Národní
bezpečnostní
úřad

NBÚ - NCKB novinky 2015

Jaroslav Šmíd

Obsah prezentace

- Zákon o KB
- Bezpečnostní strategie ČR
- Národní strategie kybernetické bezpečnosti ČR na období 2015-20
- Akční plán k Národní strategii KB ČR
- Současný stav určování KII
- Aktivity GovCERT.CZ
- Kybernetické incidenty v období leden-duben 2015

Zákon o kybernetické bezpečnosti
a
jeho prováděcí předpisy

- 181/2014 Sb. – uveden ve Sbírce zákonů dne 29.8.2014, vstup v účinnost 1.1.2015
- 315/2014 Sb. - Nařízení vlády, kterým se mění nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury
- 316/2014 Sb. - Vyhláška o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti (vyhláška o kybernetické bezpečnosti)
- 317/2014 Sb. - Vyhláška o významných informačních systémech a jejich určujících kritériích

Zákon o kybernetické bezpečnosti
-
principy

- Individuální zodpovědnost provozovatele za bezpečnost vlastní sítě (jak zajištění proti útokům zvenčí, tak i zabezpečení proti zneužití k útokům na jiné sítě)
- Rozdělení kyberprostoru na část spravovanou **vládním CERT** (kritická informační infrastruktura definovaná nařízením vlády a významné informační systémy) a **národním CERT**
- Princip technologické neutrality
- Minimalizace zasahování do práv soukromoprávních subjektů
- Princip ochrany informačního sebeurčení člověka

Zákon o kybernetické bezpečnosti

-

pilíře

- Povinnost aplikovat bezpečnostní opatření
  pro správce komunikačních nebo informačních systémů kritické informační infrastruktury
  a pro správce významných informačních systémů

- Povinnost hlásit kybernetické bezpečnostní incidenty

Bezpečnostní strategie České republiky

NBÚ inicioval na podzim 2014 otevření debaty nad aktualizací Bezpečnostní strategie
České republiky. Konkrétně 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 ČR byla dne 21. listopadu 2014 projednána ve Výboru pro koordinaci zahraniční a bezpečnostní politiky Bezpečnostní rady státu, poté schválena Bezpečnostní radou státu a následně 4. února 2015 i Vládou ČR.

Nová Národní strategie kybernetické bezpečnosti 2015 – 2020 (NSKB)

- NSKB připravil NBÚ za pomoci svých partnerů (právní poradci, experti, zainteresovaná ministerstva, Policie ČR, atd.).

- Návrh Strategie prošel meziresortním připomínkovým řízením v průběhu srpna a září 2014 a veškeré připomínky byly úspěšně vypořádány. Strategie byla poté (dne 22. prosince 2014) schválena Bezpečnostní radou státu, 16. února 2015 jí ředitel NBÚ předložil Vládě ČR a kabinet Bohuslava Sobotky jí přijal.

Nová Národní strategie kybernetické bezpečnosti 2015 – 2020 (NSKB)

Hlavní cíle:

- Zajistit efektivitu a posilování všech struktur, procesů a spolupráce při zajišťování kybernetické bezpečnosti
- Aktivní mezinárodní spolupráce
- Spolupráce se soukromým sektorem
- Výzkum a vývoj a jeho podpora
- Podpora vzdělávání a osvěta, rozvoj informační společnosti
- Kybernetická kriminalita - spolupráce s orgány činnými v trestním řízení
- Ochrana národní KII a VIS
- Podíl na právní úpravě pro kybernetickou bezpečnost (národní a mezinárodní úroveň)

Akční plán k Národní strategii kybernetické bezpečnosti na období 2015-20

- Na Strategii následně naváže Akční plán k Národní strategii kybernetické bezpečnosti České republiky na období let 2015 až 2020, na jehož přijetí NBÚ nyní usilovně pracuje, a který již definuje konkrétní kroky, stanovuje u nich zodpovědnost a termíny jejich plnění

- Co se týče samotného procesu přípravy Akčního plánu, NBÚ v rámci pracovních setkání oslovil a následně spolupracoval s mnoha resorty a institucemi. Například s Ministerstvem vnitra bylo do Akčního plánu zapracováno mnoho úkolů, pomocí nichž budou naplněny potřeby Policie ČR pro účinnějším potírání informační kriminality, s Ministerstvem zahraničních věcí byly určeny úkoly v oblasti mezinárodní spolupráce a v neposlední řadě s Ministerstvem obrany byl vymezen postup vytváření a následného zajišťování kybernetické obrany v ČR.

Akční plán k Národní strategii kybernetické bezpečnosti na období 2015-20

- Tímto způsobem byl zpracován návrh Akčního plánu, který byl vložen na začátku března 2015 do meziresortního připomínkového řízení, a jeho vypořádání proběhlo úspěšně se všemi zainteresovanými subjekty, které návrh připomínkovali. Nyní bude Akční plán předložen (15. dubna 2015) na jednání Bezpečnostní rady státu a následně (do konce 2. kvartálu 2015) i vládě ČR

- 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 ČR informována každoročně prostřednictvím Zprávy o stavu kybernetické bezpečnosti v České republice.

Současný stav určování KII

Od 8. 12. 2014 do 10. 4. 2015 proběhlo ohledně určování KII 53 jednání, kterých se účastnili zástupci NCKB. Na základě těchto jednání a následné komunikace se subjekty bylo k 15. 2. k zařazení do KII navrženo 45 informačních/komunikačních systémů, jejichž správci jsou organizační složky státu. Seznam prvků byl 15. 2. předložen MV – GŘ HZS. To vyzvalo subjekty k připomínkování. V následném připomínkovém řízení byl jeden systém prozatím vyřazen a další dva byly přidány (všechny spravuje MV). Proti tomuto byla vznesena jedna zásadní připomínka ze strany jednoho ministerstva, na následném vypořádán nebylo dosaženo souladu a toto ministerstvo o svém dalším postupu neinformovalo nás ani HZS. **Celkem tedy bylo navrženo 46 KII, které byly projednány VCNP (Výbor pro civilní a nouzové plánováni) dne 20. 3. 2015.**

Současný stav určování KII

Správce	Počet systémů	Správce	Počet systémů
ČNB	3	MSp	4
ČSÚ	2	MV	17
ČÚZK	1	MZd	1
MD	2	ÚOOÚ	1
MF	5	ČSSZ	1
MMR	2	MPO	1
MPSV	5	NBÚ	1

Současný stav určování KII

Harmonogram dalšího schvalování:

15. 4. 2015 – Bezpečnostní rada státu

Cca 15. 5. 2015 – Vláda (termín není přesně daný – podle informaci od HZS po projednání BRS bude materiál předložen v nejbližším možném termínu)

Současný stav určování KII

Harmonogram dalšího určování:

1. vlna určování (ústřední orgány státní správy) – dokončena - navrženo 46 systémů – viz výše.

2. vlna určování (ostatní organizační složky státu) – zahájena probíhají sběr informaci a jednání s konkrétními subjekty

3. vlna určování (soukromé subjekty) – zahájena – probíhají jednání – prozatím vytipováno 5 KII u dvou subjektů (Mero a Čepro). Probíhají druhá a třetí kola jednání s telefonními operátory, skupinou ČEZ, plynárnami, bankami apod.

Současný stav určování KII

Současný stav VIS:

Nyní je v příloze vyhlášky uvedeno 92 významných informačních systémů, které spravuje 35 subjektů.

Předpokládána aktualizace seznamu VIS - průběžně jsou identifikovány nové významné informační systémy a některé stávající jsou přeřazeny do kategorie kritické informační infrastruktury (konkrétně se jedná o 15 nových VIS a současně bude 30 stávajících VIS uvedených ve vyhlášce přeřazeno do KII).

U některých dalších subjektů probíhá posuzování jejich systémů z hlediska VIS (např. Česká obchodní inspekce, atd.).

Kontinuálně probíhají jednání s kraji – poskytnuty metodické materiály a podpora. Kraje provádějí analýzu svých systémů ohledně VIS. 21. 4. proběhne jednání se zástupci asociace krajů a bude konzultována jejich analýza – následně bude uskutečněno jednání se zástupci všech krajů ohledně zařazení jejich systémů do VIS.

Aktivity GovCERT.CZ

Na čem se pracuje a co se událo:

Počátkem roku 2015, kdy začal platit nový zákon o kybernetické bezpečnosti, jsme začali dostávat velké množství kontaktní údajů na osoby odpovědné za „Významné Informační Systémy (VIS)“.
S těmito kontaktními údaji, jsme obdrželi další pro nás velmi důležité technické informace. Pro účely shromáždění těchto informací byla vytvořena databáze, kterou jsme nedávno začali těmito daty postupně plnit. V souvislosti se získáváním těchto údajů, jsme subjektům spravujícím VIS, zaslali nabídku námi provozovaných a připravovaných služeb. Většina z oslovených institucí projevila velký zájem o nabízené služby a chtěla je podrobněji prodiskutovat.
Z tohoto důvodu jsme začali jednotlivé zástupce zvát na pracoviště NCKB do Brna na diskuze v technické rovině.

Aktivity GovCERT.CZ

Na čem se pracuje a co se událo:

Dalším hodně řešeným úkolem bylo výběrové řízení, týkající se síťových sond, které by měly být na základě dohod mezi jednotlivými rezorty a Národního bezpečnostního úřadu (NBÚ) umístěny do jejich informačních sítí. V současnosti probíhá příprava pilotního projektu s jedním ministerstvem.

Na počátku roku jsme navázali na úspěšně provedené penetrační testy webových stránek NBÚ. Účelem prvotního penetračního testu bylo zjistit jaké informace je schopen útočník získat z metadat volně stažitelných z webových stránek. V současnosti jsou tyto penetrační testy aplikovány na webové stránky jednotlivých ministerstev. Na základě velkého zájmu oslovených institucí spravujících VIS byla započata technická a právní příprava druhé fáze penetračních testů, která by měla zkoumat zranitelnost webových serverů. V rámci pilotního projektu by měl být otestován webový server Úřadu vlády.

Aktivity GovCERT.CZ

Na čem se pracuje a co se událo:

V rámci proaktivních činností probíhá vývoj nástroje na zpracování dat získávaných od Organizace Shadowserver. Projekt je postaven na základech námi vyvinutého nástroje pro zpracování dat z Botnet Feed, ale z důvodu rozdílnosti zpracovávaných dat je potřeba značných úprav v programu. Co se týče ostatních nástrojů (Botnet Feed a IHAT) využívaných pro proaktivní činnost GovCERT.CZ, tak jsme začali dostávat a reportovat informace týkající se státní správy a VIS.

Kybernetické incidenty v období leden- duben 2015

ČSÚ - DDoS - dne 30. 1. 2015 jsme od Českého statistického úřadu (ČSÚ) obdrželi informace týkající se probíhajících a opakovaných DDoS útoků na webový server czso.cz. První útok na server byl zaznamenán 15. 1. 2015 a trval přibližně dvě hodiny. Další útoky následovaly 19. 1., 23. 1., 24. 1. a 27. 1. Na základě obdržených informací jsme zjistili, že se pravděpodobně nejednalo o cílený útok, který měl za úkol jakkoliv poškodit volby probíhající v nadcházejícím víkendu (31. 1. - 1. 2. 2015), ale jednalo se o chybu v nastavení čínského DNS serveru. Pravděpodobně se jednalo o chybný překlad seznamu předem definovaných domén (torrenty, facebook, twitter) na náhodné IP adresy. Tyto dotazy následně zahlcovaly provozem server czso.cz. Na základě těchto zjištění jsme doporučili určitá řešení. Ta pracovníci ČSÚ konzultovali se správci dotčených serverů, ale vzhledem ke krátké době nezasahovali do nastavení těchto serverů. V současnosti probíhají zátěžové a penetrační testy na novém webu.

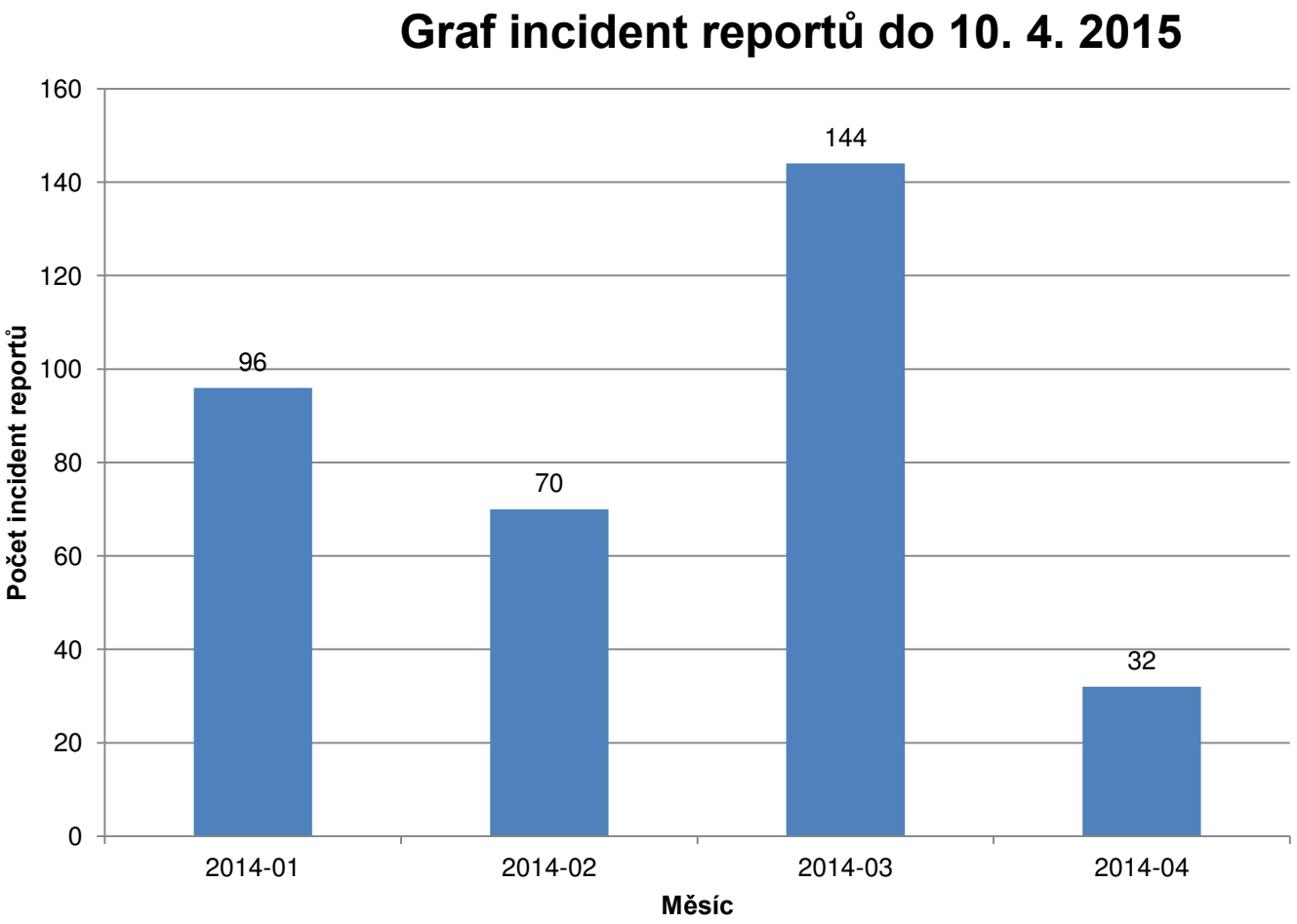
Kybernetické incidenty v období leden- duben 2015

Turla (Uroburos, Snake, Carbon) - od CERT-EU a bezpečnostní společnosti BAE System jsme obdrželi dokument týkající se kompromitovaných IP adres a domén. Mezi nimi byla i česká doména hostovaná v Rusku. Dne 3. 3. jsme od BAE Systems obdrželi doplňující informace, že incident Shortener-Bug attack je ve skutečnosti další instancí špionážního malware Turla (Uroburos, Snake, Carbon). Na základě tohoto zjištění došlo ke sloučení s incidentem #1657. V průběhu řešení incidentu jsme požádali jednotlivá ministerstva o kontrolu síťových logů, zda některá ze stanic v jejich rozsahu nekomunikovala se škodlivými webovými stránkami. Ze 14-ti oslovených ministerstev (23. 2.) jsme doposud obdrželi vyjádření od 8 z nich. Z osmi konečných výsledků hledání bylo nalezeno 9 potenciálně infikovaných stanic. Tři ministerstva ze 14-ti doposud nikdy nereagovala na naše výzvy.

Kybernetické incidenty v období leden- duben 2015

Zranitelnost FREAK - po zveřejnění informací o zranitelnosti FREAK v protokolu TLS/SSL jsme ve spolupráci s Národním CSIRT týmem zahájili skenování serverů státních institucí, které jsou vůči této chybě v zabezpečení zranitelné. V mezidobí jsme obdrželi anonymní e-mail, který nás na tuto skutečnost upozorňoval. Poté jsme rozšířili sken o další zranitelnosti. V souvislosti se zranitelností FREAK bylo nalezeno 107 potenciálně zranitelných serverů a varováno 73 státních institucí.

Kybernetické incidenty v období leden- duben 2015



NCKB – slavnostní otevření 13. května 2014

Národní
bezpečnostní
úřad

nckb@nbu.cz
http://www.govcert.cz/

Děkuji za pozornost.