informační systémy“ v první etapě se pohybuje v řádu stovek.



V současné chvíli NBÚ/NCKB evidují 184 důležitých informačních a komunikačních systémů, které se dále dělí na dvě podskupiny – významné informační systémy, kterých je 149, a kritické informační systémy, kterých je 35. Vzhledem k dobíhajícímu mapování a vyhodnocování orgánů veřejné správy tento počet pravděpodobně nebude konečný.



V roce 2012 bylo vyhodnoceno 44 veřejnoprávních subjektů, kde 28 z nich spravovalo významné informační a komunikační systémy a 14 subjektů kritické informační a komunikační systémy. V roce 2013 bylo osloveno dalších 24 subjektů veřejné správy.

Během poskytování zpětné vazby subjektům po vyhodnocení je přihlíženo mimo jiné k těmto faktorům:

Existence nebo provádění následujících opatření:

- Řízení informační bezpečnosti (PDCA)
- Odpovědnost za bezpečnost informačních a komunikačních systémů
- Existence útvaru provádějícího správu IT/IS
- Program zvyšování bezpečnostního povědomí
- Bezpečnostní politika
- Plán obnovy funkčnosti
- Provedení analýzy rizik nikdy nebo starší dvou let
- Finance na bezpečnost méně než 3 %
- Kalkulace návratnosti investic (ROI)
- Audit informační bezpečnosti
- Zprávy o stavu bezpečnosti subjektu
- Poskytování informací CERT

4.2 Druhá etapa

Druhá etapa se zaměřuje na informační a komunikační systémy soukromoprávních subjektů a subjektů s majetkovou účastí státu. Jedná se o ty systémy, které jsou významné či kritické pro fungování státu, jeho bezpečnost a ekonomické zájmy. Tato etapa byla odstartována v roce 2013, v současné době probíhá oslovování a mapování situace v subjektech spadajících pod kritickou infrastrukturu dle průřezových a odvětvových kritérií pro určení prvku kritické infrastruktury.[2]

Dále NBÚ v roce 2013 uskutečnil společná jednání se všemi dotčenými/povinnými subjekty, na kterých ověřil poskytnuté údaje, zejména v oblasti řízení a zvládání rizik. Partnery jednání jsou ústřední orgány státní správy, pod které spadá krizové řízení dotčených subjektů, zejména Ministerstvo průmyslu a obchodu, Ministerstvo dopravy, Česká národní banka, Ministerstvo zdravotnictví a další. Při této příležitosti NBÚ detailně prezentoval a vysvětloval celkové pojetí řízení informační bezpečnosti, včetně nastavení úzké vzájemné spolupráce v této oblasti. Následně bude po vzájemné dohodě stanoven pro každý subjekt bezpečnostní projekt, tedy konkrétní postup pro zvyšování bezpečnosti důležitých informačních a komunikačních systémů. U subjektů, které dosud neprovedly analýzu rizik nebo nezávislý bezpečnostní audit, bude požadována jejich realizace, aby NBÚ/NCKB co nejdříve stanovily všechna rizika spojená s provozem a správou důležitých informačních a komunikačních systémů a mohly je efektivně řídit.

[2] Příloha k nařízení vlády č. 432/2010 Sb.

5. Budování Národního centra kybernetické bezpečnosti

V současné době probíhají dokončovací práce na budově Národního centra kybernetické bezpečnosti, která bude i sídlem GovCERT.CZ, technického zázemí NCKB. Budova získaná od Ministerstva obrany prošla stavební rekonstrukcí a byla zkolaudována na konci roku 2013. Pracovníci NCKB se do ní nastěhovali v lednu 2014. V mezidobí jsou naplánovány instalace speciálních zařízení a vybavení nezbytných pro výkon GovCERT.CZ. V sídle NCKB budou vybudovány zabezpečené oblasti pro ukládání a zpracovávání utajovaných informací a pro provoz šifrovacích zařízení nutných pro připojení utajovaných sítí. Zároveň je zajišťována konektivita do všech potřebných komunikačních sítí a uzlů. Na problematice související s agendou kybernetické bezpečnosti se kromě zaměstnanců NCKB, kterých je v tuto chvíli 16, podílí nepřímo i další zaměstnanci NBÚ. V průběhu celého roku probíhají výběrová řízení na obsazení pracovních míst, která jsou systemizována pro NCKB. Kapacita pro rok 2013 již byla naplněna a výběrová řízení pro rok 2014 již probíhají.

5.1 Trendy v kybernetické bezpečnosti v roce 2013

V měsíci lednu roku 2013 doznívala masivní kampaň špionážního malwaru označovaného odborníky jako „Red October" (Rudý říjen). Tato kampaň, využívající zranitelnosti softwaru Java od společnosti Oracle nebo zranitelnosti softwaru Microsoft Office, byla zacílena především na východní Evropu, země bývalého sovětského bloku a Střední Asii. Oběti však pocházely z celého světa. Cílem tohoto špionážního malwaru byly převážně diplomatické a státní instituce. Vedle nich se kampaň zaměřila také na výzkumné instituce, energetická a jaderná uskupení, obchodní subjekty a organizace působící v leteckém průmyslu. Konkrétně se jednalo o trojského koně, který umožňoval útočníkům neautorizovaný přístup k napadeným systémům. Na jejich základě pak bylo možné získávat přístupy i do dalších systémů. Z nich byly odcizovány soubory předem vybraných typů. Mezi nimi byly i soubory, které jsou využívány softwarem „Acid Cryptofiler", který využívá např. Evropská unie a NATO. Podle analýzy provedené společností Kaspersky Lab se mezi zasaženými oblastmi objevila i Česká republika, zde se ovšem nepodařilo odhalit oběti útoku. Dle predikcí lze v budoucnu očekávat častější setkávání s podobně sofistikovaným softwarem (Například ve finské vládní síti byl na jaře objeven podobný typ malwaru, který měl za účel zaznamenávat komunikaci mezi Evropskou unií a finským Ministerstvem zahraničních věcí.).

Únor byl zajímavý zejména útoky, které byly opět zaměřeny na zranitelnost okolo softwaru Java od společnosti Oracle. Pracovníci NCKB v tomto období obdrželi varování od belgického CERT týmu, že stanice spadající pod Ministerstvo financí ČR by mohla být napadena trojským koněm, který této zranitelnosti využívá. Na základě spolupráce s administrátorem dotčené sítě se však toto podezření nepodařilo prokázat.

Měsíc březen by podle řešených incidentů bylo možné označit za měsíc DDoS útoků, kdy tyto útoky probíhaly ve třech vlnách a každá s odlišným zaměřením na jinou cílovou skupinu. Cílem první vlny DDoS útoků se stala česká internetová média (idnes.cz, ihned.cz, denik.cz a další). Následující vlna byla zaměřená na český vyhledávací portál seznam.cz. Třetí vlna měla za cíl bankovní instituce.

Období duben až květen bylo relativně klidné, žádný z příchozích typů incidentů výrazně nevyčníval. Vyskytoval se zde např. incident s podvrženými stránkami, kdy členové NCKB na řešení incidentu spolupracovali s operátorem Telefónica CZ. Dále byl zaznamenán případ s nebezpečným kódem na webových stránkách jedné soukromé firmy.

V červnu se řešilo několik různých incidentů, z nichž jeden se týkal mail serveru umístěného na území ČR. Tento server byl využíván pro zasílání phishingu na srílanského telekomunikačního operátora. Vzniklý incident byl vyřešen zrušením služby předplacenému zákazníkovi jejím poskytovatelem. Dále v tomto období proběhl blíže nespecifikovaný útok z IP adresy spadající pod Policejní akademii ČR na poskytovatele VHosting. Rovněž NCKB v tomto měsíci informovalo průmyslové společnosti, které se mohly stát potenciálně napadnutelné vlivem zranitelnosti v systému CoDeSys, který tyto společnosti využívají. Jednalo se především o společnosti poskytující komunikační a síťové služby.

Období prázdnin, červenec až srpen, se vyznačovalo převážně phishingovými útoky na zákazníky České pošty, které probíhají v podstatě až doposud. Poslední vlna byla zaznamenána 7. listopadu. Oddělení NCKB se tyto incidenty snažilo průběžně řešit se zástupci České pošty. Jediným možným řešením však bylo vždy kontaktovat poskytovatele služeb, na kterých se nachází podvržená webová stránka, či odkud jsou odesílány phishingové zprávy. Na základě této komunikace byly tyto služby anonymnímu zákazníkovi zrušeny, popřípadě musel na základě požadavku od poskytovatele tyto stránky sám stáhnout. Během řešení tohoto incidentu byli kontaktováni poskytovatelé z Nizozemska, USA a Ruska. V některých případech byla využita i pomoc spřátelených CSIRT týmů v dotčených zemích. Další řešené incidenty se týkaly počítače spadajícího pod správu ústředního orgánu státní správy a jejich e-mailového serveru, kdy došlo k eskalaci oprávnění[3]. Útočníci po kompromitaci účtu běžného uživatele získali přístup k administrátorskému účtu. Dále se v těchto měsících řešily drobné nákazy webových stránek, případně jiných systémů, malwarem. Systémy většinou vlastnily instituce, které by mohly patřit do kritické informační infrastruktury nebo jsou v oblasti zájmu NCKB.

[3] Více informací v Příloze 2.

V podzimních měsících září, říjnu a listopadu probíhalo dořešení některých incidentů týkajících se ústředních orgánů státní správy a také phishingových útoků na Českou poštu. Ty probíhaly za abnormálně velké frekvence, kdy docházelo během týdne k zablokování stránek a následující den k obnovení této činnosti na jiném serveru a pod jinou doménou. V této době došlo také k rozběhnutí služby Botnet feed, kdy NCKB začalo předávat data administrátorům sítí o IP adresách, které jsou podle námi dostupných dat od společnosti Microsoft začleněny do některého botnetu. Jednalo se převážně o bankovní sektor a subjekty, s nimiž máme navázanou spolupráci.

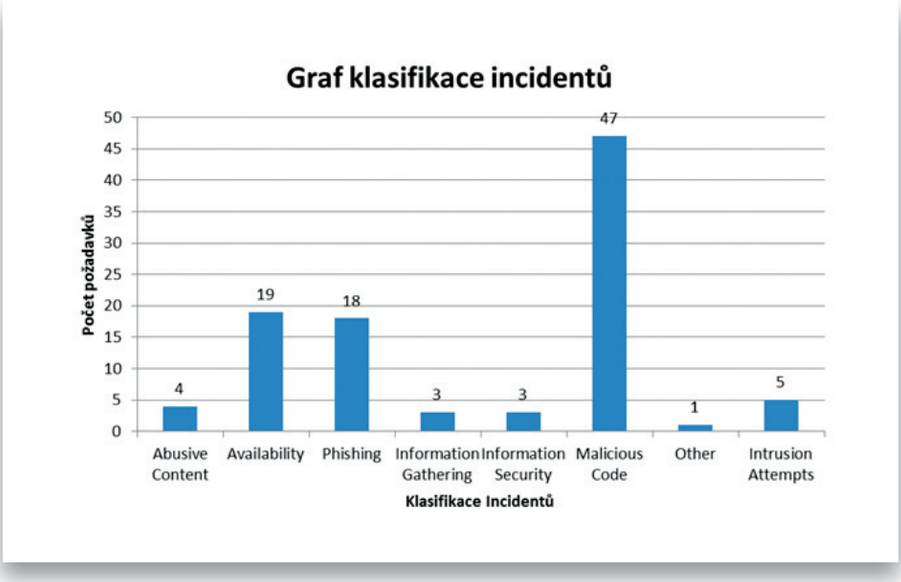
V souhrnu lze říci, že mezi nejčastější typy útoků lze zařadit útoky na bázi sociálního hackingu (např. phishing) a DDoS. Tyto útoky probíhají průběžně po celý rok. Liší se pouze svou intenzitou a napadeným subjektem. Zbylé útoky je spíše doplňují. Většina těchto útoků cílí na státní organizace nebo organizace s velkým počtem zaměstnanců, případně zákazníků, kde je velká pravděpodobnost, že některý z uživatelů vyzradí tajné informace (přístupové údaje), eventuálně se nakazí nebezpečným kódem, který umožní útočníkovi získávat pro něj užitečné informace. Tyto informace lze následně zpeněžit na černém trhu nebo využít je k dalším útokům. V takových případech je proto důležitá osvěta nejenom zaměstnanců, ale i široké veřejnosti. Neméně důležité je také správné sestavení a jedinečnost hesel, aby nedocházelo k případům, kdy uživatel má k dvěma různým účtům stejné heslo. Pro administrátory těchto velkých sítí je naopak užitečné získávat informace týkající se zranitelnosti jimi vytipovaných kritických systémů, přes které by se mohl útočník dostat k informacím na síti.

5.2 Statistika kybernetických incidentů

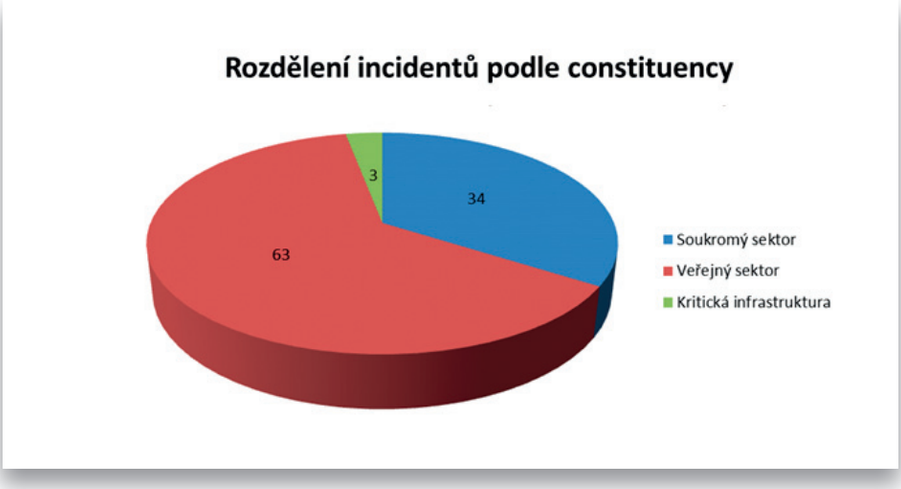
Následný graf zobrazuje počet incidentů, které byly obdrženy a následně zpracovány pracovníky NCKB. Graf znázorňuje počet incidentů obdržených pracovníky vždy za jeden kalendářní měsíc. V grafu nejsou zakresleny údaje za měsíce leden až květen, a to z důvodu přechodu na jinou verzi systému. Incidenty za období leden až květen jsou tudíž zahrnuty do statistiky za měsíc červen.

Z těchto přijatých a zpracovaných incidentů (celkem 100) jich je vyřešených 71 a otevřených 29, viz následující graf.

Další graf zobrazuje podrobnou klasifikaci incidentů podle problematiky, kterou se daný incident zaobíral.



Na následujícím grafu je možné vidět rozřazení incidentů podle zasažené oblasti (constituency):



5.3 Popis vybraných incidentů

Popis vybraných incidentů je uveden v Příloze 2 této Zprávy.

6. Zvyšování povědomí o kybernetické bezpečnosti

NCKB v souladu se svým posláním informuje veřejnost o svém zaměření a aktivitách. Ředitel NCKB poskytl pět velkých rozhovorů na téma kybernetická bezpečnost v České republice internetovým zpravodajským serverům pro širokou i odbornou veřejnost. Další z rozhovorů byl poskytnut čtrnáctideníku Veřejná správa, který je určen veřejnému sektoru. Velký zájem médií o informace od NCKB byl začátkem března při DDoS útocích na některá média, portál seznam.cz a mobilní operátory. Tehdy NCKB plnilo svou funkci koordinátora a přijímalo a poskytovalo relevantní informace. Zástupci NBÚ a NCKB se intenzivně vyjadřovali do všech druhů médií po dobu cca dvou týdnů. Od této doby se na zástupce NCKB média pravidelně obracejí se žádostmi o komentování různých kybernetických témat, čehož NCKB využívá k další osvětě a vzdělávání široké veřejnosti.

Zaměstnanci NCKB také organizovali a účastnili se odborných seminářů a diskusí pro odbornou veřejnost. NCKB v květnu zorganizovalo společně s poslanci Zdeňkem Boháčem a Viktorem Paggiem seminář pro poslance, senátory i širokou veřejnost na téma „Kybernetická bezpečnost v České republice a návrh zákona o kybernetické bezpečnosti“. Na tomto semináři přednášeli významní partneři NCKB, např. zástupce společnosti Microsoft. Dále se NCKB aktivně účastnilo seminářů pořádaných sdruženími CSIRT.CZ a AFCEA, kde pracovníci NBÚ rovněž informovali o aktuálním stavu a o změnách, které budou vyplývat z navrhované legislativy o kybernetické bezpečnosti v České republice.

V říjnu NCKB podpořilo záštitou a prezentacemi mezinárodní kampaň „Evropský měsíc kybernetické bezpečnosti“, kterou vyhlásila Evropská agentura pro síťovou a informační bezpečnost (ENISA), a v České republice organizovalo neziskové sdružení Národní centrum bezpečnějšího internetu. Pracovníci NCKB přednášeli o kybernetické bezpečnosti i na dalších fórech pořádaných např. Českým institutem manažerů informační bezpečnosti, ICT unií a Radou Asociace krajů ČR.

Během čtvrtého čtvrtletí NCKB společně s některými partnery (Národním CSIRTem apod.) začalo plánovat typy a způsoby provedení osvětových a vzdělávacích kampaní na další období.

NCKB na svých internetových stránkách průběžně poskytovalo a poskytuje aktuální informace o událostech z kyberprostoru, o stavu návrhu zákona o kybernetické bezpečnosti a především o zranitelnostech informačních systémů, včetně doporučení jejich řešení a preventivních opatření.

PŘÍLOHA 1

Metodika a způsob provedení mapování důležitých informačních a komunikačních systémů

Pro vytvoření základního přehledu důležitých informačních a komunikačních systémů, tedy technologií pro fungování státu, byla zvolena forma dotazníků rozesílaných na jednotlivé odpovědné subjekty. Tento způsob zjišťování stavu byl vybrán z důvodu snahy minimalizovat finanční a časovou náročnost celého procesu výběru těchto důležitých informačních a komunikačních systémů, prováděného jak NBÚ, tak spolupracujícími subjekty.

Vlastní realizace celé databáze je rozdělena do dvou časově navazujících etap.

Cílem první etapy pro rok 2012 je realizace databáze důležitých informačních a komunikačních systémů pod správou veřejnoprávních subjektů a zjištění úrovně jejich základních bez-pečnostních parametrů, včetně analýzy rizik.

Cílem druhé etapy, která je v plánu na rok 2013, je databáze důležitých informačních a komunikačních systémů pod správou soukromoprávních subjektů a zjištění úrovně jejich základních bezpečnostních parametrů, včetně analýzy rizik.

Důležité informační a komunikační systémy se dělí do dvou kategorií.

Kritická informační infrastruktura: Jedná se o takový systém, který je prvkem sám o sobě nebo je podpůrným prvkem kritické infrastruktury státu naplňující průřezová a odvětvová kritéria podle zákona č. 240/2000 Sb., krizový zákon, ve znění pozdějších předpisů, jehož fungování je pro chod státu nezbytné.

Významné informační systémy jsou takové systémy, které nejsou kritickými informačními a komunikačními systémy, ale u kterých má porušení bezpečnosti informací, tj. důvěrnosti, integrity a dostupnosti, významný dopad na výkon veřejné správy.

Klíčovým parametrem je hodnocení úrovně vyspělosti systému řízení informační bezpečnosti (dále jen „ISMS“ – Information Security Management System) a souvisejících rizik pro důležité informační a komunikační systémy státu prostřednictvím odpovědných subjektů. Pro hodnocení je vytvořena sedmistupňová hodnotící škála.

- Pro kritické informační a komunikační systémy a technologie je požadována minimálně kvalitativní úroveň ISMS 5 – implementovaný ISMS v souladu s normou. V této úrovni řízení ISMS musí být zavedeny procesy, které zajistí provedení analýzy rizik primárních a sekundárních aktiv a realizaci relevantních bezpečnostních opatření, které snižují hodnoty rizik na akceptovatelnou úroveň včetně jejich průběžné optimalizace.

- Pro významné informační a komunikační systémy a technologie je požadována minimálně kvalitativní úroveň ISMS 4 – částečně implementovaný ISMS v souladu s normou. V této úrovni řízení ISMS musí být zavedeny procesy, které zajistí provedení analýzy rizik primárních aktiv a provedení opatření snižujících hodnotu alespoň těch nejvýznamnějších rizik na akceptovatelnou úroveň.

Pro případ, že daný subjekt nemá ještě vypracovanou analýzu rizik pro důležité informační a komunikační systémy a její provedení mu bude nějaký čas trvat, může neprodleně zavést sadu bezpečnostních opatření stanovených zákonem o kybernetické bezpečnosti pro dva stupně regulace, tzn. kritické a významné informační a komunikační systémy a technologie.

Tento metodický postup byl následně schválen Radou pro kybernetickou bezpečnost.

V lednu 2012 byl 44 subjektům rozeslán první dotazník kybernetické bezpečnosti, jehož cílem bylo zejména určení celkového počtu důležitých informačních a komunikačních systémů s připojením do internetu. Obsahoval deset základních evidenčních údajů, jako je název informačního systému (IS), kontaktní údaje na bezpečnostního manažera a správce IS, připojení do komunikační infrastruktury veřejné správy apod. Po vyhodnocení prvního dotazníku byl vytvořen základní přehled o cca 730 informačních systémech, které veřejnoprávní subjekty považovaly za důležité informační a komunikační systémy státu. Tento seznam bohužel obsahoval i systémy, které nebyly důležité pro fungování státu, např. IS Myslivecké a rybářské průkazy, IS Evidence restaurátorů, IS Evidence knihoven apod. Na druhé straně v seznamech u některých subjektů zjevně chyběly jejich kritické systémy podléhající krizovému zákonu. Z těchto zjištění vycházelo zpřesnění původní množiny důležitých informačních a komunikačních systémů, které bylo zahrnuto ve druhém dotazníku kybernetické bezpečnosti. Jednalo se o definování kritických a významných systémů vycházejících z krizového zákona a zákona o ISVS a vypuštění parametru nutného pro připojení těchto systémů do internetu.

V měsíci srpnu 2012 byl rozeslán druhý dotazník kybernetické bezpečnosti, který obsahoval 54 otázek s detailnějším zaměřením na popis vybraných bezpečnostních parametrů. Výsledkem je vytvoření seznamu s celkovým počtem cca 170 důležitých informačních a komunikačních systémů státu. Přibližný počet je uváděn zejména z důvodu různého stupně agregace IS na úrovni hodnocení jednotlivých subjektů, které budou zpřesněny na plánovaných společných jednáních NBÚ a dotčených subjektů v příštím roce.

PŘÍLOHA 2

1. DDoS útoky

Ve dnech 4. až 7. března tohoto roku došlo k tzv. DDoS útokům. Jednalo se o útoky, které probíhaly ve třech vlnách, přičemž každá vlna byla zaměřena na jinou oblast (constituency).

První vlna útoků cílila na česká média (idnes.cz, ihned.cz, denik.cz, živě.cz, mobilmania.cz a další). Zpětně byl oznámen incident na Krajském úřadě Zlínského kraje (KÚZK), kdy se úřad stal obětí vedlejších následků útoku na Českou televizi. Byla zajištěna komunikace mezi dotčenými subjekty a došlo k vysvětlení nastalé události. Ze získaných informací bylo zjištěno, že na KÚZK nestačila kapacita linky.

Tato vlna útoků pokračovala následující den, kdy se útočníci zaměřili na český vyhledávací portál seznam.cz. V závislosti na tomto útoku probíhalo šetření, zda se jej neúčastní počítače ze sítí Masarykovy univerzity (MU) a Národního bezpečnostního úřadu jakožto součásti botnet sítě. Toto šetření proběhlo bez pozitivního nálezu v obou sítích.

Další den došlo ke změně strategie útočníka, kdy místo klasického DDoS útoku začal používat útok DNS Reflection Denial of Service (DRDoS). Cílem těchto útoků se tentokrát stal bankovní sektor, konkrétně Česká spořitelna. Následně byla v závislosti na tomto útoku zřízena videokonference pod záštitou CESNETu, do které byly zapojeny jednotlivé CERTy/CSIRTy a další odborná pracoviště. Největší přínos této konference spočíval v části, kdy se podařilo zapojit odpovědného pracovníka České spořitelny, díky čemuž bylo možné v reálném čase nastavovat pravidla na hraničních routerech CESNETu, čímž byl snížen datový tok směřující na servery České spořitelny o třetinu. Tato praktická zkušenost ukázala nutnost zavedení některých činností, které by mohlo mít v kompetenci NCKB. Po odeznění této druhé vlny byly zpětně nahlášeny incidenty o útocích na ČSOB, Fio banku a ČNB. Získaná data z tohoto útoku byla následně analyzována Vládním CERTem.

Útoky měly pokračování i následujícího dne, kdy se zaměřily na mobilní operátory. Zde bylo využito zkušeností získaných z předchozího dne a bylo provedeno podobné nastavení pravidel na hraničních routerech operátorů. V síti MU byl identifikován závadný provoz spojovaný s útoky, a tak se MU zaměřila na získání malwaru. Pracovníkům MU se tak sice podařilo určit závadnou stanici, výsledná analýza však neprokázala žádný pozitivní nález malwaru.

Na základě informací získaných v průběhu útoků byl v součinnosti s národním CSIRTem a rozhodnutím Rady pro kybernetickou bezpečnost (RKB) vypracován dokument, který by měl objasnit dotčeným subjektům, jak se v nastalé situaci zachovat a zároveň jak usnadnit jejich vzájemnou komunikaci. Tento výsledný dokument se plánuje distribuovat mezi dotčené oblasti (constituency) prostřednictvím sdružení CZ.NIC a NCKB.

2. E-mailový server ústředního orgánu státní správy

Pracovníci GovCERT.CZ obdrželi od ústředního orgánu státní správy hlášení o hackerském útoku, který byl zaznamenán v srpnu 2013. Útok byl cíleně zaměřen na poštovní e-mailový server orgánu.

První fáze útoku není zcela známá. Útočníkovi se s největší pravděpodobností podařilo získat přístupové údaje k některému z účtů uložených v systému. Na základě této znalosti byl útočník schopen si zřídit administrátorský přístup k poštovnímu systému, na kterém je provozován e-mailový systém ústředního orgánu.

Administrátorský účet byl poté zneužit k přístupu k rozhraní pro správu, dále byla zneužita zranitelnost, která umožňuje zadávat příkazy operačnímu systému. Útočník této zranitelnosti využil pro získání informací o systému, stažení a spuštění programu sloužícího k přeposílání dat na určenou IP adresu, vytvoření uživatelského účtu a jeho přidání do skupiny administrátorů. Takto získaný přístup útočník využíval v dalších dnech. Reakcí pracovníků ústředního orgánu státní správy na tento útok byla změna všech administrátorských účtů jak poštovního systému, tak systémových. Dále byly zablokovány nástroje a služby, které útočník použil k provedení útoku. Na síťové úrovni byla zablokována možnost vzdáleného připojení k systému. Na základě analýzy, kterou provedlo pracoviště GovCERT.CZ, byla administrátorům ústředního orgánu státní správy předána doporučení, která by měla vést ke zlepšení bezpečnosti.

3. Incident kompromitace notebooku státní správy

Pracovníci GovCERT.CZ obdrželi prostřednictvím zahraničního partnera informace o zapojení stanice XY [4] do sítě botnet. Ze získaného dokumentu bylo patrné, že stanice XY spadá pod správu ústředního orgánu státní správy a byla zapojena do sítě botnet s řídicím serverem v Hongkongu. Na základě obdržených informací se podařilo pracovníkům GovCERT.CZ získat výpis command and control, který se nacházel na uvedeném řídicím serveru. Ze zmíněného výpisu se podařilo zaměstnancům ústředního orgánu státní správy určit příslušného uživatele. Bylo zjištěno, že zmíněná stanice nespadá pod správu ústředního orgánu státní správy, ale jedná se o soukromý notebook, který byl nakažen škodlivým programem. Na základě dohody mezi orgánem a NBÚ byl umožněn pracovníkům GovCERT.CZ přístup k tomuto počítači a zkopírování zájmových souborů, které objasnily, jak byl počítač napaden.

[4] XY je označení pracovní stanice pro potřeby popisu incidentu

Z výsledné forenzní analýzy provedené pracovištěm GovCERT.CZ byly zjištěny následující poznatky. Počítač naposledy komunikoval s řídicím serverem pravděpodobně koncem srpna 2013 a komunikace neproběhla ze sítě ústředního orgánu státní správy, ale prostřednictvím sítě standardního poskytovatele internetového připojení (pravděpodobně domácí síť). Ze zájmových souborů byla analýzou v uzavřeném prostředí zjištěna přítomnost trojského koně Backdoor/Win32.Swrort. Obecně lze říct, že tento typ trojského koně umožnil vzdálenému útočníkovi zasílání, přijímání, spouštění a mazání souborů, získávání důvěrných dat a logování aktivity na tomto počítači. Ze získaných informací je možné usoudit, že se útočník snažil získat informace o počítači, systémových proměnných, naposledy použitých souborech, síťovém nastavení, spuštěných procesech a službách. Dále byla zjištěna možná spojitost jednoho ze zájmových souborů se souborem US_military_options_in_Syria.pdf.exe. Na základě zjištěných informací, které byly uvedeny ve zpracovaném dokumentu o zpracované forenzní analýze, se domníváme, že začlenění do sítě botnet bylo provedeno pomocí tohoto souboru. Tento soubor mohl být např. součástí phishingového e-mailu, který uživatel obdržel na svůj osobní, případně pracovní e-mail. Z výše uvedeného také usuzujeme, že se nejednalo o cílený útok na pracovníka ústředního orgánu státní správy.