Vysoká škola ekonomická v Praze
Fakulta informatiky a statistiky

Bakalárska práca

2015 **Dominika Rezníčková**

Vysoká škola ekonomická v Praze
Fakulta informatiky a statistiky

CERT / CSIRT tímy a kybernetická bezpečnosť

Vypracovala: Dominika Rezníčková
Vedúci práce: Ing. Tomáš Klíma
Rok vypracovania: 2015

Čestné prehlásenie:

Prehlasujem, že som túto bakalársku prácu vypracovala samostatne. Všetky použité podklady, z ktorých som čerpala informácie, sú uvedené v zozname použitej literatúry a citované v texte podľa normy ČSN ISO 690.

V..... dňa ..... Podpis: .....

Poďakovanie:

Rada by som poďakovala Ing. Tomášovi Klímovi za odborné vedenie tejto práce a za jeho cenné rady a pripomienky, ktoré mi pomohli behom jej tvorby. Zároveň chcem poďakovať Mgr. Zuzane Duračinskej a Pavlovi Baštovi za osobný rozhovor, ktorý mi poskytli a pomohli mi ním nazrieť do fungovania a významu Národného CSIRT tímu Českej republiky v praktickom ponímaní.

Abstrakt

Cieľom tejto bakalárskej práce je popis súčasnej úlohy národného tímu CERT v oblasti kybernetickej bezpečnosti na základe uvedenia Zákona č.181/2014 Sb., o kybernetickej bezpečnosti do účinnosti a porovnanie teoretických prístupov s ich uplatnením v praxi. Prvá, teoretická časť práce, obsahuje základné informácie o kybernetickej bezpečnosti, kybernetickej kriminalite a bezpečnostných incidentoch a následne sa špecificky zameriava na vznik a vývoj CERT organizácií, ich rolu v oblasti kybernetickej bezpečnosti a bezpečnostných incidentov, funkciu v dnešnej dobe a možnosti vzájomnej spolupráce pracovísk na medzinárodnej úrovni. V druhej časti práce je priestor venovaný analýze Zákona o kybernetickej bezpečnosti a jeho dôsledkov. Konkrétne práca upriamuje pozornosť na funkciu a pole pôsobnosti národného tímu CERT v Českej republike upravenú novoprijatým zákonom. Ďalej práca nazrie do praxe a praktického fungovania národného tímu CERT, prevádzkovaného združením CZ.NIC, vďaka osobnému rozhovoru so zamestnancami tohto centra, vrátane prezentácie konkrétneho príkladu koordinácie riešenia bezpečnostného incidentu. Záverom práce je zhrnutie dosiahnutých výsledkov a prínosu práce v závislosti na nadobudnutých informáciách.

Kľúčové slová

Kybernetická bezpečnosť, bezpečnostný incident, CERT/CSIRT tím, Zákon o kybernetickej bezpečnosti, Národný CSIRT tím Českej republiky CSIRT.CZ.

Abstract

The main goal of this bachelor thesis is to provide brief description of contemporary situation in the field of cyber security and the role of national CERT team in it according to the newly adopted Law no. 181/2014 Coll., on Cyber Security and to make comparison of theoretical principles with their applying in praxis. Thesis is divided into two main parts. First one, a theoretical part, comprehends basic information on cyber security, cybercrime and security incidents and consequently focuses on roles of CERT / CSIRT teams in a perspective of security incidents and cyber security in general, reasons for a formation of the first CERT team and following development, its functions and responsibilities nowadays and finally the thesis presents possible opportunities of collaboration between CERT teams within international organisations and platforms. The second part of the thesis is practical and consists of content analysis of The Law on Cyber Security and its consequences and impacts. The main focus of the thesis is set up on explaining a role of a national team and its sphere of authority in the Czech Republic after the law has entered into force. To provide information about practical operation directly from the source, I will interview two cyber security specialists working in The National CSIRT Team of the Czech Republic called CSIRT.CZ, which is currently operated by the association CZ.NIC. Among other information, I will include a specific example of coordinating activity happened under the auspices of the team during the security incident. As a conclusion of this work is a summary of the achievements and benefits of work depending on the previous foreground and the comparison.

Keywords

Cyber security, security incident, CERT/CSIRT team, The Law on Cyber Security , The National CSIRT Team of the Czech republic CSIRT.CZ.

Obsah

1 Úvod

V rokoch 2001 - 2014 vzrástol počet užívateľov Internetu viac ako 700-krát a momentálne sa odhaduje na viac ako 3 miliardy. [1]

Hoci v dejinách ľudstva sa objavili mnohé prevratné vynálezy a objavy, ktoré zmenili smer jeho vývoja, od objavenia ohňa ešte v praveku, cez vznik kníhtlače a prvej žiarovky, prepojenie prvých počítačových sietí položilo základ fenoménu dnešnej doby a revolučnému nástroju v rukách každého jedného užívateľa – Internetu. Odvtedy uplynuli viac ako štyri dekády a Internet prenikol do každodenného života nielen súkromných užívateľov, ale aj ekonomických podnikov a vládnych orgánov.

Pri množstve výhod, ktoré tieto informačné a komunikačné siete ponúkajú, sa často zabúda na riziká s nimi spojené. S každým novým užívateľom množstvo dát na sieti exponenciálne stúpa a hoci si svoju dátovú stopu bežní užívatelia nemusia ani uvedomovať, otvárajú vďaka nej cestu k získaniu kompromitujúcich údajov o nich samých alebo svojom okolí. S rastom užívateľských dát prístupných cez Internet preto „ruka v ruke“ rastie aj nelegálna aktivita vo forme kybernetickej kriminality a množstvo zaznamenaných bezpečnostných incidentov. Práve preto sa pre nadnárodné korporácie, finančné organizácie či vládne inštitúcie stáva zabezpečenie interných informácií alebo informácií o svojich zákazníkoch a nepreniknuteľnosť počítačovej siete jednými z priorít poslednej doby, či ide o využívanie systému ISMS, alebo vytváranie vlastných bezpečnostných centier v rámci organizácie.

1.1 Téma práce a odôvodnenie výberu

Jednou z ďalších možností, ktoré spoločnosť v prípade zaznamenania bezpečnostného incidentu má, je obrátiť sa na skupiny externe pôsobiace v oblasti kybernetickej bezpečnosti a bezpečnostných incidentov, tzv. CERT / CSIRT tímy. Hoci ich existencia nemusí byť širokému obyvateľstvu známa, hrajú významnú úlohu v zabezpečení siete, príprave na potenciálne napadnutie a častokrát sa stávajú poslednou možnosťou na čo najrýchlejšie vyriešenie, minimalizáciu škôd a opravu problému. V Českej republike pôsobia tieto centrá už pár rokov, ale až začiatkom tohto roku po dlhej príprave vstúpil do účinnosti nový Zákon o kybernetickej bezpečnosti, ktorý sa obsahovo zameriava práve na vymedzenie kompetencií a procesu koordinácie riešenia problémov v oblasti kybernetickej bezpečnosti a vzťahu medzi kritickými a významnými objektmi informačnej infraštruktúry v krajine a centrami CERT / CSIRT, ich povinnosťami a úlohou v oblasti.

S ohľadom na aktuálnosť a možností, ktoré vstup nového zákona do účinnosti ponúka k preskúmaniu, stali sa CERT / CSIRT tímy a ich pôsobenie na vládnej a národnej úrovni v Českej republike hlavnou témou mojej bakalárskej práce.

1.2 Ciele práce a prínos

Primárnym cieľom bakalárskej práce je popis súčasnej úlohy národného tímu CERT v oblasti ochrany kritickej informačnej štruktúry na základe uvedenia Zákona o kybernetickej bezpečnosti do platnosti a porovnanie teoretických prístupov s ich uplatnením v praxi. Na dosiahnutie hlavného cieľa je nutné najskôr venovať pozornosť dosiahnutiu čiastočných cieľov, ktorými sú v prípade tejto bakalárskej práce prvotné uvedenie do problematiky kybernetickej bezpečnosti a bezpečnostných incidentov, teoretické predstavenie CERT/CSIRT tímov v historickej, technickej a funkčnej oblasti, medzinárodných aj národných možností spolupráce, obsahová analýza a vyhodnotenie nového Zákona o kybernetickej bezpečnosti a dôsledky z neho dopadajúce do praxe a nakoniec predstavenie praktického fungovania národného CSIRT tímu, vrátane konkrétneho príkladu koordinácie pri riešení bezpečnostného incidentu, pričom získané informácie sa stanú základom pre porovnanie.

Po úspešnom naplnení všetkých cieľov bakalárskej práce je prínosom pre čitateľa nadobudnutie nových teoretických poznatkov v oblasti kybernetickej bezpečnosti a pochopenie role, ktorú v nej hrajú CERT / CSIRT tímy, porozumenie novo účinného Zákona o kybernetickej bezpečnosti a predstavenie dôsledkov, ktoré z neho vyplývajú a praktická orientácia v tejto problematike, ktorá vysvetlí fungovanie a postupy národného CSIRT tímu pri riešení konkrétneho bezpečnostného incidentu v praxi. Posledným, ale nemenej dôležitým prínosom bakalárskej práce sú výsledky porovnania teoretických informácií s ich presadením v reálnom fungovaní a závery z neho plynúce.

1.3 Štruktúra práce

Bakalárska práca je rozdelená do dvoch častí, teoretickej a praktickej.

Hlavným účelom teoretickej časti je postaviť teoretické základy pre porozumenie problematiky a následnej vlastnej analýze, ktorá patrí k praktickej časti. Preto táto časť obsahuje základné informácie a definície pojmov v oblasti kybernetického priestoru, kybernetickej bezpečnosti, poskytuje úvodné informácie o kybernetickej kriminalite, bezpečnostných incidentov a systéme ich riešenia vo firme. Konkrétne upriami pozornosť na vznik tímu CERT, založeného univerzitou Carnegie Mellon a incidentu s Morrisovým červom. Bližšie rozoberá ich funkciu a pole pôsobnosti v dnešnej dobe, štyri najznámejšie organizácie poskytujúce možnosť vzájomnej medzinárodnej spolupráce v oblasti, legislatívne ošetrenie kybernetickej bezpečnosti na európskej úrovni a nakoniec prezentuje konkrétne návrhy a postupy pri zakladaní CERT tímu. Pozornosť sa následne sústredí na územie Českej republiky, kľúčových orgánov v oblasti kybernetickej bezpečnosti na jej území a legislatívneho rámca, ktorý sa k tejto oblasti vzťahuje.

Druhá časť práce sa potýka s praktickým uplatnením nadobudnutých teoretických znalostí v dvoch smeroch. Prvým je analýza Zákona o kybernetickej bezpečnosti, predstavenie legislatívnych predchodcov tohto zákona, postupu a záštity nad jeho tvorbou, obsahovej zložky a dôsledkov, ktoré prináša, na čo plynule nadväzuje postavenie a funkcia vládneho a národného tímu CERT / CSIRT v Českej republike. Druhým smerom, ktorý je preskúmaný v tejto časti je vlastná analýza fungo-

vania národného CERT tímu, ktorá prebehla ako osobný rozhovor so zamestnancami tímu CSIRT.CZ, prevádzkovaného združením CZ.NIC, ktorý na základe Zákona o kybernetickej bezpečnosti oficiálne preberá funkciu národného centra pre kybernetickú bezpečnosť. V rozhovore sa preberá bežné fungovanie tímu a riešenie nahlásených incidentov, konkrétne prípady, ktoré rezonovali v poslednom období, medzinárodná spolupráca a spolupráca s inými tímami na území Českej republiky a dôsledky pociťované v praxi v súvislosti s novým zákonom. Po získaní a zanalyzovaní všetkých informácií je výstupom práce porovnanie týchto dvoch smerov, teoretického „písaného“ podkladu vytvoreného zákonom a praktického fungovania v praxi.

Záverom práce je zhrnutie dosiahnutých výsledkov a vyvodenie záverov a prínosu práce v závislosti na nadobudnutých informáciách.

1.4 Rešerše

Vďaka povahe bakalárskej práce a aktuálnosti jej témy sa stal mojím hlavným zdrojom informácií z praktického fungovania národného tímu CSIRT.CZ práve osobný rozhovor s Pavlom Baštou a Zuzanou Duračinskou, ktorí pracujú na pozícií špecialistov počítačovej bezpečnosti. Počas rozhovoru (viz Príloha 8) sa vyjadrili k technickému a organizačnému zázemiu pracoviska, formám spolupráce, poskytovaným službám a k procesu návrhu, schvaľovania a následných dopadov Zákona o kybernetickej bezpečnosti na organizácie. Doplňujúce otázky, predovšetkým s technickým zameraním, boli zodpovedané v e-mailovej správe, ktorú je rovnako možné nájsť v prílohách práce (viz Príloha 9). Ostatné informácie a dáta či už k histórií, prebiehajúcim projektom alebo kontaktné údaje boli čerpané z oficiálnej webovej stránky národného tímu CSIRT.CZ, www.csirt.cz.

Teoretickým podkladom pre analýzu a predstavenie fungovania CERT tímov vo všeobecnosti, ich funkcii a spôsobu zakladania, sa stala príručka vydaná európskou organizáciou ENISA, s názvom CSIRT Setting up Guide, ktorá je dostupná aj v českom preklade. Oficiálne postavenie organizácie a univerzálna aplikovateľnosť príručky poskytli príležitosť ju využiť ako kvalitný základ všeobecného predstavenia CERT tímov.

Zdroje v knižnej podobe boli využité pri spracovaní teoretickej časti v oblasti kybernetického priestoru, kybernetickej kriminality a bezpečnosti. Prvá publikácia je dielo Václava Jirovského, Kybernetická kriminalita, ktorá sa v prvej polovici venuje práve vzťahu hrozieb a bezpečnostných incidentov, problematike kybernetického priestoru a kriminality z legislatívneho uhla pohľadu, obtiažnosti právneho definovania oboch pojmov aj legislatívnemu zázemiu ČR, a preto sa jej obsah stal tematickou inšpiráciou a informačným zdrojom teoretickej časti bakalárskej práce.

Druhou je kniha Michala Matějku, Počítačová kriminalita, ktorej obsah v jednoduchej a stručnej forme prináša základné informácie o histórii, vývoji a najčastejších druhoch počítačovej kriminality. Bakalárska práca práve kvôli prívetivosti voči čitateľovi čerpala námet pre historické delenie z nej.

Základom pre terminologický slovník a definície v rámci textu bakalárskej práce sa stal vo väčšine prípadov Výkladový slovník kybernetickej bezpečnosti vo svojej druhej verzii, ktorý vytvorila Policajná akadémia ČR v spolupráci s Českou pobočkou AFCEA.

2 Problematika bezpečnosti kyberpriestoru

V roku 1876, konkrétne ráno 26. januára, sa podarilo siedmim mužom z New York City odísť z banky s viac ako 1,6 miliónom dolárov v hotovosti a cenných papieroch. Išlo dovtedy o historicky najväčšiu bankovú lúpež v dejinách Spojených štátov amerických. Celý incident neprebehol za použitia hrubého násilia, práve naopak, skupina, samozvaná Rufus, prepad detailne plánovala, sledovala okolie banky, získala informácie o bezpečnostnom zabezpečení a rozložení banky. Zatiaľ čo banka, rovnako šerif o prichádzajúcom útoku ani netušili. Uplynulo skoro 150 rokov, banky mnohonásobne zdokonalili svoje zabezpečenie a „zlí chlapci“ prešli od vykopávania podzemných tunelov k omnoho elegantnejšiemu napádaniu počítačovej siete, ale základný princíp sa nezmenil. Pokiaľ organizácia nie je dostatočne pripravená na potenciálny útok a minimalizovanie jeho dopadu, škody môžu byť fatálne. [2]

Aj z tohto príkladu je zrejmé, že mnohé udalosti vo svete sú kľúčovo postavené na komunikácií a výmene informácií. Práve interakcie medzi jednotlivcami alebo skupinami, ich predávanie a zdokonaľovanie dokážu vyústiť vo vývoj celej spoločnosti. Od čias, kedy bolo zdieľanie informácií možné len na fyzickej úrovni, osobne, sa vďaka prepojeniu štyroch univerzitných počítačov v roku 1968 a vzniku siete ARPANET, možnosti rozšírili o dimenziu virtuálneho, kybernetického sveta. Hoci na tejto úrovni nie je možné plne vnímať neverbálnu komunikáciu a jej funkcia bola čiastočne nahradená využívaním emotikon v texte, interaktivita a potlačenie obmedzení v geografickej a časovej oblasti dovolili preniknúť tomuto svetu do nášho reálneho života tak hlboko, že sa kyberpriestor stal prostredím nesúcim všetky rysy dnešnej spoločnosti a spoločenských atribútov, ktorému sa už môže pripísať prívlastok neodmysliteľný. Rovnako ako v realite, tak aj v kybernetickom svete sa nájdu jedinci, ktorí sa riadia svojimi vlastnými pravidlami a čakajú na príležitosť ako využiť neopatrnosti a chyby v systéme. Veľkým motivátorom k páchaniu nelegálnej činnosti je rúško anonymity, ktoré virtuálny priestor poskytuje a komplikuje prenos overených štandardizovaných vyšetrovacích techník a postupov z fyzického sveta do toho kybernetického. Z tohto dôvodu sa posledné roky prikladá zvýšená pozornosť štúdiu kybernetickej kriminality, problematike odhaľovania a vyšetrovania bezpečnostných incidentov v kybernetickom priestore, legislatívnemu ošetreniu takejto nelegálnej činnosti a boja proti nej. [3]

Na začiatku práce je nutné bližšie sa zoznámiť so základnými termínmi a definíciami z oblasti kybernetickej bezpečnosti a kriminality, ktorých pochopenie vytvorí teoretické podklady pre následnú praktickú časť práce a správne porozumenie celej práce a jej cieľov. V tejto kapitole preto upriamim pozornosť v prvom rade na vysvetlenie a definovanie základných pojmov z oblasti, bližšie je v kapitole rozobraný význam slovného spojenia kybernetický priestor a jeho základné vlastnosti. Jedna podkapitola je špeciálne venovaná Internetu, ktorý je považovaný za jednu z najvýraznejších sieti kyberpriestoru. S tak prudkým rozšírením ale vyvstali na povrch aj mnohé otázky ohľadom bezpečnosti jeho užívateľov, preto sa podkapitola venuje aj nebezpečenstvám, ktoré užívateľom hrozia. Takýmto spôsobom práca prenesie pozornosť na kybernetickú kriminalitu a faktory podporujúce nárast zločinnosti práve v kybernetickom priestore, tzv. kriminogénne faktory. Na úvod je stručne podaný historický vývoj kybernetického zločinu rozdelený do troch väčších období, v každom z nich sú okrem najznámejších konkrétnych zločincov a prípadov na záver stručne zhrnuté typické znaky obdobia a trendy. Kapitola následne plynulo nadviaže chápaním kybernetickej kriminality v dnešnej dobe, kde je slovné spojenie nielen zadefinované, ale ná-

sledne sa pomocou najrozšírenejších konkrétnych druhov zločinov kybernetická kriminalita rozdelí na trestnú činnosť páchajú s využitím počítača a trestnú činnosť namierenú proti počítaču. Posledná z troch tém rozoberaných v kapitole je práve kybernetická bezpečnosť, kde je na začiatok nutné pochopiť, čo sa skrýva pod pojmom hrozba. Hrozby sú v kapitole taxonomicky rozdelené do štyroch kategórií. Po stanovení významu kybernetickej bezpečnosti kapitola venuje časť prípadnému narušeniu ochrany v podobe bezpečnostného incidentu a dôležitosti bezpečnostného povedomia medzi zamestnancami. Koniec kapitoly patrí systému zvládania bezpečnostných incidentov v organizáciách a jeho životnému cyklu.

2.1 Kybernetický priestor

Definovanie a určenie hraníc abstraktných pojmov v novo vyvíjajúcich sa disciplínach, ktoré ešte nemajú rokmi zaužívané fráze patrí bez diskusie medzi náročné úlohy. Rovnako to platí aj pre pojem kyberpriestor. Zásluha za vytvorenie originálneho pomenovania cyberspace patrí spisovateľovi Williamovi Gibsonovi, ktorý ho použil a spopularizoval vo svojej knihe s názvom Neuromancer, z roku 1984, v ktorej je opísaný ako „*grafická reprezentácia dát abstrahovaných z bánk všetkých počítačov ľudského systému*. ([3], s.17)“ [3]

Parlament Českej republiky legislatívne vymedzuje definície siedmim pojmom z oblasti kybernetickej bezpečnosti, vrátane kyberpriestoru, v § 2, Zákona č. 181/2014 Sb., o kybernetickej bezpečnosti. [4] Táto práca sa ich znení bude venovať v 4.2.2 venovanej priamo Zákonu o kybernetickej bezpečnosti.

Policajná akadémia ČR a Česká pobočka AFCEA zadefinovali kyberpriestor ako „*digitálne prostredie umožňujúce vznik, spracovanie a výmenu informácií, tvorenú informačnými systémami, a službami a sieťami elektronických komunikácií* ([5], s.59)“. Matějka použil výklad z praktickejšieho uhla pohľadu, kedy je termínom kyberpriestor jednoducho označený „*neidentifikovateľný priestor medzi počítačmi, ... kde sa odohráva všetko dianie na sieti* ([6], s.19)*“*.

Základnými vlastnosťami kyberpriestoru sú virtuálnosť a vzájomné pôsobenie, interakcia, postavená na sieťovom prepojení zariadení. Virtuálna povaha súvisí s nezávislosťou na konkrétnom čase a mieste, to znamená, že účastníci interakcie sa nemusia stretnúť na tom istom mieste, v tom istom čase za účelom komunikácie. Na druhej strane, je kyberpriestor limitovaný nutnosťou pripojenia k Internetu alebo inej sieti a pri jeho výpadku sa zároveň stráca možnosť interakcie. Tá je kvalifikovaná ako činiteľom úmyselne vykonaná činnosť, ktorá vedie k prevedeniu reakcie na strane prijímateľa, pričom nemusí ísť nevyhnutne o fyzickú činnosť prijímateľa voči činiteľovi v podobe odpísania správy na klávesnici. V prípade interakcie s prístrojom alebo zariadením je postačujúca reakcia v podobe spätnej väzby softwaru alebo odpovede na základe prijatého podnetu. [7]

2.1.1 Internet

Mnohým bežným užívateľom sa môže zdať, že kyberpriestor a Internet sú synonymá. Nie je však tomu tak. Kyberpriestor je vnímaný ako globálne komunikačné médium, priestor, spájajúci počítače vo virtuálny svet. A v tomto svete ako širokej verejnosti najznámejšia sieť figuruje Internet, nazývaný aj „*sieťou sietí* ([8], s.14)“ alebo „*matkou všetkých sietí* [9]“.

Internet Solange Ghernaouti-Helie definuje v svojej knihe ako „*verejne dostupnú počítačovú sieť spájajúcu mnoho sietí z celého sveta za účelom elektrickej výmeny dát (* [10]*, s.435)*“. Okrem Internetu sa v tomto svete nachádzajú diametrálne odlišne charakterizované siete, napríklad intranet, ktorého základnou vlastnosťou je privátnosť v rámci organizácie alebo spoločnosti a obyčajne sú izolované od Internetu programovou ochranou, tzv. firewall. [10]

Už na základe tohto príkladu je zrejmé, že pojmy Internet a kyberpriestor spolu úzko súvisia, ale nedajú sa ľubovoľne zamieňať alebo pokladať za totožné. Internet je súčasťou kybernetického sveta, postavený na vzájomnej komunikácií počítačov na základe skupiny protokolov TCP/IP. [8]

Užívatelia Internetu a hrozby na nich pôsobiace

Vývoj technológií, čoraz výraznejšie zjednodušenie ich ovládania a využitie nových procesov a ich uplatnenie v praktickom živote spôsobili masové rozšírenie po celom svete, Internet, sa dá považovať za fenomén dnešnej doby. Natoľko, že na základe práce španielskeho sociológa Manuella Castellsa, vznikol nový myšlienkový prúd, ktorý sleduje práve prepojenie technológií so spoločnosťou a mnohí odborníci ho považujú za jeden z kľúčových prúdov pri sledovaní správania sa a myslenia novodobej spoločnosti. Dôležitým faktorom umožňujúcim hromadné používanie Internetu, je jeho otvorenosť. Vlastnosť, ktorá dovoľuje každému, kto spĺňa základné vstupné kritéria, stať sa súčasťou siete, jej užívateľom, získavať a prezentovať ľubovoľné informácie. [3]

Užívateľom sa podľa Krátkeho slovníka slovenského jazyka nazýva osoba, spotrebiteľ alebo konzument, ktorá „*má niečo v užívaní* [11]“.

Od dôb vzniku siete ARPANET, s ktorou pracovali len špecializovaní a odborne poverení vedci a technici, sa súčasné spektrum užívateľov kvantitatívne zmenilo a Internet prenikol do každodenného života bežných ľudí. Od vyhľadávania rôznorodých informácií cez webové stránky Google, skontaktovanie potenciálneho zamestnávateľa skrz platformu LinkedIn či nákupu tovaru pomocou obchodného a aukčného internetového portálu Ebay.

Pocit anonymity a bezpečia z nej vyplývajúci, ktorý tento kyberpriestor ponúka vďaka svojej technickej zložitosti a neosobnej komunikácií, sa stali jedným zo stimulov pre vznik unikátneho javu tohto desaťročia zvaného sociálne siete. Užívatelia sú odbremenení od geografických a časových obmedzení reálneho sveta, môžu komunikovať a interaktovať bez ohľadu na časové pásmo či lokalitu, v ktorej sa nachádzajú. Vystupovanie pod internetovým avatarom im poskytuje slobodnú možnosť prezentácie svojich názorov, väčšiu dávku sebadôvery a otvorenosti. Takýto prístup podnecuje socializáciu a začleňovanie sa jednotlivcov do skupín a subkultúr, v ktorých zdieľajú spoločné presvedčenie a záujmy či už ide o diskusné fóra a chatovacie miestnosti, alebo spomínané sociálne siete. [3]

Na druhej strane, ukrývanie sa za užívateľský profil dovoľuje manipulovať a upravovať informácie, ktoré užívateľ poskytuje podľa jeho predstáv a neraz zavádzajúco. Takáto forma vytvorenia vymysleného užívateľského profilu za účelom nadviazania kontaktu s inou osobou, častokrát romantického charakteru, sa v bežnej internetovej praxi nazýva „*catfishing* [12]*"*. Pokiaľ je primárnym cieľom zisk osobných údajov alebo iných kritických informácií, ide o jednu z techník sociálneho inžinierstva. Človek je totiž vo svete informačnej a komunikačnej bezpečnosti považovaný za najslabší článok. Prípady, v ktorých bol zamestnanec konkrétne napadnutej firmy vedome či nevedome zodpovedný za takýto útok, tvorili v USA za posledné roky 94% z celkového počtu a len ostatných 6% boli kybernetický útočníci, ktorí pochádzali mimo prostredia organizácie. [3] Rôzne metódy manipulácie s ľuďmi s cieľom získania prístupových informácií a jeho digitálnej identity sa súhrnne nazývajú sociálne inžinierstvo.

Ďalšou z hrozieb, ktoré so sebou prináša „život on-line" je premietanie virtuálnej reality do tej skutočnej, pretože ľudská psychika a sociálne správanie sa je výrazne ovplyvnené dianím na sieti. Život v nej sa môže stať pre užívateľa atraktívnym v takej miere, že pri jeho nedostatku začne pociťovať pocity úzkosti a smútku, ktoré sa nevytratia, kým sa k nej opäť nevráti. Podľa výskumu lekárskej fakulty Stanfordskej univerzity, ktorý prebehol pod vedením Elias Aboujaoude, MD, až 13,7% respondentov považovalo vzdať sa prístupu na Internet po dobu niekoľkých dní za ťažké a 8,2% pociťovalo úľavu a príjemné pocity pri používaní Internetu. [13] Spolu s ostatnými príznakmi ako sú prioritizácia virtuálnej reality, neustále zvyšovanie času stráveného na sieti a konflikty s okolím súvisiace s trávením času na Internete môžu viesť k závislosti, ktorá sa nazýva netholizmus. V európskych krajinách ako Švédsko alebo Rakúsko ňou trpí približne 0,6% užívateľov Internetu, čo je pre porovnanie o jednu tretinu väčšie číslo ako počet ľudí závislých na heroíne. [3]

2.2 Kybernetická kriminalita

Popri psychologických hrozbách a hrozbách sociálneho inžinierstva spomenutých v predchádzajúcej kapitole, ktorým sa užívatelia Internetu vystavujú, je svet kyberpriestoru plný iných nástrah majúcich technický charakter, ktorým môže koncový užívateľ poslúžiť ako ľahká obeť a zdroj citlivých informácií slúžiacich ako vstupná brána do inak bezpečne chráneného informačného systému. Benevolentnosť pri vstupe do siete a demokratičnosť v jej užívaní má totiž bez hraničných obmedzení a kontroly za následok tendencie k anarchii alebo jej nelegálnemu zneužitiu. Samotná zložitosť informačných systémov a technológií sa môže zdať nedobytnou, ale zároveň sa javí ako výzva pre páchateľov nelegálnej činnosti, ktorí chybu v systéme dokážu využiť vo svoj prospech. Množstvo dát, ktoré sa pohybuje a ukladá v celosvetovom prostredí je nemožné neustále a jednotlivo kontrolovať a v kombinácií s dôverou, ktorú užívatelia vkladajú do týchto systémov je pre zločincov jednoduché zostať po dlhšiu dobu nepovšimnutí. Ani prípadné odhalenie protiprávneho jednania nezaručuje dopadnutie samotného zločinca skrývajúceho za obrazovkou počítača, v anonymite. Celosvetové rozšírenie a „*deteritorializácia* ([3], s.35)" kyberpriestoru komplikuje lokalizáciu. Obtiažnosť výkladu a aplikácie legislatívy upravujúcej oblasti IT zase umožňuje využiť medzery v zákonoch a globálnosť siete dovoľuje kolidovať jednotlivým jurisdik-

ciám a štátnym správam. Vymenované činitele sa považujú za základné kriminogénne faktory uľahčujúce alebo vedúce ku kybernetickej kriminalite. [6]

2.2.1 História počítačovej kriminality

Viaceré zdroje vnímajú vývoj počítačovej kriminality odlišne a rozdeľujú ho do etáp na základe desaťročí alebo podľa svojho uváženia významných míľnikov. V tejto kapitole sa práca bude pridržiavať prehľadného a jednoduchého členenia o troch obdobiach, ktoré uviedol Matějka v knihe Počítačová kriminalita.

Prvé obdobie je nazvané pravekom a trvá do roku 1981, kedy sa na komerčný trh dostal prvý počítač. Názov trefne popisuje počiatky éry počítačového zločinu. S nadhľadom sa dá za prvý takýto zločin označiť prípad z roku 1801, kedy zamestnanci zo strachu pracovného miesta sabotovali vývoj zariadenia umožňujúceho automatizáciu niektorých tkacích činností. Do vzniku prvého elektronického počítača pomenovaného ENIAC, 14. februára 1946, ubehlo takmer 150 rokov. Začala počítačová éra. V tomto období rovnako vzniklo aj pomenovanie hacker, ktoré však označovalo programátorov snažiacich sa o pozitívnu, hoci svojpomocnú úpravu programu, pretože neexistovala žiadna technická podpora, akú poznáme dnes. Modifikáciu s úmyslom vlastného prospechu využil Abbie Hoffman v roku 1971, aby uskutočňoval hovory zdarma. V 70. rokoch v dôsledku zvýšenej dostupnosti kazetového magnetofónu do domácností sa začali prvýkrát kopírovať a distribuovať nahrávky porušujúce autorské právo s následným masovým rozšírením pri rozvoji Internetu. [6]

Druhou stranou mince boli zločiny páchané na počítačoch a ich sabotáže. Už v roku 1969 študenti v Kanade pri proteste zničili techniku a počítačové dáta patriace univerzite. Incidenty fyzického ničenia počítačových systémov boli najbežnejšími zo zločinov v tak skorej dobe, ale úplne sa nevytratili dodnes. [14]

Obdobie stredoveku počítačovej kriminality začína nástupom prvého osobného počítača značky IBM PC 5150 na trh a končí v roku 1994 známym prípadom Citibank. Medzitým film War Games o mladom hackerovi spopularizoval toto prostredie a časopis Phrack pravidelne informoval o trikoch a možnostiach obchádzania systému. Legion of Doom, ktorí dokázali presmerovať telefonáty smerujúce ku kurátorovi Palm Beach na sexuálnu linku, sa stali legendou doby a podnietili záujem počítačovej polície. V roku 1988 sa objavil v počítačovej sieti nový typ napadnutia, prieniku do siete za využitia cielenej infekcie, internetový červ. Ten prvý nesie meno Morrisov červ, po Robertovi Morrisovi, ktorý ho vytvoril. Stal sa zároveň impulzom pre vznik prvého bezpečnostného tímu CERT. Časom prišla zmena primárneho cieľu zo získania slávy na zisk peňazí, ktorá sa premietla do profesionalizácie kybernetických zločincov. Prevod 10 miliónov dolárov z účtov banky Citibank na konto ruskej hackerskej skupiny pod vedením Vladimíra Levina znamenal koniec éry stredoveku. [6] Počítačové zločiny páchané predovšetkým nadšencami alebo jednotlivými zamestnancami zneužívajúcimi svoje postavenie boli nahradené organizovaným zločinom typickým systematickou a cielenou prípravou, špeciálne so zameraním na finančné systémy a inštitúcie. [14]

Začalo obdobie počítačového novoveku, datované od roku 1994 dodnes, typické masovým rozšírením osobných počítačov a mobilných zariadení, elektronickej pošty, Internetu a prostredia World

Wide Web, ktoré zároveň priniesli nové možnosti zneužitia na špionážne účely či vzostup internetových vírusov. Kontinuálne s rastom počtu užívateľov elektronickej pošty koncom 90. rokov prudko vzrástol počet nechcených, spamových, ale aj podvodných e-mailov či e-mailov infikovaných vírusom. Vírusu Melissa v roku 1999 stačilo pár hodín k celosvetovému rozšíreniu vďaka samopreposielaniu sa prvým 50 kontaktom v e-mailovom adresári. V roku 2000 sa objavila prvá sieť P2P v programe Napster, ktorý dovoľoval užívateľom medzi sebou zdieľať hudobné nahrávky. Americký súd svojím verdiktom o zablokovaní tohto programu vytvoril precedens, na základe ktorého je aj samotný potenciál programu k zneužitiu pri porušovaní autorských práv ich porušením, hoci za obsah zodpovedajú užívatelia sami. Podobných stránok a programov však pribúdalo a nastala „*zlatá éra počítačového pirátstva* ([6], s.41)“. [6]

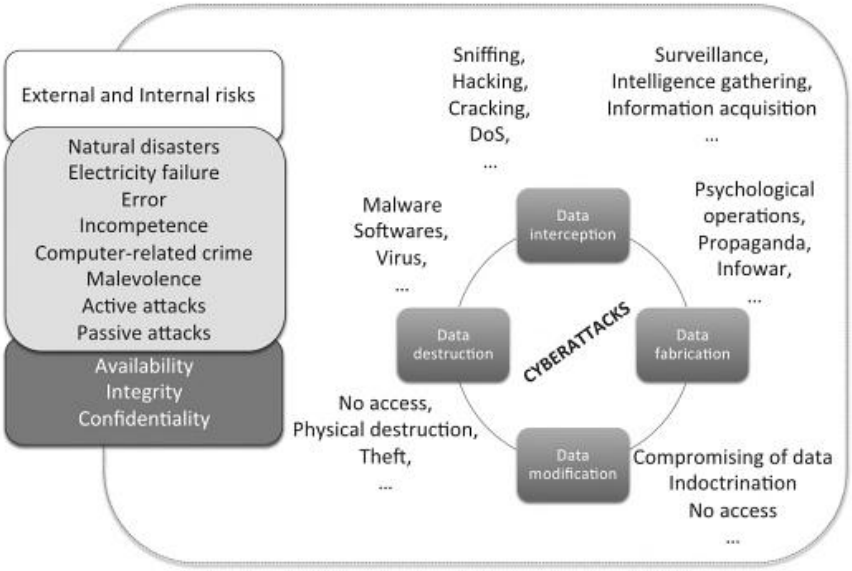
Začiatok nového milénia sa niesol v znamení špecializácie útokov na bankové a finančné inštitúcie a kreditné karty užívateľov platiacich za služby a tovar on-line. Medzi rokmi 2005 a 2007 sa podarilo Albertovi Gonzalezovi preniknúť do databáz amerického reťazca TJX vlastniaceho TJ Maxx a získať tak informácie o viac ako 45 miliónoch kreditných kárt svojich užívateľov, čo podnietilo vývoj bezpečnejšieho systému. Útoky prestávajú byť ničivé vo fyzickom slova zmysle, trendom sa stalo infiltrovanie a penetrácia systému zvnútra a jeho následné narušenie. [15]

2.2.2 Kybernetická kriminalita dnes

Kybernetická kriminalita očividne patrí k oblastiam, ktoré v čase výrazne podliehajú rýchlo sa meniacim trendom a novým kreatívnym možnostiam a prístupom kriminálnej činnosti, a preto je ťažké určiť jej konkrétne hranice. Vysvetlenie pojmu kybernetická kriminalita ako ho vníma Policajná akadémia ČR a Česká pobočka AFCEA sa nachádza vo Výkladovom slovníku kybernetickej bezpečnosti, ktorý za kybernetickú kriminalitu považuje „*trestnú činnosť, v ktorej figuruje určitým spôsobom počítač ako súhrn technického a programového vybavenia (vrátane dát) alebo iba niektorá z jeho komponent, prípadne väčšie množstvo počítačov samostatných alebo prepojených do počítačovej siete a to buď ako predmet záujmu tejto trestnej činnosti ... alebo ako nástroj trestnej činnosti* ([5], s.57)“.

Predmetom záujmu sa v tomto kontexte rozumie určenie počítača ako primárneho cieľa útoku, zväčša vo forme preniknutia do jeho systémov s úmyslom vykonania nelegálnej činnosti. Typickým príkladom je priemyselná špionáž, kedy je počítačový systém infikovaný vírusom alebo napadnutý hackerom v reálnom čase. V oboch prípadoch je zámerom útočníka prístup k interným, kreditným či inak citlivým informáciám a dátam s ich následným zneužitím. Hacking, prelomenie bezpečnostnej ochrany a infiltrácia počítačového systému, ako je zrejmé z predchádzajúcej kapitoly o histórií kybernetickej kriminality, je stabilnou a rozšírenou súčasťou zločinnej činnosti, hoci častokrát variuje v účele jeho prevedenia. Násilným hackingom sa rozumie osobný útok na držiteľa prístupových informácií, ktorý ho donúti tieto informácie vydať. Carding pomenúva zneužitie údajov o platobnej karte, ktoré boli získané nelegálnou trestnou činnosťou. Zisk osobných údajov môže viesť ku krádeži identity. Niekedy stačí na spôsobenie škody dáta hackerom vymazať či zmeniť, čím sa poškodí kredibilita a dobré meno spoločnosti. [6]

Potenciálne problémy nastávajúce pri používaní Internetu, vo forme vonkajších aj vnútorných rizík sú zachytené na ľavou stranou nasledujúceho obrázku (viz Obrázok 1). Príkladmi takýchto rizík sú práve skutočnosti zapísané v sivom rámčeku, ako neovplyvniteľné prírodné katastrofy, zlyhanie elektrickej siete alebo cielené počítačové zločiny a aktívne útoky. V centre obrázka sú zobrazené niektoré z tých najznámejších kybernetických útokov a ich dopad na dáta v počítačovej sieti, na ktoré útočia. Vyššie spomenutá už bola zmena dát (data modification) či ich kompletné zničenie a vymazanie (data destruction). Ďalšími možnosťami sú zachytávanie, respektíve odpočúvanie dát (data interception) a tvorba fiktívnych dát (data fabrication). Podľa autorky obrázka, Solange Helie sa pri dodržiavaní troch zásad tieto bezpečnostné riziká zmenšujú. Sú nimi dostupnosť, integrita a dôvernosť. [10]



Obrázok 1: Rôznorodosť kybernetických útokov a ich dopad na dáta (Zdroj: [10], s.45)

V pozícii nástroja trestnej činnosti figuruje počítač pri nelegálnom sťahovaní a šírení softwaru, nahrávok, filmov či iných médií, kedy páchateľ jeho prostredníctvom porušuje autorské práva. Pre osobu zodpovednú za prelomenie vstavanej ochrany proti kopírovaniu sa používa pomenovanie cracker a diela, ktoré vznikli za takýchto podmienok sa označujú ako warez. Počítač ako médium a jeho rozšírenie v radách bežných užívateľov poskytlo príležitosť podvodníkom zmodernizovať svoje stratégie. Podvodné on-line obchody, fiktívne stránky ponúkajúce sexuálne služby za poplatky či v skutočnosti neexistujúce obchody s komoditami alebo menami, sú spôsobom zisku priamo finančného obnosu alebo platobných informácií. Vďaka kvalitným grafickým programom je taktiež uľahčené falšovanie bankoviek alebo cenných papierov. Anonymný kontakt s koncovým užívateľom, ako jeden z kriminogénnych faktorov, má významnú úlohu pri trestnej činnosti typu kybernetická šikana, elektronické vydieranie alebo podpora a propagovanie extrémistických skupín. [6] V prípade útoku alebo ovládnutia počítačovej sieť a informácií, ktoré obsahuje, s plánom vydierať alebo zastrašovať užívateľov, správcu siete alebo vládu za účelom vyžiadania si ich podpory v politických alebo iných cieľoch sa jedná o kyberterorizmus a je rovnako považovaný za trestnú činnosť. [3]

2.3 Kybernetická bezpečnosť

Dejiny ukázali, že samotný vznik a vývin kybernetickej bezpečnosti je podmienený hlavne nachádzaním a zneužívaním bezpečnostných nedostatkov v systéme. A zároveň vylepšenie zabezpečenia automaticky prekladá novú výzvu zločincom, ktorý ho chcú prekonať. Vďaka tomuto cyklu sa kybernetická kriminalita stala sofistikovanou natoľko, že sa zdá nemožné takýmto napadnutiam zabrániť. [15]

2.3.1 Hrozby v kybernetickom priestore a ich taxonómia

Napriek tomuto trendu však stále platí, že zdokonaľovaním a vylepšovaním ochrany informačných systémov v spoločnosti je možné pravdepodobnosť vydareného útoku aspoň zmenšiť. Hrozba predstavuje čokoľvek, čo eventuálne vytvára príležitosť na narušenie systému a môže mať za následok zmenu dát, ich vymazanie alebo iné z dôsledkov, ktoré poškodzujú systém alebo samotnú organizáciu a jej chod. Nie sú to len fyzické osoby, ale aj myšlienky, aktivita alebo technické prostriedky umožňujúce vykonať útok. Útokom sa následne rozumie samotná realizácia hrozby. Podľa Jirovského taxonómie hrozieb v oblasti informačného systému a jeho bezpečnosti existujú štyri základné druhy hrozieb [3]:

1. Neoprávnený prístup – zisk prístupových informácií subjektom bez oprávnenia k nim s následnou možnosťou ich zneužitia.
2. Neoprávnené zmeny – subjekt bez oprávnenia vytvorí nekonzistentné dáta vymazaním alebo zmenou pôvodných súborov alebo vytvorením nových.
3. Neoprávnené použitie – využitie zdroja subjektom bez oprávnenia alebo využitie neschváleným spôsobom narušujúce dôveryhodnosť zdroja.
4. Neoprávnené potláčanie dostupnosti – oprávnenému subjektu je odoprené právo k službe z dôvodu preťaženia systému požiadavkami subjektu alebo viacerých subjektov bez oprávnenia.

K svojej realizácií ale potrebujú byť aktivované pomocou takzvaných aktivačných hrozieb. Tie predstavujú možnosti a cesty subjektu k získaniu, zaznamenávaniu a sledovaniu dôverných informácií, umožňujúcich prevedenie niektorej z hrozieb základných. Existujú dva spôsoby, ktorým informácie získavajú. Môžu byť spočiatku nečinnou súčasťou nainštalovaného softwaru a až po určitej vopred naprogramovanej dobe alebo po priamom aktivovaní od autora je uvedený do činnosti škodiacej systému. Príkladom je trójsky kôň ako jedna z najklasickejších implantovaných hrozieb alebo zadné vrátka slúžiace k obchádzaniu bezpečnostnej ochrany systému pri použití špecifického vstupného reťazca. Druhým spôsobom je priama penetrácia systému s využitím maškarády, klamlivého vydávania sa za odlišný subjekt a privlastnenia si jeho výsad a prístupov, s objavením a využitím zraniteľného miesta systémovej ochrany a z toho vyplývajúcim obídením identifikácie subjektu potrebnej k využitiu jeho prístupov a s použitím platného, povoleného prístupu za účelom, pre ktoré nebol pridelený a nie je v súlade s bezpečnostnými predpismi. V takomto prípade prichádza hrozba zvnútra organizácie a je o to náročnejšie sa proti nej brániť. Bežne sa ale stáva, že aktivačné hrozby vedú, resp. môžu viesť k uskutočneniu viacerých základných hrozieb, pričom v takejto situácií sa im hovorí podkladové hrozby. [3]

Môže sa zdať, že väčšina hrozieb prichádza s úmyslom poškodiť informačný a komunikačný systém organizácie, ale pravdou je, že minimálne 50% prípadov je neúmyselných. Kľúčovým faktorom je v takýchto situáciách ľudský činiteľ, ktorého aktivita sa vďaka jeho nepozornosti, nevedomosti alebo nepresnému dodržiavaniu stanovených predpisov stáva pre systém hrozbou. [16]

2.3.2 Definovanie kybernetickej bezpečnosti

Ako je z predchádzajúcich kapitol tejto práce zrejmé, za útokom môžu stať najrôznejšie faktory, útočník môže mať najrôznejšie pohnútky a ciele a môže zvoliť najrôznejšie cesty k ich dosiahnutiu. Organizácia nevie kedy a ako budú jej informačné systémy narušené, aké škody a následky takýto útok prinesie a ako rýchlo sa ich podarí neutralizovať. Čo je jedinou stabilnou premennou v spleti neznámych faktorov, je potreba bezpečnostnej ochrany.

V kontexte kybernetického priestoru na zabezpečenie jeho ochrany a ochrany informácií v ňom sa nachádzajúcich slúži „*súhrn právnych, organizačných, technických a vzdelávacích prostriedkov* ([5], s.57)“, označovaný ako kybernetická bezpečnosť. Jej cieľom je zaistiť ochranu z troch časových hľadísk voči času útoku [16]:

- Pred útokom – systém ochrany má v tejto fáze preventívnu funkciu a pomocou automatizovaných nastavení, ako je napríklad odhlásenie zo systému pri nečinnosti prihláseného subjektu znižuje riziko napadnutia a hrozby.
- Počas útoku – v tomto momente je najdôležitejšie včasné zachytenie problému, určenie jeho povahy a rozsahu hrozby, kedy je najefektívnejšou cestou pravidelná kontrola upozorňujúca príslušné autority na akékoľvek podozrivé zmeny a nezrovnalosti v systéme.
- Po útoku – po spozorovaní napadnutia systému je nutné čo najrýchlejšie odstrániť zdroj problému zo systému a znížiť tak potenciálny rozsah škôd na minimum.

Prvotné finančné investície do vytvorenia a implementovania prostriedkov ochrany vo veľkých či malých organizáciách sú na začiatku projektu vysoké a tieto náklady sa nevrátia okamžite, ani v krátkom časovom horizonte. Je potrebné si uvedomiť, že eventuálne spôsobené škody vyjadrené vo finančných jednotkách a náklady na opravu a obnovu informačného systému však môžu byť ešte vyššie. [16]

2.3.3 Bezpečnostný incident

Aj tá najlepšia a najmodernejšia ochrana je ale málokedy stopercentná a obyčajne obsahuje zraniteľné miesta, slabiny, ktoré predstavujú príležitosť na jej prelomenie. Riziko úspešného napadnutia takéhoto miesta ochrany a následne systému sa zvyšuje priamo úmerne s množstvom a hodnotou chránených informácií a pravdepodobnosťou úspechu plánovaného útoku, a naopak klesá so znižujúcim sa objemom a hodnotou dát v systéme pri nízkej pravdepodobnosti úspešného prelomenia ochrany. Ešte pred finálnym nastavením bezpečnostnej politiky je preto vhodné vyhodnotiť všetky

riziká s ohľadom na spomenuté atribúty pomocou ich analýzy a vyčísliť náklady na ich ochranu. [3]

Nečakaná situácia alebo stav informačného systému, ktorý predstavuje možnosť narušenia, ovplyvnenia alebo zlyhania kybernetickej bezpečnosti, jej zadefinovaných postupov a pravidiel, sa nazýva bezpečnostná udalosť a väčšinou s ňou do styku prichádza ako prvý bežný užívateľ. Ten musí rozpoznať či sa jedná o bezpečnostnú udalosť, alebo o bezpečnostný incident, bezprostredné „*narušenie bezpečnosti IS/ICT a pravidiel definovaných k jeho ochrane ..., ktoré je obvykle spojené s výpadkom služby alebo zhoršením jej kvality* ([17], s.12)". Je potrebné vnímať rozdiel medzi týmito dvoma pojmami. Zatiaľ čo infikovanie počítača vírusom je považované za bezpečnostnú udalosť, bezpečnostným incidentom sa stane napríklad jeho aktivácia a odosielanie platobných údajov o kreditnej karte subjektu s infikovaným počítačom. [16]

Hoci sa bezpečnostné incidenty riešia pomocou všeobecne používaných manažérskych zásad uplatňovaných pri akomkoľvek inom nepredpokladanom zásahu do systému alebo neštandardnej situácie, v praxi je viditeľný rešpekt manažérov voči takýmto incidentom vyplývajúci z nízkeho množstva predchádzajúcich skúsenosti. Nejde o nedostatok odborných znalostí, problémom je dramatický nárast využitia informačných a komunikačných technológií v spoločnostiach a organizáciách, rastúca závislosť na informačných systémoch, rýchlosť ich vývoja a prikladanie kľúčového významu čo najefektívnejšej reakcii a riešeniu bezpečnostných incidentov. Rozhodujúcim faktorom je pripravenosť, porozumenie každodennému fungovaniu systému a uvedomenie si potenciálnych incidentov. Po pochopení týchto súvislostí je manažér následne schopný na základe prijatých informácií o rozsahu incidentu, jeho dôležitosti a možných následkoch zaradiť bezpečnostný incident a vybrať vhodný a účinný postup pri jeho riešení aj vo vypätých situáciách vyžadujúcich rýchle a kvalifikované rozhodnutia. Bremeno zodpovednosti v oblasti informačných technológií a bezpečnosti informačného systému neleží výhradne na ramenách manažérov. Už v kapitole 2.3.1 Hrozby v kybernetickom priestore a ich taxonómia zaoberajúcej sa hrozbami informačných systémov bolo spomenuté, že viac ako polovica hrozieb pochádza zvnútra spoločnosti a sú neúmyselné. Zároveň sú práve zamestnanci tí, ktorí podávajú hlásenia, a tak informujú manažéra o podozrivej aktivite v systéme. Preto je nadmieru dôležité vytvoriť v organizácií dostatočne kvalitné bezpečnostné povedomie, ktoré minimalizuje neúmyselné incidenty a k tomu poskytne základ potrebný k správnemu odlíšeniu bežnej udalosti od hrozby. Efektívna tvorba bezpečnostného povedomia medzi pracovníkmi spoločnosti prebieha postupne, kontinuálnym prísunom nových informácií a organizovanými preventívnymi školeniami zameranými práve na bezpečnosť, ktoré spoločnosť pripravuje pre svojich zamestnancov. Napriek tomu, že tvorba bezpečnostného povedomia je z pohľadu bezpečnosti nezanedbateľná, v praktickom živote nie je v každej spoločnosti na rovnakej úrovni. Rozlišujú sa tri základné úrovne [16]:

- Najvyšší level – typicky predstavovaný medzinárodnými korporáciami, finančnými a bankovými inštitúciami a najvyššími štátnymi úradmi ako je Ministerstvo obrany, Národný bezpečnostný úrad, pre ktoré je ochrana a udržanie si citlivých informácií prioritou. Zamestnanci sú veľmi dobre informovaní o bezpečnom využívaní informačných systémov a schválenými postupmi pri v prípade narušenia bezpečnosti.
- Stredný level – tvorený hlavne súkromnými spoločnosťami, v ktorých je len úzka časť zamestnancov špecializovaná a veľmi dobre informovaná o bezpečnosti informačných systé-

mov, pričom zbytok zamestnancov má len základné povedomie o tejto oblasti alebo nie sú informovaní nijak.

- Najnižší level – zastúpený predovšetkým malými a strednými podnikmi, ktoré nepredstavujú primárny cieľ pre útočníkov. Z toho dôvodu nie je nedostatok bezpečnostného povedomia veľkým rizikom. Výnimkou sú organizácie štátnej a verejnej správy fungujúce na regionálnej úrovni, ktoré majú prístup k veľkému množstvu citlivých údajov a napriek tomuto faktu je povedomie o bezpečnosti informačných technológií u zamestnancov na veľmi nízkej úrovni.

Je na zvážení vedenia spoločnosti aké vysoké riziko bezpečnostného incidentu je ochotná niesť a či náklady na dôsledné vyškolenie zamestnancov nebudú v dlhodobej perspektíve nižšie ako náklady eventuálnych škôd.

2.3.4 Systém zvládania bezpečnostných incidentov (SIMS)

Systém zvládania bezpečnostných incidentov so skratkou SIMS odvodenej z anglickej verzie pomenovania, Security Incident Management System, je upravenou aplikáciou pôvodného modelu PDCA. Rovnako ako model PDCA je aj SIMS zameraný na zefektívňovanie procesov, používa sa ale na riešenie a vyhodnocovanie bezpečnostných incidentov v spoločnosti a s nimi súvisiacich procesov. Celý postup pozostáva zo štyroch základných fáz, etáp [16]:

a) Fáza PLAN – Základným stavebným kameňom k zvládaniu bezpečnostných incidentov je vytvoriť návrh, ktorý bude korešpondovať s bezpečnostnou politikou spoločnosti a prípadne iných záväzných noriem. Súčasťou tohto návrhu je okrem vytvorenia a popisu formalizovaných procesov a nastavenia súvisiacich základných ukazovateľov, spôsobu zberu informácií a dát aj tvorba plánu v prípade vyústenia bezpečnostného incidentu do krízového stavu v spoločnosti. Rovnako je v tejto fáze dôležité pripraviť plán vyškolenia zamestnancov v oblasti bezpečnosti informácií, prideliť právomoci a zodpovednosti za jednotlivé procesy ich konkrétnym vlastníkom a taktiež vytvoriť tím ISIRT, tím riešenia bezpečnostných incidentov. Je potrebné vymedziť právomoci aj vnútri tímu, stanoviť pole pôsobnosti a špecifikovať prípadné vonkajšie kontakty a spolupracujúce tímy.

b) Fáza DO – Po schválení návrhov nastáva moment ich nasadenia do praxe, kedy sa najdôležitejšími činnosťami stávajú spozorovanie bezpečnostného incidentu, jeho správne identifikovanie a následné rozhodnutie o riešení a aplikácia návrhu riešenia. Spozorovanie, respektíve detekovanie incidentu je kľúčovým okamžikom, pri ktorom je kvalitné bezpečnostné povedomie užívateľov základným predpokladom k rýchlemu nahláseniu incidentu a efektívnej odozve tímu ISIRT. Čo možno najpodrobnejšia dokumentácia primárnych informácií o incidente, napríklad skrz formuláre pre hlásenie bezpečnostných udalostí a incidentov, rovnako uľahčí bezpečnostným technikom nasledujúci proces identifikácie, určenia či sa naozaj jedná o bezpečnostný incident, miesta a príčiny jeho vzniku a rozsahu možného ohrozenia. Samotné vyriešenie bezpečnostného incidentu je v rukách profesionálneho tímu ISIRT. Je nutné overiť im predané informácie, prípadne incident preklasifikovať, zistiť doplňujúce dáta a vyhodnotiť ich a na analýzou podložených výsledkoch určiť postup riešenia. Všetky kroky je potrebné prejsť v čo najkratšom čase a za najvy-

ššej efektivity. V prípade, kedy nie je ani tím ISIRT schopný riešiť situácia, spoločnosť vyhlási krízový stav a postupuje podľa návrhov špecifikovaných pre tieto situácie.

c) Fáza CHECK – Celou predchádzajúcou etapou sprevádza jednotlivých účastníkov povinnosť dokumentovať celý incident dôkladne a spoľahlivo. Tieto informácie sú nutné nielen pre eventuálne zažiadanie poisťovne o náhradu škôd, ale hlavne z dôvodu vyhodnotenia incidentu. Nie je to jednokrokový proces, naopak, skladá sa z hĺbkovej analýzy incidentu a jeho záverov, obnovenia databázy bezpečnostných incidentov, rozšírenia bezpečnostného povedomia v organizácií o poučenie z vyriešeného incidentu a rozboru efektívnosti procesu zvládania incidentu.

d) Fáza ACT – Pokiaľ spoločnosť detailne vyhodnocuje každý bezpečnostný incident, závery sú dostatočne objektívne a môžu sa využiť na zdokonalenie a rozvoj samotného systému riadenia bezpečnostných incidentov v organizácií. Zovšeobecnené výsledky je možné aplikovať v iných oblastiach, nielen informačných a komunikačných technológií a informačných systémov.

Poslednou fázou sa uzatvára kruh, ktorý na základe všetkých informácií získaných v jednotlivých etapách riešenia bezpečnostného incidentu umožňuje podať strategickému vedeniu cennú spätnú väzbu. Práve tá poskytuje príležitosť na úpravu a zmenu nastoleného chodu, a tak napomáha zdokonaľovať a zefektívňovať celý proces rešenia bezpečnostného incidentu ako aj iných procesov v spoločnosti. [16]

3 Základné informácie o CERT tímoch

Na margo predchádzajúcich informácií sa môže zdať, že kybernetická bezpečnosť a bezpečnostné incidenty sa týkajú len veľkých komerčných organizácií alebo vládnych orgánov pracujúcich s citlivými informáciami. V reálnom svete ale mávajú bezpečnostné incidenty ďalekosiahlejšie následky ohrozujúce niekedy celú infraštruktúru sietí či dokonca všetky siete v krajine, vrátane bežných užívateľov. Príkladom môže byť napadnutie systémov banky. Vďaka vysokým eventuálnych ziskom sa finančné a bankové inštitúcie stávajú častým terčom hackerov a iných kybernetických zločinov, pričom únik informácií o klientskych účtoch a klientoch samotných sa dotýka bežných užívateľov, môže siahať do vládnej sféry, rovnako prepojenie systémov centrály a príslušných pobočiek poskytuje príležitosť k celoplošnému ohrozeniu . Takáto krízová situácia prináša mnohé potenciálne hrozby, ktoré je nutné vyriešiť a odstrániť čo najrýchlejšie pri minimalizácií škôd.

Práve za účelom rýchleho riešenia a širokoplošnej koordinácie vznikol a bol vyvíjaný koncept CERT tímov. Faktom je, že kybernetická bezpečnosť je sama o sebe novou oblasťou, ktorá nadobudla relevanciu s pribúdajúcim využívaním informačných systémov spracovávajúcich veľké množstvo citlivých dát a údajov, preto sú CERT tímy rovnako považované za pomerne novú záležitosť a povedomie o ich funkcii a dôležitosti nie je vysoké. Z tohto dôvodu sú v nasledujúcej kapitole prezentované základné informácie o CERT tímoch vrátane vysvetlenia rozdielu medzi pomenovaním CERT a CSIRT, informácie o zrode prvého CERT tímu a nasledovnom vývoji, rôznych typoch CERT tímov, ktoré sa vyvinuli a jednotlivých funkciách a službách, ktoré ponúkajú. Časť kapitoly taktiež ponúka stručný popis procesu zakladania vlastného CERT tímu od definície kľúčových služieb po technologické a organizačné vybavenie, ktorý je v súlade s odporúčaniami Európskej únie. S tým súvisiacej európskej legislatíve v oblasti kybernetickej bezpečnosti, možnostiam medzinárodnej spolupráce tímov a organizáciám, ktoré takúto kooperáciu podporujú sa rovnako venuje práca práve v tejto kapitole.

3.1 Vznik a vývoj CERT tímov

Počítačový červ s názvom Morrisov červ sa stal historickým míľnikom v oblasti kybernetickej kriminality a internetových vírusov, ale prvenstvo mu patrí aj na poli kybernetickej bezpečnosti. Aj v tomto prípade totiž platí pravidlo, že akcia zákonite vyvoláva reakciu. Morrisov červ vďaka rýchlej prenosnosti dokázal infikovať veľké množstvo informačných systémov a ohroziť tak počítačove infraštruktúry v celosvetovom rozpätí. Hrozba týchto rozmerov preto neostala nepovšimnutá a len pár dní po útoku, bol na akademickej pôde Univerzity Carnegie Mellon v Pittsburghu, Pensylvánia, vytvorený Projekčnou agentúrou pre výskum zdokonalenej obrany, DARPA, prvý CERT tím. Bol založený už v roku 1988, avšak aktívne pôsobí dodnes vo forme Koordinačného strediska CERT (CERT / CC). Na európskom kontinente bol prvým zriadeným CERT tímom SURFnet-CERT v roku 1992, taktiež na akademickej pôde holandskej univerzity. Jeho hlavným cieľom bolo zaisťovať bezpečnosť a riešiť bezpečnostné incidenty na surfovacej sieti SURFnet. [18]

Hoci prvotným cieľom tímu bolo vytvorenie stratégie obrany konkrétne proti Morrisovmu červu, významnejším prínosom bola myšlienka vytvorenia univerzálneho vopred pripraveného plánu, ktorý by v podobnom prípade narušenia informačného systém bezpečnostným incidentom mohol byť použitý už v okamžiku jeho odhalenia. Tento moment sa podľa Kropáčovej dá považovať za začiatok éry CERT tímov a tvorby svetovej CERT infraštruktúry. Ako sa časom Internet rozširoval a začal využívať v každodennom chode firiem aj vládnych orgánov, informačné systémy sa stali nosným prvkom komunikácie, zdieľania a uchovávania informácií, rástla aj potreba ochrany týchto systémov a množstvo CERT tímov. Agentúra ENISA pravidelne vydáva prehľad o počte CERT tímov v jednotlivých členských krajinách, tzv. Zoznam činností CERT v Európe. Podľa správy z decembra 2014 momentálne pôsobí v Európskej únii 251 tímov CERT, okrem akademickej pôdy aj vo forme interných, národných či vládnych tímov. Práve dôležitosť národných a vládnych CERT tímov v krajine sa ukazuje v prípadoch akým boli útoky na Gruzínsko v roku 2008, kedy krajina nemala ani národný, ani vládny CERT tím, ktorý by koordinoval obranu a riešenie bezpečnostného incidentu, a preto sa tejto funkcie chopil jediný CERT tím, ktorý v krajine pôsobil, konkrétne CERT-GE prevádzkovaný výskumnou a vzdelávacou organizáciou GRENA. [17] [19]

Pokiaľ ide o územie Českej republiky, prvý CERT tím CESNET-CERTS, vznikol v roku 2004, národný tím bol oficiálne vyhlásený v decembri 2010 a vládny CERT tím bol vytvorený až nadobudnutím účinnosti Zákona o kybernetickej bezpečnosti 1. januára 2015. Všetkým trom CERT tímom sa bakalárska práca venuje podrobnejšie v kapitole 4 Kybernetická bezpečnosť v Českej republike. [17] [20] [21]

3.2 Význam skratiek CERT a CSIRT

Ako prvé je na mieste vysvetliť rozdiel medzi skratkami CERT a CSIRT a ich užitím. Zjednodušene sa dá povedať, že žiadny nie je. Oba termíny môžu byť aplikované na tím s rovnakým zameraním a funkciou v organizácií. Avšak z krátkeho nahliadnutia do histórie v predchádzajúcich riadkoch je zrejmé, že prvýkrát sa použil názov Computer Emergency Response Team, skrátene CERT, ktorý bol však krátko potom zaregistrovaný Koordinačným strediskom CERT v USA. Z tohto dôvodu sa hlavne v Európe namiesto chráneného názvu CERT rozšíril termín CSIRT, respektíve Computer Security Incident Response Team, ktorý vznikol na konci 90. rokov. V praxi sa môžeme stretnúť aj s označením IRT ako Incident Response Team, CIRT, Computer Incident Response Team, SERT skracujúcim Security Emergency Response Team alebo už spomínaným ISIRT, Information Security Incident Response Team. [18]

Každá organizácia má možnosť výberu pomenovania, ktoré sa k nej samotnej a budúcemu poľu pôsobnosti tímu hodí najviac. V tejto práci však budem používať CERT a CSIRT ako synonymá. V kapitole zameranej na tímy CERT / CSIRT účinkujúce na území Českej republiky sa pomenovania jednotlivých tímov riadia oficiálnym názvom alebo Zákonom o kybernetickej bezpečnosti (181/2014 Sb.), ako je to v prípade vládneho CERT tímu, referovaný ako GovCERT.CZ alebo Vládny CERT tím Českej republiky a národnému CERT tímu, referovaný ako CSIRT.CZ alebo Národný CSIRT tím Českej republiky. [21]

3.3 CERT tímy v medzinárodnom kontexte

Keďže tvorba CERT tímov nie je nijak oficiálne povinnou záležitosťou v krajinách Európskej organizácie ani na vládnej úrovni, ani na úrovní komerčných organizácií, ich dobrovoľný vznik a zánik komplikuje udržovanie vzájomného prehľadu o existencii tímov. Za týmto účelom boli vytvorené medzinárodné platformy svetového aj európskeho charakteru, ktoré poskytujú možnosť vzájomnej komunikácie a nadväzovania spolupráce medzi CERT tímami, aj vďaka pravidelne usporadúvaným stretnutiam. Spolupráca je, ako bude ešte v tejto bakalárskej práci viackrát prízvukované, jednou z najdôležitejších činností, ktoré CERT tímy vykonávajú či už vo forme pomoci pri prvotnom zriaďovaní a uvedení do svetovej infraštruktúry, alebo pri zdieľaní informácií a skúseností z vlastnej praxe. [17]

Najaktívnejšími z platforiem v oblasti kybernetickej bezpečnosti sú organizácie [18]:

- FIRST – celosvetovo pôsobiace Fórum tímov pre riešenie bezpečnostných incidentov a bezpečnosti je poprednou organizáciou v oblasti kybernetickej bezpečnosti, ktorého prioritou je pomocou spolupráce a vzájomnej komunikácie svojich členov rozvíjať kvalitu poskytovaných služieb a reakcií na bezpečnostné incidenty.

- ENISA – v marci 2004 bola vytvorená Európska agentúra pre bezpečnosť sietí a informácií, ktorej úlohu je zvyšovať úroveň ochrany sietí pred potenciálnymi hrozbami poskytovaním odborných rád a návrhov opatrení, pomáhať pri tvorbe CERT tímov a podnecovať povedomie o kybernetickej bezpečnosti medzi bežnými užívateľmi, organizáciami aj štátnymi inštitúciami v členských štátoch Európskej únie, ktoré k ochrane prispieva.

- TERENA – predstavuje Trans-európske združenie pre výskum a tvorbu vzdelávacích sietí, ktoré s cieľom podpory spolupráce CERT tímov pôsobiacich v Európe a priľahkých krajinách vytvorilo pracovnú skupinu TF-CSIRT poskytujúcu služby fóra pre vzájomné zdieľanie informácií, služby pomoci pri tvorbe nových tímov a školení zamestnancov a pomoc pri tvorbe spoločných noriem zameraných na kybernetickú bezpečnosť v Európe.

3.4 Definovanie a funkcia tímu CERT

Odhliadnuc od skratky použitej na označenie konkrétneho tímu, spoločným znakom pre všetky je cieľ, ktorý zdieľajú. V dokumente z roku 2010 vypracovanom medzinárodne pôsobiacou organizáciou ENISA je takýto tím chápaný ako „*tím expertov v oblasti bezpečnosti IT, ktorých hlavnou úlohou je reagovať na bezpečnostné incidenty počítačov* ([18], s.7)“, pričom zabezpečuje okrem služby rýchleho a efektívneho riešenia incidentu aj podporu zložkám pri obnove poškodených systémov. Zložkou sa v kontexte tímov pre riešenie bezpečnostných incidentov rozumie zákazník, klient. Svoju snahu o minimalizáciu rizika a pokles počtu zásahov podporuje poskytovaním preventívnych vzdelávacích školení a odborných rád, čím prehlbuje bezpečnostné povedomie u zamestnancov a v konečnom dôsledku tak napomáha ochrane informačných systémov obsahujúcich citlivé informácie rôzneho druhu. Odbornosť a profesionalita CERT tímov vyplývajúca z nutnosti sledovať nové trendy a rozvoj v oblasti, ich predurčuje pôsobiť zároveň ako kontaktné miesto, centrum, na ktoré smerujú všetky otázky z oblasti IT bezpečnosti. Tieto otázky sa skoordinujú,

odpovedia jednotlivo užívateľom alebo sa vyvodia hromadné závery podnecujúce koordináciu s manažmentom spoločnosti alebo konkrétne cielenou skupinou vedúcu k preškoleniu alebo dokonca zmene procesov. [18]

Zoznam všetkých potenciálnych služieb poskytovaných tímom CERT sa nachádza v priloženom obrázku (viz Obrázok 2). Vytvorený bol priamo Koordinačným strediskom CERT a zachytáva kľúčové činnosti, zvýraznené tučným fontom, rozdelené do dvoch skupín. Reaktívne služby priamo súvisia s riešeným bezpečnostným incidentom, zatiaľ čo aktívne služby sú zamerané na prevenciu a dvíhanie úrovne bezpečnostného povedomia. Kolonka Zachádzanie s artefaktmi vymenúva služby naviazané na analýzu alebo riešenie objektu či súboru v systéme považovaného za eventuálne škodlivý. Posledným celkom služieb sú poradenské a vzdelávacie činnosti s dlhodobými cieľmi, nazvané Management akosti bezpečnosti. V praxi sa tímy nevenujú všetkým službám, ale vyberú si podľa svojich potrieb a zamerania. [18]

Reaktivní služby	Aktivní služby	Zacházení s artefakty
• **Výstrahy a varování** • **Řešení bezpečnostních incidentů** • **Analýza bezpečnostních incidentů** • **Podpora reakce na bezpečnostní incidenty** • **Koordinace reakcí na bezpečnostní incidenty** • Reakce na bezpečnostní incidenty na místě • Řešení zranitelnosti • Analýza zranitelnosti • Reakce na zranitelnost • Koordinace reakcí na zranitelnost	• **Oznámení** • Sledování techniky • Audity nebo hodnocení bezpečnosti • Konfigurace a udržování bezpečnosti • Vývoj nástrojů bezpečnosti • Služby detekce narušení • Šíření informací týkajících se bezpečnosti	• *Analýza artefaktů* • *Reakce na artefakty* • *Koordinace reakcí na artefakty* ***Management jakosti bezpečnosti*** • *Analýza rizik* • *Kontinuita obchodu a obnovení provozu po havárii* • *Poradenství v bezpečnosti* • *Vytváření povědomí* • *Vzdělávání/výcvik* • *Hodnocení nebo certifikace produktů*

Obrázok 2: Zoznam všetkých služieb poskytovaných CERT tímom (Zdroj: [18], s.11)

Ako sa všetky činnosti navzájom spájajú do jedného celku a vytvárajú jednotný systém spolupracujúci s ostatnou časťou organizácie je bližšie vysvetlené v jednej predchádzajúcich kapitol, konkrétne kapitola 2.3.4 Systém zvládania bezpečnostných incidentov (SIMS).

3.5 Založenie CERT tímu

Je nepopierateľné, že možnosť obrátiť sa s bezpečnostným problémom na vlastný CERT tím, ktorý je oboznámený s fungovaním informačných systémov v organizácií, dokáže promptne reagovať a vyriešiť bezpečnostné incidenty 24 hodín denne, 7 dní v týždni je pravdepodobne podstatou vzniku a fungovania tímov CERT v mnohých veľkých organizáciách, ale odnedávna sa CERT tímy začali vnímať aj ako kritický nástroj umožňujúci regulovať bezpečnostné procesy v organizácií

a dohliadať nad ich efektívnosťou. Táto možnosť pramení práve zo zbierania a vyhodnocovania informácií k aktuálnym aj už vyriešeným incidentom, tretia a štvrtá fáza systému zvládania bezpečnostných incidentov. Tretím impulzom k vytvoreniu CERT tímu v organizácií je zákonná povinnosť, ktorá vyslovene nariaďuje založiť si vlastný tím pre riadenie bezpečnostných incidentov alebo stanovuje spoločnosti orgán, na ktorý sa môže s prípadným bezpečnostným problémom obrátiť. Príkladmi takýchto zákonov v Spojených štátoch amerických sú štátny zákon Kalifornie SB 1386 alebo Akt Sarbanes-Oxley. Zákonu o kybernetickej bezpečnosti platnému na území Českej republiky sa práca bude venovať podrobne v kapitole 4.2.2 Zákon o kybernetickej bezpečnosti (č. 181/2014 Sb.). Všetky tri podnety vedúce k vzniku CERT tímu zapríčinili citeľný nárast ich počtu za posledné roky. [22]

V nasledujúcich kapitolách sú postupne stručne opísané hlavné kroky vedúce k vytvoreniu CERT tímu tak, ako ich navrhuje organizácia ENISA v dokumente CSIRT Setting up Guide z roku 2010.

3.5.1 Stanovenie pôsobnosti a služieb CERT tímu

Prvým krokom k vytvoreniu efektívne pracujúceho tímu je pripraviť detailný plán, ktorý obsahuje základné informácie definujúce vnímanie termínov súvisiacich s činnosťou tímu, vymedzenia pôsobnosti tímu a konkrétnych poskytovaných služieb, špecifikovanie rolí a zodpovednosti v rámci tímu a aplikovateľné postupy riešenia bezpečnostných incidentov, postupy prevencie aj postupy v prípadoch, kedy tím nie je schopný bezpečnostný incident vyriešiť. Plán je pripravený v časovom horizonte, ktorý musí počítať so skúšobnou dobou nutnou na overenie fungovania prvotnej prevádzky. Skúšobná doba, odporúčaná v trvaní od 18 mesiacov do 2 rokov, poskytuje možnosť prípadnej opravy chýb a chybných predpokladov pred konečným oficiálnym uvedením tímu do prevádzky. Na začiatku, pri prvotnom zakladaní tímu CERT, je „zlatým pravidlom“ podľa Paula Robertsa sústrediť sa na bezpečnostnú politiku a procesy súvisiace len s kľúčovými službami, ktoré bude tím poskytovať. Až v prípade, kedy sú tieto kľúčové služby plne zabezpečené je vhodné sa zamerať na služby menej kritické. [22]

Kompletnej škále služieb poskytovaných tímami CERT sa venovala kapitola 3.4 Definovanie a funkcia tímu CERT a ako je z nej viditeľné, varieta služieb je široká. Nie je v silách každého CERT tímu pôsobiť ako centrum s najvyššou úrovňou odbornosťou v každej z týchto služieb a preto sa tímy začali v oblasti služieb užšie špecializovať [18]:

- Interný CERT – funguje v rámci jednej organizácie, najčastejšie bankové inštitúcie a telekomunikačné organizácie, ktorej pracovníkom a oddeleniu IT poskytuje svoje služby.
- Komerčný CERT – poskytuje platené služby najčastejšie koncovým užívateľom.
- CIP/CIIP CERT – špecializované tímy na ochranu kritických informácií a ochranu kritických informácií a infraštruktúry, častokrát úzko spolupracujú s vládnym CERT tímom.
- Vládny CERT – zabezpečuje služby štátnym orgánom, výnimočne v niektorých krajinách aj občanom, napríklad v Belgicku, Maďarsku alebo Nemecku.
- Národný CERT – sa stáva bezpečnostným kontaktným miestom konkrétnej krajiny, figurujúcim ako sprostredkovateľ pre celú krajinu, a preto obvykle nemá priame zložky.

- Vojenský CERT – zaobstaráva služby vojenským alebo úzko súvisiacim inštitúciám, ako je ministerstvo obrany, zodpovedajúcim za IT infraštruktúru nutnú za účelom obrany.

- Akademický CERT – je súčasťou vzdelávacích a výskumných organizácií, ktorým poskytuje služby v oblasti intranetu aj Internetu.

- CERT malých a stredných podnikov – je samoorganizovaným tímom so službami v konkrétnom odbore, pričom jeho zložkami sú najmä pracovníci podnikov alebo záujmové skupiny.

Obchodný plán pre tím CERT

Súčasťou prvej časti plánu je stanovenie obchodného plánu tímu. CERT tím akéhokoľvek z vyššie uvedených druhov je súčasťou obchodnej spoločnosti, samotnou obchodnou spoločnosťou alebo súčasťou štátnych orgánov, a preto sa zahrňuje do globálneho obchodného plánu spoločností a musí sa riadiť stanovenými pravidlami a rozpočtom. Práve definovanie finančného modelu pre CERT tím je hlavným prvkom jeho obchodného plánu. Na strane nákladov primárne figurujú mzdy závislé na počte zamestnancov, odbornosti a dĺžke ich pracovnej doby. Strana výnosov pozostáva z možného členského poplatku, dotácií alebo výnosov z platených služieb. [18]

3.5.2 Technologické a organizačné aspekty tímu CERT

Po špecifikovaní základnej pôsobnosti a kľúčových ponúkaných služieb je možné v plánovaní pokračovať v detailnejšej rovine, kedy sa plán zameriava na organizačné a technologické aspekty fungovania tímu CERT, možnosti prepojenia tímu so zložkami, ktorým má poskytovať svoje služby a vzťahy s ostatnými tímami na národnej aj medzinárodnej úrovni.

Organizačná štruktúra tímu

ENISA rozlišuje v typickom tíme pre riadenie bezpečnostných incidentov štyri základné skupiny rolí [18]:

- Generálny riaditeľ

- Prevádzkovo – technická časť tímu tvoriaca jeho jadro. Zahŕňa technikov, ktorí dodávajú poskytované služby, vedúceho technického tímu a výskumný útvar.

- Pracovná časť tímu zodpovedá za činnosti priamo nesúvisiace s kľúčovými službami tímu CERT, ale nutné pre fungovanie tímu, ako je účtovníctvo, právne poradenstvo a poradenstvo v oblasti komunikácie. Dôležitosť pozície odborníka na komunikáciu v tíme je zreteľná v prípadoch, kedy je potrebné usmerňovať komunikáciu medzi technickou časťou tímu a zložkami alebo médiami, napríklad pri „preklade“ technických otázok kladených klientovi alebo naopak pri predávaní spätnej väzby od klienta technickému centru.

- Externí konzultanti

Organizačná štruktúra v konkrétnom tíme však vychádza z viacerých faktorov priamo ovplyvňujúcich a upravujúcich odporúčané, respektíve typické rozdelenie a hierarchiu rolí v tíme. Výrazne sa

na nej podpisuje už zavedená organizačná štruktúra hostiteľskej organizácie, ale taktiež dostupnosť dostatočne kvalifikovaných špecialistov na konkrétne pozície a typ úväzku, na ktorý sa najímajú. Okrem stabilného zamestnania odborníka na plný úväzok, je možné jeho služby využiť len pri špecifických prípadoch ako externého alebo dočasného zamestnanca. Pri zameraní sa tímu CERT na dve hlavné služby je odporúčaný počet technikov zamestnaných na plný pracovný úväzok aspoň 4. V prípade poskytovania plných služieb a systémovej údržby je požadovaný počet 6 až 8 pracovníkov. [18]

Komunikačné kanály so zložkami

CERT tímy fungujú ako dodávatelia služieb, a preto je pre ne, rovnako ako iné spoločnosti s obchodným plánom, kľúčové položiť si a nájsť optimálne odpovede na otázky „Ako sa s nami zákazník spojí? Pomocou akých ciest budeme schopný efektívne komunikovať s klientmi? Akými spôsobmi budeme môcť dostatočne rýchlo šíriť informácie?“. Najosobnejším spôsobom, ktorý prehlbuje dôveru medzi tímom a jeho zložkami a zároveň tak uľahčuje vzájomnú komunikáciu a spoluprácu sú osobné návštevy zložiek vykonávané na pravidelnej báze. Je častokrát jednoduchšie prediskutovať konkrétne záležitostí pri osobnom stretnutí, kedy sú väčšinou obe strany ochotnejšie a otvorenejšie novým nápadom, zložky reagujú pozitívne na možnosť konverzácie v súkromí ich vlastných priestorov, čo rovnako prináša výhodu aj na strane tímu, ktorý má príležitosť nahliadnutia k fungovaniu spoločnosti „z prvej ruky“ a taktiež má zložka šancu klásť otázky s okamžitou spätnou väzbou. Neraz však kapacity tímu nie sú dostačujúce na zabezpečenie takejto pravidelnej a časovo náročnej služby každej zložke, používajú sa preto iné komunikačné kanály, ktoré sú dostatočne účelné. Patria medzi ne verejné webové stránky tímu, na ktorých môže potenciálny klient nájsť informácie o ponúkaných službách, zložení tímu a kontaktné údaje v podobe e-mailovej adresy, telefónneho či faxového čísla a adresy, pomocou ktorých môže formou e-mailu, SMS správy či listu kontaktovať CERT tím. Na webových stránkach sa rovnako môžu nachádzať internetové formuláre určené pre hlásenie bezpečnostných incidentov. Všetky komunikačné cesty existujú s cieľom uľahčiť prijímanie hlásení o bezpečnostnom incidente, jeho riešenie a sprostredkovanie spätnej väzby a prípadnú koordináciu s inými tímami pracujúcimi na bezpečnostnom incidente. [18]

Ako bolo už v kapitole venujúcej sa systému SIMS podrobnejšie rozobraté, tím CSIRT, respektíve CERT, musia z hlásenia o bezpečnostnom incidente získať čo možno najviac relevantných informácií súvisiacich s bezpečnostným incidentom a okolnosťami vzniku. ENISA v dokumente CSIRT Setting up Guide uvádza vzorové schéma formulára vhodného pre hlásenie bezpečnostných incidentov. V tejto práci je formulár umiestnený v časti Prílohy (viz Príloha 1).

Technická infraštruktúra CERT tímu

V momente, keď tím CERT definuje služby, ktoré bude ponúkať, je možné začať plánovať technickú infraštruktúru, „kostru“ a podporu nutnú pre plynulý chod a efektívne a bezpečné fungovanie, komunikáciu a správu údajov tímu. Nevyhnutnosťou, základom v oblasti technickej vybavenosti sú telefón, fax, e-mail a webová stránka. Všetky štyri patria ku komunikačným kanálom a umožňujú prvotnú komunikáciu so zložkami, okrem toho ale plnia komunikačné funkcie aj v rámci tímu. Zariadenie v podobe počítačov a ich hardwaru, laptopov, tlačiarní a ostatného prísl-

šenstva závisí na veľkosti tímu, počte zamestnancov, rozpočte a iných faktoroch. Samozrejmosťou je pripojenie k Internetu, ale pravidlom býva existencia vlastnej siete, neprepojenej s inými externými či internými sieťami, ktorá preberá pri riešení bezpečnostných incidentov úlohu testovacej platformy. Výber operačného systému záleží na preferenciách tímu a kompatibility s ostatnými systémami, ale podľa Daniela Peneda z portugalského tímu CERT.PT zodpovedného za národnú vzdelávaciu a výskumnú sieť je dobrým riešením na pokrytie variability operačných systémov využitie softwaru VMware alebo VirtualPC/VirtualServer, ktorý umožňuje tímu CERT využívať na jednom počítači viaceré druhy operačných systémov. Pokiaľ tím preferuje použitie len jedného, platforma Linux je považovaná za všestrannú a prispôsobivú, funkčnú pre všetky bežne používané penetračné nástroje. Rovnako systémy Windows NT 4.0, XP, 2003 a vyššie poskytujú dostatočnú flexibilitu a podporu hackingovým nástrojom. Operačný systém MacOS X je alternatívou, ktorú ocenia hlavne UNIX užívatelia zvyknutí používať štandardný príkazový riadok. [23]

Každý tím má rovnako povinnosť zaznamenávať si informácie o nahlásených bezpečnostných incidentoch. V prípade tímov s väčšou klientelou, dlhou históriu či jednoducho veľkým množstvom hlásení je najefektívnejšou voľbou implementovať do systému nástroj, ktorý sa o správu nahlásených bezpečnostných incidentov postará sám. Sleduje informácie z celého procesu hlásenia a riešenia bezpečnostného incidentu, kto riešil konkrétnu fázu, aké kroky urobil a postupy použil, s kým incident konzultoval, zaznamenáva všetky prihlásenia do systému, dôkazné materiály a rovnako vypovedajú o štádiu, v ktorom sa riešenie incidentu práve nachádza a aké kroky sa momentálne podnikajú. Nástroje, systémy, ktoré sa používajú na tieto účely sa nazývajú ticketové systémy. Príkladom je webová aplikácia AIRT, Application for Incident Response Teams, umožňujúca združovať informácie o vývoji a progrese riešenia bezpečnostného incidentu. Obsahuje vstavané vyhľadávanie predchádzajúcich incidentov podľa IP adresy, e-mailové šablóny a formáty vhodné na export dát. Systém Request Tracker for Incident Response, skrátene RTIR, je prvým open source systémom v oblasti administrácie údajov o bezpečnostných incidentoch. Bol vyvinutý v spolupráci s britskou sieťou pre vzdelávanie a výskum JANET a jej tímom pre riešenie bezpečnostných incidentov, JANET-CERT. Okrem nástrojov pre spravovanie informácií sa používajú v CERT tímoch systémy určené pre bezpečnostné audity, forenzné dátové analýzy, systémy na sledovanie prienikov do siete, takzvané IDS systémy a iné. Vybrané nástroje a príručky k použitiu odporúčané pre tímy CERT na základe predchádzajúcich skúseností viacerých európskych tímov, sa nachádzajú na stránke CHIHT, Informačné centrum nástrojov pre riešenie bezpečnostných incidntov, ktorá funguje ako pilotný projekt pod záštitou organizácie TERENA. [17] [23]

Za účelom zachovávania a spracovávania informácií nesúvisiacich priamo s riešením bezpečnostných incidentov, to jest kontaktné informácie na samotných členov tímu alebo členov iných tímov a informácie o spokojnosti zákazníkov, sa používajú nástroje CRM v prípade riadenia starostlivosti o zákazníkov, ENISA uvádza konkrétne SugarCRM a Sugarforce, a v prípade vyhľadávania kontaktných informácií odporúča využiť informačné zdroje organizácie RIPE, TI alebo objektu IRT. [18]

Vo všeobecnosti CERT a CSIRT tímy pracujú a spravujú veľké množstvo údajov o svojich zložkách, charaktere bezpečnostných incidentov a rozsahu škôd, ktoré sa považujú za citlivé a pri ich úniku či neautorizovanom a nevhodnom použití by mohli spôsobiť ujmu zložkám aj samotným tímom a ich dôveryhodnosti. Z tohto dôvodu musí byť ich technická infraštruktúra zabezpečená dostatočne vysokou úrovňou ochrany.

Elementárne pravidlá platiace pre vybavenie IT v tíme:

- Používať technológie a vybavenie, ktoré dokážu zamestnanci ovládať a používať, čím sa predíde zbytočným komplikáciám spôsobeným nesprávnou obsluhou.
- Zabezpečiť odolnosť systémov ich aktualizáciou a ochranou pred hrozbami internetového pripojenia použitím bezpečnostných softwarov, antivírových skenerov, programov proti sledovaniu a pod.
- Zabezpečiť elektronickú poštu softwarom pre šifrovanie elektronickej pošty a správ, napríklad podporou PGP, GnuPG alebo S/MIME.

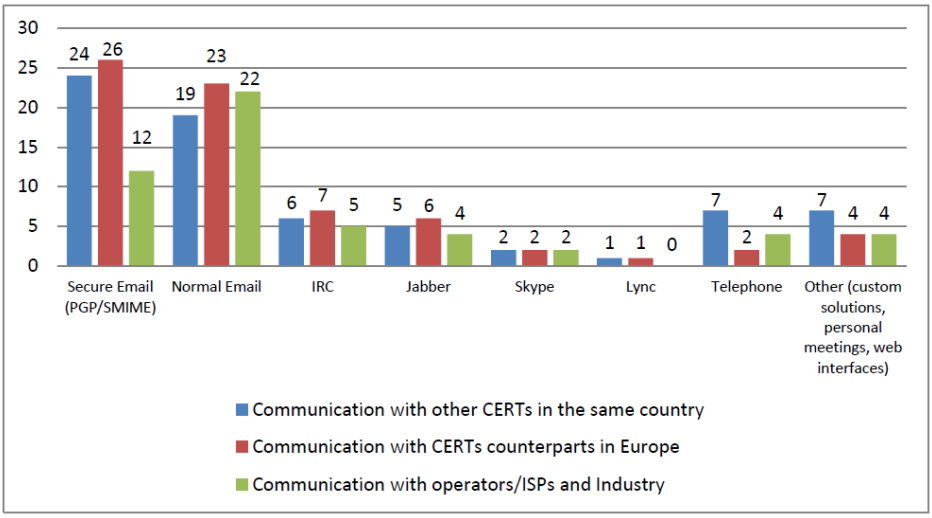
Tieto pravidlá sú tie základné a z istej časti intuitívne. Podľa druhu CERT tímu, citlivosti údajov, s ktorými pracuje, jeho špecializácie a ponúkaných služieb však môže podliehať pravidlám bezpečnosti vyplývajúcim zo zákona na vnútroštátnej, európskej a medzinárodnej úrovni, predpisom a normám. Stručný zoznam takýchto zákonov a noriem je priložený na konci práce (viz Príloha 2). [18]

Okrem ochrany informácií pred ich zneužitím sa CERT tím potrebuje chrániť aj pred možnou stratou, respektíve vymazaním týchto údajov v prípade nepredvídateľných katastrofálnych udalostí. Zálohovanie dát, považované za jeden z ochranných mechanizmov, by za takýchto okolností poskytlo príležitosť k obnoveniu časti, prípadne všetkých pôvodných dát. Viacnásobné kópie by mali byť bezpečne uskladnené v sklade v podobe externých diskov, DVD a CD nosičoch, páskach iného druhu alebo uskladnené na webových úložiskách. Všetky druhy zálohovaných dát musia byť pravidelne testované, aby sa zachovala integrita a zamedzilo sa strate informácií. Operačné systémy Windows a Linux majú zálohovacie nástroje zabudované priamo v systéme, ale rovnako je možné použiť nástroj Norton Ghost, ktorý zálohuje dáta v ich binárnej podobe na platformy Intel. [23]

3.5.3 Vzájomná spolupráca CERT tímov

Dôležitosť spolupráce tímov CERT, respektíve CSIRT, medzi sebou v rámci krajiny či na medzinárodnej úrovni je dôležitá nielen v prípadoch, kedy tím CERT nedokáže prísť s riešením bezpečnostného incidentu a potrebuje externú pomoc, ale aj z dôvodu zdieľania nových informácií, výskumu a vývoja nových praktík a technológií. Preto býva zvykom, že každý nový CERT tím skontaktuje ostatné tímy pôsobiace v tom istom, poprípade príbuznom odvetví alebo tímy ponúkajúce rovnaké či podobné služby. Význam a potenciál benefitov plynúcich z kooperácie tímov si organizácie fungujúce v oblasti riešenia bezpečnostných incidentov plne uvedomujú a snažia sa takúto spoluprácu podnecovať. Na medzinárodnej úrovni je viditeľná iniciatíva celosvetovej organizácie FIRST, spoluprácu na európskom kontinente podnecujú organizácie ENISA a TERENA. Všetky tri organizácie boli detailnejšie predstavené v kapitole 3.3 CERT tímy v medzinárodnom kontexte. V Európe rovnako figuruje pracovná skupina TF-CSIRT, ktorá pod záštitou organizácie TERENA, pôsobí ako medzinárodné fórum pre akreditované tímy aj bežných užívateľov a právomocami schválenými . Jej prioritnými cieľmi je „*poskytovať fórum pre výmenu skúseností a znalostí, vytvoriť pilotné služby pre európsku skupinu tímu CSIRT a napomáhať vytváraniu nových CSIRT* ([18], s.31)“, angažuje sa však aj pri tvorbe a presadzovaní noriem a postupov v oblasti bezpečnostných incidentov. [18]

Z výsledkov prieskumu, pri ktorom ENISA oslovila 27 tímov CERT z rôznych krajín a pýtala sa na prostriedky komunikácie používané pri kontakte s inými CERT tímami v krajine, respektíve medzinárodnej komunikácií, vyplýva, že najčastejšie používaným komunikačným kanálom je zabezpečený e-mail (viz Obrázok 3). Ten používa 26 z 27 opýtaných tímov pri komunikácií s tímom z inej krajiny a 24 z 27 tímov pri kontakte s tímom v rámci rovnakej krajiny. Výsledky pre národnú a medzinárodnú komunikáciu sa výrazne líšia len v prípade telefónnej komunikácie, kedy oproti 7 tímom používajúcim telefón ako prostriedok komunikácie v rámci krajiny, ho pri medzinárodnom kontakte využívajú len 2 CERT tímy. Preferencie v oblasti okamžitej komunikácie cez Internet patria systému IRC a Jabber, Skype a Lync využíva na komunikáciu len 2, prípadne 1 CERT tím. [24]



Obrázok 3: Nástroje používané pri komunikácií medzi CERT tímami (Zdroj: [24], s.4)

3.6 Európska legislatíva v oblasti kybernetickej spolupráce

Hoci je spolupráca tímov a vzájomná výmena informácií v oblasti bezpečnostných incidentov viac než vítanou činnosťou, kvôli citlivému a dôvernému charakteru správ podlieha prísnym pravidlám ochrany. V prípade, že sa členské štáty Európskej únie chcú stať autorizovanými členmi zabezpečeného informačného systému a podieľať sa na zdieľaní informácií, sú na základe splnomocnenia Európskej komisie povinní zabezpečiť ľudské, finančné a technické zdroje na úrovni postačujúcej pre efektívnu a bezpečnú spoluprácu, vrátane dostupnej kompatibilnej a zabezpečenej informačnej infraštruktúry na národnej úrovni. Cvičné materiály a tréningové príručky sprevádzajúce CERT tímy procesom integrácie do spoločnej infraštruktúry sú poskytované organizáciou ENISA, rovnako sa v svojich publikáciách zameriava na praktické a procesné fungovanie tímu, jeho technické zázemie a v neposlednej rade venuje pozornosť legislatívnej stránke kybernetickej bezpečnosti a zdieľania informácií, spoločnej pre všetky zúčastnené krajiny. Návrh smernice, ktorý nesie origi-

nálny názov Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union[1] , je súčasťou projektu A Europe Initiative 2020 a vznikol za účelom zjednotenia legislatív jednotlivých krajín v oblasti kybernetickej bezpečnosti, ochrany údajov a zdieľania informácií. Každá krajina Európskej únie má totiž svoju legislatívu, ktorá sa k nej stavia a definuje túto oblasť rôzne, napríklad IP adresa sa v jednej krajine pokladá za osobný údaj, v inej nie. Tieto rozpory komplikujú a predlžujú proces integrácie do spoločnej informačnej infraštruktúry. Viaceré tímy CERT zúčastňujúce sa prieskumu podporili tento názor a zjednotenie interpretácie na legislatívnej úrovni naprieč členskými štátni Európskej únie považujú za pozitívny prínos. [24]

Pripravovaná smernica nie je jediným predpisom, dokumentom či manuálom medzinárodnej pôsobnosti so snahou vytvoriť podporný rámec v boji proti kybernetickej kriminalite. Majú však „*charakter jednoúčelových doporučení či koncepčných materiálov, so širokým rozsahom pôsobnosti a s nekonkretizovaným účelom ich aplikácie* ([26], s.54)“, čo v konečnom dôsledku znamená, že členské štáty sa môžu, ale nemusia týmito odporúčaniami riadiť, nemajú oporu v legislatíve krajiny a pri zavádzaní do praxe nie je celkom jasné v akých konkrétnych prípadoch sú uplatniteľné. Príkladom je dokument „z pera“ skupiny G8 z roku 1997 predstavujúci desať základných princípov boja proti kybernetickej kriminalite, ktoré boli následne spracované do akčného plánu Európskej únie, skrátene nazvanom eEurope+. Je tvorený Uznesením Rady Európskej únie k Stratégií pre bezpečnú informačnú spoločnosť a sadou akčných plánov zameraných na rozvoj boja proti počítačovej kriminalite v členských a kandidátskych krajinách. Okrem vzájomnej spolupráce krajín a ich subjektov sa akčný plán sústredí na ochranu, šifrovanie a kontrolu komunikácie alebo technické požiadavky nutné k dostatočne bezpečnému používaniu siete. Česká republika sa k eEurope+ pripojila v roku 2002. Okrem oficiálnych aktivít pochádzajúcich zo strany Európskej únie sa iniciujú projekty založené na podnet členských štátov akým je napríklad projekt Check the Web. Projekt je zameraný na nutnosť spolupráce a zdieľania informácií v prípade teroristického zneužitia Internetu, rozdelenia právomocí a koordinácie činností. Iným projektom v oblasti spolupráce je projekt Koordinácie výskumu v oblasti kritickej informačnej infraštruktúry, ktorého cieľom je po analýze potenciálu najvýznamnejších organizácií v krajinách založiť komunikačnú sieť sprostredkúvajúcu bezpečnú komunikáciu medzi nimi. [26]

[1] Znenie Návrhu smernice je dostupné na webovej stránke Európskej komisie, v sekcii Digitálna agenda: http://ec.europa.eu/digital-agenda/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security [25]

4 Kybernetická bezpečnosť v Českej republike

Doteraz sa bakalárska práca venovala ponímaniu CERT tímov na medzinárodnej úrovni či už v kontexte medzinárodných organizácií, ktoré im poskytujú platformu na vzájomnú spoluprácu alebo legislatívnemu rámcu a odporúčaniam v rámci Európskej únie. Ako však bolo povedané, doteraz nebol schválený žiadny komplexný povinný právny predpis týkajúci sa kybernetickej bezpečnosti, ktorý by zaväzoval členské štáty k dodržiavaniu konkrétnych nariadení, a preto má každá krajina právo k vlastnej úprave.

Nasledujúca kapitola bakalárskej práce je z tohto dôvodu zameraná na predstavenie základných „stavebných kameňov" kybernetickej bezpečnosti v Českej republike. Prvá polovica kapitoly je venovaná kľúčovým orgánom v oblasti kybernetickej bezpečnosti, kde sú zmienené štátne orgány plniace zväčša kontrolnú alebo prevádzkovú funkciu, národný a vládny CERT tím a ich úloha a funkcia v Českej republike a nakoniec zoznam momentálne medzinárodne akreditovaných CERT tímov pôsobiacich v krajine. Druhá polovica kapitoly je zameraná na legislatívny rámec Českej republiky dotýkajúci sa kybernetickej bezpečnosti, s detailným upriamením sa na Zákon č. 181/2014 Sb., o kybernetickej bezpečnosti, schvaľovací proces, ktorý súvisel s jeho prijatím, obsahovú zložku zákona a jeho sprievodných dokumentov a nakoniec dopad zákona do praxe.

4.1 Kľúčové orgány kybernetickej bezpečnosti v ČR

Keďže sa rovnako ako v ostatných krajinách aj v Českej republike využívanie Internetu rozšírilo nielen k bežným užívateľom, korporáciám ale aj do vládnej sféry, je vo vlastnom záujme štátu a ochrany údajov, ktoré sa v sieťach prevádzkovaných na jeho území uchovávajú, dostatočne zabezpečiť kritické systémy pred napadnutím a hrozbami a dohliadať nad takýmto zabezpečením, ale taktiež vytvoriť systém organizácií schopný koordinovať a zakročiť v prípade zaznamenaného ohrozenia siete.

4.1.1 Najvyššie orgány pôsobiace v oblasti kybernetickej bezpečnosti

Najvyššími orgánmi pôsobiacimi v oblasti kybernetickej bezpečnosti na území Českej republiky, ktorých pôsobenie bolo upravené Uznesením vlády ČR č.781 z roku 2011, sú [27]:

- Národný bezpečnostný úrad (NBÚ) – uznesením prebral od Ministerstva vnútra ČR štatút gestora pre kybernetickú bezpečnosť v rámci republiky a stal sa najvyšším národným orgánom pôsobiacim v oblasti kybernetickej bezpečnosti. Okrem pôvodných funkcií ochrany utajovaných informácií a udeľovania bezpečnostnej spôsobilosti tak na seba prebral povinnosti autority v oblasti v podobe kontroly a dohľadu nad prevádzkovaním vládneho a národného CERT tímu. [28]

- Rada pre kybernetickú bezpečnosť (RKB) – prílohou uznesenia vlády vznikla ako poradný orgán pre predsedu vlády, ktorému raz do roka vypracováva správu o aktuálnom stave kybernetic-

kej bezpečnosti v krajine, z ktorej Vláda ČR vychádza mi stanovovaní úloh do budúceho obdobia. Okrem výročnej správy predkladá vláde podľa potreby svoje návrhy na zlepšenie alebo riešenie aktuálnej situácie týkajúcich sa kybernetickej bezpečnosti. Zároveň pomáha plniť NBÚ dohľadné a koordinačné povinnosti či v oblasti spolupráce CERT tímov. [29]

- Národné centrum pre kybernetickú bezpečnosť (NCKB) – súčasť NBÚ, vytvorená rovnako na základe uznesenia priamo za účelom prevádzkovania Vládneho CERT tímu Českej republiky GovCERT.CZ, ktoré hlavnou úlohou je v prvom rade prijímanie hlásení o bezpečnostných incidentov od osôb a orgánov spadajúcich pod kritickú informačnú infraštruktúru krajiny, koordinačná činnosť pri ich riešení, medzinárodná spolupráca a predávanie nadobudnutých informácií z oblasti, tvorba bezpečnostných štandardov používaných v Českej republike a osvetová a výskumná činnosť. [30]

4.1.2 Úloha národného a vládneho tímu CERT

Predtým než táto práca predstaví konkrétne CERT, prípadne CSIRT tímy, je namieste bližšie vysvetliť úlohu vládneho CERT a národného CERT tímu, ktoré sa v nasledujúcej kapitole objavia. Zjednodušená verzia ich úloh bola predstavená už v kapitole 3.4 Definícia a funkcia CERT, je však potrebné bližšie sa pozrieť na zodpovednosť a právomoci, ktoré majú a rolu, ktorú hrajú v kontexte kybernetickej bezpečnosti informačnej infraštruktúry v krajine.

Vládny CERT

Vládny tím CERT predstavuje v krajine svojho pôsobenia predovšetkým dohľadný orgán, ktorý dozerá na kritické a významné infraštruktúry v krajine, infraštruktúry štátnej správy a menších samospráv. Túto funkciu môžu však prebrať iné tímy CERT, často sa stáva, že pri nedostatočnej kapacite ľudských či finančných zdrojov sa role národného aj vládneho tímu spoja v jeden. V situáciách, kedy v krajine nie je oficiálne definovaný ani vládny, ani národný tím, ich funkciu preberá tím pôvodne založený organizáciou s významnou infraštruktúrou, poprípade tím z akademického sektoru a touto rolou sa prezentuje pred inými tímami a rovnako na medzinárodnej úrovni. Typicky používaným príkladom je spomínané prevzatie role národného a vládneho tímu Gruzínska tímom výskumnej a vzdelávacej asociácie, GRENA. Jej CERT-GE tím bol v tom čase v krajine jediným dostatočne špecializovaným v odbore kybernetickej bezpečnosti a preto na seba prevzal pri útokoch na informačnú infraštruktúru úlohu koordinátora obrany. Aj z tohto príkladu je viditeľná potreba existencie vládneho tímu v krajine, ktorú niektoré krajiny, ako je napríklad Fínsko či najnovšie aj Česká republika, už transformovali do legislatívy a na základe zákona určili svoje vládne tímy CERT, vrátane vymedzenia ich právomoci a zodpovednosti. [17]

V prípade Českej republiky je Vládnym CERT tímom Českej republiky GovCERT.CZ, ktorý je spravovaný Národným centrom kybernetickej bezpečnosti, NCKB. Základnou úlohou je okrem dohľadu nad infraštruktúrou, funkcia prvotného zdroja informácií z oblasti kybernetickej bezpečnosti, ich šírenie a propagácia s úmyslom dvíhania bezpečnostného povedomia a vzdelanosti v oblasti kybernetickej bezpečnosti. Rovnako pôsobí ako poradný orgán pre štátne orgány, organizácie aj občanov štátu. Táto služba je recipročná a orgánom, respektíve osobám, ktoré vymedzuje

Zákonom o kybernetickej bezpečnosti, sú povinné plniť záväzky voči vládnemu alebo národnému tímu CERT rovnako stanovené v zákone. [21]

K naplneniu jednej zo základných funkcií vládneho tímu CERT, to jest informovať o udalostiach a novinkách z oblasti kybernetickej bezpečnosti, je na webových stránkach GovCERT.CZ verejne dostupná sekcia Informačný servis, v ktorom má aj bežný užívateľ možnosť sledovať vydané publikácie, plánované a už uskutočnené akcie a udalosti, a v neposlednom rade sekcia Zraniteľnosti, kde sú chronologicky zoradené správy a varovania pred bezpečnostnými incidentmi, chybami v systéme a inými nebezpečenstvami z kybernetického sveta. Ku každej zraniteľnosti sú zverejnené charakteristiky, postihnuté systémy, dopad zraniteľnosti a spôsob riešenia takéhoto incidentu (viz Obrázok 4). [31]

Obrázok 4: Informácie o zraniteľnosti MongoDB na stránkach GovCERT.CZ (Zdroj: [32])

Národný CERT

V súvislosti s národným tímom CERT sa objavujú dva termíny, „last resort“ a „Point of Contact“. Pod pojmom Point of Contact je zachytená jedna z rolí národného CERT tímu, konkrétne zdieľanie informácií s tímami CERT na medzinárodnej úrovni alebo s tímami v rámci krajiny pri riešení bezpečnostného incidentu s vážnym charakterom alebo širokoplošným rozsahom vyžadujúcich

koordináciu viacerých subjektov. Národný CERT tím je považovaný za „*tím posledného útočiska* ([17], s.12)“, spomínaný last resort, a preto pomáha a zaoberá sa len závažnými bezpečnostnými incidentmi, incidentmi v sieti, ktoré pretrvávajú dlhú dobu alebo ich správca siete nevie, prípadne nechce riešiť, alebo sa nedá skontaktovať. Existuje mylná predstava, že národný tím CERT fyzicky rieši bezpečnostné incidenty, ale v skutočnosti je tím určený k dohľadu nad spoluprácou, jej koordinácií a varovaniu ohrozených subjektov, poskytuje priestor v podobe fóra na konzultovanie a šírenie vlastných skúseností tímov, správcov sietí, spoločností a inštitúcií, a nadviazanie potenciálnej spolupráce. Medzi jednu z najvýznamnejších funkcií národného tímu CERT patrí dvíhanie povedomia o počítačovej bezpečnosti a šírenie osvety medzi užívateľmi. Príkladom sú verejne dostupné webové stránky s informáciami, postupmi a radami, účasť a tvorba vzdelávacích akcií na školách či v komerčných organizáciách a taktiež propagácia v médiách. Veľká časť z poskytovaných služieb a forme ich poskytovania je ale závislá na konkrétnom prevádzkovateľovi tímu a jeho vízií. [17]

V Českej republike je národný CERT tím na základe podpísaného memoranda momentálne prevádzkovaný združením CZ.NIC a figuruje pod názvom CSIRT.CZ. Analýze jeho fungovania a poskytovaných služieb sa venuje celá nasledujúca kapitola 5 CSIRT.CZ, Národný CSIRT tím ČR.

4.1.3 Tímy CERT v Českej republike

Aktuálne v Českej republike pôsobí nasledujúcich päť CERT tímov, ktoré sú oficiálne akreditované na medzinárodnej úrovni [19]:

- GovCERT.CZ – Vládny CERT tím Českej republiky
- CSIRT.CZ – Národný CSIRT tím Českej republiky
- CESNET-CERTS – historický prvý CERT tím na území ČR, založený a prevádzkovaný združením CESNET z.s.p.o. od roku 2004, ktorý je špecializovaný na riešenie bezpečnostných incidentov na výskumnej a vzdelávacej sieti CESNET2 určenej prevažne študentom a zamestnancom Akadémie vied ČR a univerzít. [17]
- CSIRT-MU – akademický CERT tím Masarykovej univerzity v Brne
- CZ.NIC-CSIRT – interný CERT tím spoločnosti CZ.NIC z.s.p.o.

Trendom posledných rokov, počas ktorých sa dvíha povedomie o kybernetickej bezpečnosti a jej dôležitosti, je zriaďovanie interných CERT tímov, to jest tímov vytvorených v rámci komerčnej organizácie s cieľom poskytovať pre materskú spoločnosť službu riešenia bezpečnostných incidentov 24 hodín, 7 dní v týždni, s úzko profilovou špecializáciou na odvetvie a zameranie spoločnosti. Príkladom interných CERT tímov je vyššie uvedený CZ.NIC-CSIRT, ale aj tímy nevystupujúce na medzinárodnej úrovni ako O2.CZ CERT, Active24-CSIRT, ČDT-CERT alebo Seznam.CZ-CSIRT, predovšetkým teda spoločnosti prevádzkujúce internetové alebo komunikačné služby. [33]

4.2 Legislatíva kybernetickej bezpečnosti v ČR

Tvorba legislatívy a zákonov v oblasti kybernetickej bezpečnosti a kybernetickej kriminality má zásadný problém. Inovácia. Progres. Vývoj. Všetky tri slová popisujú jeden problém, to jest neustály a rýchly pokrok informačných a komunikačných technológií, ktorý nedáva veľa času a priestoru na reakciu vládam jednotlivých krajín. Proces návrhu a prijatia zákona je dlhý a pomalý, od prvotného nápadu a podnetu uplynú aj roky k uvedeniu zákona do platnosti. Medzitým technológie opäť pokročili, niektorá technika sa prestala používať, zločinci vymysleli nové spôsoby preniknutia do informačných systémov, navrhované definície pojmov by boli v praxi nepoužiteľné a návrh sa vďaka tomu stal zastaraným. Preto sa rozsah legislatív so zameraním na kybernetickú bezpečnosť jednotlivých krajín mnohokrát líši.

4.2.1 Cesta k Zákonu o kybernetickej bezpečnosti

Napriek tomu, že proces schvaľovania zákonov sa zdá byť „neprekonateľnou prekážkou“, v Českej republike len prednedávnom, 1. januára 2015, vstúpil do účinnosti nový Zákon o kybernetickej bezpečnosti (č. 181/2014 Sb.). Na jeho príklade je možné predviesť ako dlho v skutočnosti trvá celý schvaľovací proces až po uvedenie do platnosti a následne účinnosti. Všetko začalo 19. októbra 2011 uznesením vlády ČR, ktoré dalo novovytvorenému NCKB povinnosť vytvoriť nový zákon o kybernetickej bezpečnosti. Vecný zámer zákona sa objavil prvýkrát 30. mája 2012 a po schválení vládou prešiel do stavu konzultovania odborných náležitostí. Samotný návrh zákona a zmeny súvisiacich zákonov boli 15. apríla 2013 odoslané do pripomienkového riadenia. Pri tvorbe návrhu spolupracovali zástupcovia NBÚ, Ministerstva vnútra, Ministerstva obrany, Českého technického učení a odborných inštitúcií ako je CSIRT.CZ (v tej dobe pilotný projekt Ministerstva vnútra). Návrh bol vláde predložený 28. júna 2013, ktorá ho schválila 2. januára 2014, následne putoval k prejednávaniu v Parlamente Českej republiky. Po schválení návrhu Poslaneckou snemovňou Parlamentu ČR 18. júna 2014 a schválení 23. júna 2014 Senátom Parlamentu ČR bol zákon podpísaný prezidentom Milošom Zemanom dňa 13. augusta 2014. Zákon č.181/2014 Sb., o kybernetickej bezpečnosti a o zmene súvisiacich zákonov nadobudol platnosť 29. augusta 2014 a do účinnosti vstúpil 1. januára 2015. Celý proces tak trval tri roky, dva mesiace a dvanásť dní. [27]

V prípadoch trestnej činnosti informačného charakteru sú ďalej uplatňované zákony [3]:

- Zákon o práve autorskom č. 121/2000 Sb.
- Zákon o ochrane osobných údajov č. 101/2000 Sb.
- Zákon o elektrickom podpise č. 227/2000 Sb.
- Zákon o slobodnom prístupe k informáciám č. 106/1999 Sb.
- Zákon o niektorých službách informačnej spoločnosti č. 480/2004 Sb.
- Zákon o regulácií reklamy č. 40/1995 Sb.
- Zákon o informačných systémoch verejnej správy č. 365/2000 Sb.
- Zákon o prevádzkovaní rozhlasového a televízneho vysielania č. 231/2001 Sb.

- Zákon o elektronickej komunikácií č. 127/2005 Sb.
- Zákon o ochrane utajovaných informácií a o bezpečnostnej spôsobilosti č. 412/2005 Sb.

4.2.2 Zákon o kybernetickej bezpečnosti (č. 181/2014 Sb.)

Samotný Zákon č. 181/2014, o kybernetickej bezpečnosti vyvolal už pri návrhu rozpačité ohlasy, niektorí uvítali iniciatívu vytvorenia legislatívneho rámca pre kybernetickú bezpečnosť, iní sa naopak obávali zmien, ktoré jeho uvedenie do účinnosti privedie.

Zmeny v Zbierke zákonov a štruktúra zákona

Schválenie zákona č. 181/2014, ktorého oficiálny názov znie Zákon o kybernetickej bezpečnosti a o zmene súvisiacich zákonov, prinieslo do Zbierky zákonov jemný „vetrík" v podobe novelizácie štyroch zákonov z oblasti informačných technológií spomenutých v predchádzajúcej kapitole, konkrétne Zákon o slobodnom prístupe k informáciám, o prevádzkovaní rozhlasového a televízneho vysielania, o elektronickej komunikácií a o ochrane utajovaných informácií a bezpečnostnej spôsobilosti. Týmto zmenám sa venuje časť druhá až piata, z celkového počtu piatich častí. Prvá časť o rozsahu 33 paragrafov rozdelených do VI hláv sa venuje kybernetickej bezpečnosti, a preto je z pohľadu tejto bakalárskej práce kľúčová. Obsah je rozobraný detailnejšie v nasledujúcej kapitole. [4] [34]

K Zákonu o kybernetickej bezpečnosti sa dodatočne vzťahujú dva sprievodné právne predpisy, schválené 15. decembra 2014 a publikované v Zbierke zákonov 19. decembra 2014 [34] :

- Vyhláška č. 316/2014, o bezpečnostných opatreniach, kybernetických bezpečnostných incidentoch, reaktívnych opatreniach a o stanovení náležitostí podania v oblasti kybernetickej bezpečnosti (vyhláška o kybernetickej bezpečnosti)
- Vyhláška č. 317/2014, o významných informačných systémoch a ich určujúcich kritériách

Rovnako obsah vyhlášok je uvedený nižšie. Novým zákonom sa menili kritéria pre určenie prvku kritickej infraštruktúry a musel byť prijatý nový právny predpis Nariadenie vlády č. 315/2014 Sb., ktorým sa mení nariadenie vlády č. 432/2010 Sb., o kritériách pre určenie prvku kritickej infraštruktúry. [35]

Obsah Prvej časti zákona

Nový Zákon o kybernetickej bezpečnosti „*upravuje práva a povinnosti osôb a pôsobnosti a právomoci orgánov verejnej moci v oblasti kybernetickej bezpečnosti* ([4], § 1)", s výnimkou informačným systémov pracujúcich s utajovanými informáciami. Jeho cieľom je vytvorením právneho rámca zabezpečiť dostatočnú ochranu informačných systémov a kritickej infraštruktúry na základe stanovenia právomoci a povinností vládneho a národného CERT tímu a ostatných orgánov a osôb pôsobiacich v oblasti kybernetickej bezpečnosti. Nové pravidlá štandardizujú bezpečnostné opatrenia a proces hlásenia bezpečnostného incidentu a útokov, čím sa má urýchliť proces ich riešenia a vyhodnocovania a následne tak predísť potenciálnym bezpečnostným hrozbám. [36]

Táto práca je zameraná predovšetkým na časti zákona súvisiace priamo s tímami CERT a ich prevádzkou. Na začiatok definuje základné pojmy a vymenúva osoby, ktorých sa povinnosti priamo dotýkajú. Ide o správcov významného informačného systému, informačného alebo komunikačného systému kritickej informačnej infraštruktúry, osoby zaisťujúce významnú sieť alebo poskytovateľa služieb elektronických komunikácií a zaisťovateľa ich sietí. Zahrnutí nie sú ani bežní užívatelia, ani dodávatelia obsahu, čo korešponduje so snahou neukladať povinnosti súkromným subjektom. Za „srdce" zákona je možné považovať Hlavu II, týkajúcu sa systému zaistenia kybernetickej bezpečnosti, ktorá sa najviac dotýka CERT tímov a ich úloh a kompetencií. Definuje čo sa rozumie pod pojmom kybernetická bezpečnostná udalosť a kybernetický bezpečnostný incident, vo všeobecnej rovine, bez konkrétnych určení. Práve tu, § 8, vzniká osobám povinnosť hlásiť bezpečnostné incidenty trom inštanciám podľa zaradenia osôb zákonom a to NBÚ, národnému tímu CERT alebo nadradenej (významnej, resp. kritickej) sieti. Konkrétne prevádzkovateľovi národného tímu CERT musí bezpečnostné incidenty hlásiť „*orgán alebo osoba zaisťujúca významnú sieť* ([4], § 3)", pokiaľ nie je správcom komunikačného systému kritickej informačnej infraštruktúry. Náležitosti a spôsob hlásenia na základe rôznych typov a kategórií bezpečnostných incidentov stanovuje Vyhláška č. 316/2014 Sb. Evidenciu všetkých hlásení vedie NBÚ, pričom ich kvôli zaisteniu ochrany kybernetickej bezpečnosti v primeranom rozsahu môže poskytnúť národnému CERT tímu a iným orgánom a osobám pôsobiacim v tejto oblasti. Informácie by neboli poskytnuté v prípade ohrozenia bezpečnosti alebo odhalenia subjektu, ktorý bezpečnostný incident nahlásil. [4]

Národný CERT má zákonom jasne stanovenú funkciu nestranného „*zdieľania informácií na národnej a medzinárodnej úrovni v oblasti kybernetickej bezpečnosti* ([4], § 17)" a jeho prevádzkovateľovi stanovuje nasledujúce povinnosti, ktoré vykonáva bezúplatne [4]:

- Prijímať a vyhodnocovať hlásenia o bezpečnostných incidentoch od osôb a orgánov zákonom stanoveným spolu s ich kontaktnými údajmi, všetky informácie evidovať a uchovávať. Údaje o bezpečnostných incidentoch poskytuje NBÚ, avšak kontaktné údaje postihnutých orgánov a osôb môže vydať len v prípade vyžiadania Národným bezpečnostným úradom v stave kybernetického nebezpečenstva.

- Pôsobiť ako kontaktné miesto pre osoby a orgány zákonom stanovené a poskytovať im pomoc a podporu pri riešení bezpečnostné incidentu.

- Hodnotiť zraniteľnosti v oblasti kybernetickej bezpečnosti.

Zmieňovaným prevádzkovateľom národného CERT sa podľa zákona môže stať iba právnická osoba, ktorá s NBÚ uzavrie zmluvu s predpísanými náležitosťami a splňuje osem stanovených podmienok, medzi ktorými sú minimálne 5-ročné skúsenosti so správou a prevádzkou informačných systémov alebo služieb, dostatočné technické predpoklady v oblasti kybernetickej bezpečnosti, členstvo v nadnárodnej organizácií z oblasti. Samozrejmosťou je bezúhonnosť voči záujmom Českej republiky, trestná bezúhonnosť, neexistencia nedoplatkov v daňovej evidencii. [4]

V prípade vládneho CERT tímu sú stanovené povinnosti takmer rovnaké, platiace však pre iné osoby a orgány, tj. prijímanie, vyhodnocovanie a evidencia hlásení bezpečnostných incidentov, evidencia kontaktných údajov, poskytovanie pomoci, vyhodnocovanie zraniteľností. Zároveň prijíma a vyhodnocuje údaje od zahraničných orgánov z oblasti kybernetickej bezpečnosti a národného CERT, ktorým môže za účelom ochrany kybernetickej bezpečnosti vydať údaje zo svojej

evidencie. Ďalej zákon novo definuje stav kybernetického nebezpečenstva a podmienky jeho vyhlásenia. Aby sa udržal celý systém pod kontrolou, zákon stanovuje Národný bezpečnostný úrad kontrolným orgánom dohliadajúcim na plnenie povinností vyplývajúcich zo zákona. V prípade zistených nedostatkov môže orgánu alebo osobe určiť spôsob a časovú lehotu na ich odstránenie alebo v situácií, kedy nedostatky informačného systému zaradeného v kategórii kritickej informačnej infraštruktúry môžu významne tento systém poškodiť či úplne zlikvidovať, NBÚ má právo používanie tohto systému do odstránenia nedostatkov zakázať. Ak však osoba alebo orgán svoje povinnosti nesplní, NBÚ má právo udeliť sankcie a tresty v závislosti na charaktere správneho deliktu. Finančné pokuty sa pohybujú v hodnotách od 10 000 Kč po 100 000 Kč. [4]

Sprievodné právne predpisy k zákonu č. 181/2014 Sb.

Vyhláška o významných informačných systémoch a ich určujúcich kritériách a nové nariadenie vlády č. 315/2014 Sb., vymedzuje kritéria kritickej infraštruktúry a významných informačných systémov a tým špecifikuje jednotlivé prvky patriace do týchto kategórií. Podľa NCKB by mala byť prepojením zákona s realitou. Jej účelom je dopomôcť k jednoznačnému a rýchlemu určeniu prvkov na základe odpovedí na konkrétne otázky vo forme grafického diagramu, na ktorého konci sa užívateľ dozvie či patrí, alebo nepatrí do kategórie Kritická informačná infraštruktúra[2], prípadne Významný informačný systém[3]. [37]

Vyhláška o významných informačných systémoch obsahuje prílohu, ktorá priamo vymenúva 92 významných informačných systémov. K nájdeniu je medzi nimi informačný systém Vojenskej Polície Ministerstva obrany, informačný systém o dávkach štátnej sociálnej podpory Ministerstva práce a sociálnych vecí alebo centrálna evidencia stíhaných osôb Ministerstva spravodlivosti. [38]

Nariadenie vlády meniace kritéria určujúce prvky kritickej infraštruktúry je súborom kritérií pre každé z najdôležitejších odvetví zvlášť, kritériom sa vo väčšine prípadov rozumie číselná hodnota. Odvetviami sú energetika, vodné hospodárstvo, potravinárstvo a poľnohospodárstvo, zdravotníctvo, doprava, informačné a komunikačné systémy, finančný trh a mena, núdzové systémy a verejná správa. Za všetky spomeniem „*informačný systém spravovaný orgánom verejnej moci obsahujúci osobné údaje o viac ako 300 000 osobách* ([35], s.3968)“ alebo plocha väčšia ako 4 000 ha, na ktorej farma, respektíve poľnohospodársky podnik, pestuje jednu plodinu. [35]

Najrozsiahlejšou z trojice právnych predpisov je Vyhláška o kybernetickej bezpečnosti, ktorá pojmy, ktoré nie sú definované zákonom, ako napríklad bezpečnostná politika či hrozba a vymenúva pre ne konkrétne podmienky. K nariadeniu patrí sedem príloh určujúcich stupnice hodnotenia dopadov, hrozieb, zraniteľností a rizík, vymenúva technicky detailne špecifické minimálne požiadavky na kryptografické algoritmy, štruktúru bezpečnostnej dokumentácie a ďalšej dokumentácie ako je audit kybernetickej bezpečnosti. Posledné tri prílohy patria formulárom vrátane Formulára hlásenia kybernetického bezpečnostného incidentu (viz Príloha 3). [39]

---

[2] Proces určovania kritickej informačnej infraštruktúry podľa vyhlášky č. 317/2014 Sb. je dostupný na stiahnutie na stránkach GovCERT.CZ v sekcii KII/VIS: http://www.govcert.cz/cs/kii--vis/kriticka-informacni-infrastruktura/

[3] Proces určovania významného informačného systému podľa vyhlášky č. 317/2014 Sb. je dostupný na stiahnutie na stránkach GovCERT.CZ v sekcii KII/VIS: http://www.govcert.cz/cs/kii--vis/vyznamne-informacni-systemy/

4.2.3 Dopad Zákona o kybernetickej bezpečnosti do praxe

Hoci to znie ako veľa povinností a kritérií, ergo veľa zmien, ktoré sa musia pretaviť z textovej formy do praxe, nie je tomu celkom tak. Väčšina bezpečnostných opatrení, technických alebo organizačných, ktoré sú zákonom vyžadované, totiž vychádza z noriem ISO/IEC 27000. Organizácie, ktorých systém riadenia bezpečnosti informácií spĺňuje tieto normy by teda nemali mať s vstupom zákona do účinnosti a jeho požiadavkami problém. Veľké zmeny v oblasti kybernetickej bezpečnosti či už ide o implementáciu nástrojov ochrany, riadenie prístupu a overovania identity, či monitoring významných informačných systémov, by mali postihnúť jedine organizácie, ktoré bezpečnosť svojich informácií predtým zanedbávali. [36]

Rovnaký názor s redakciou BusinessInfo.cz zdieľajú aj Pavel Bašta a Zuzana Duračinská z národného CERT tímu, CSIRT.CZ. Zákon ale prináša v tomto zmysle jednu novinku. Zatiaľ čo pred nástupom jeho účinnosti boli hlásenia bezpečnostných incidentov dobrovoľné, po 1. januári 2015 sú hlásenia pre zákonom vymedzené orgány a osoby povinné. So zmenami fungovania je to podobne aj v prípade národného a vládneho tímu CERT. Napríklad práva a povinností národného CERT tímu boli spísané ešte pred schválením zákona v Memorande o CERT/CSIRT tímoch Českej republiky a vychádzajú z odporúčaní organizácie ENISA v oblasti prevádzky, fungovania aj spolupráce a zdieľania informácií. Prevádzkovateľom národného CERT tímu sa podľa zákona môže stať len tím, ktorý je členom medzinárodnej organizácie, ergo spĺňa ňou stanovené základné požiadavky. Zákon o kybernetickej bezpečnosti sa teda nesnaží zmeniť CERT tímy podľa svojich požiadaviek, pretože také už boli. Poskytuje hlavne právny rámec a legislatívnu oporu pre už zažité fungovanie tímu, ktorý vykonáva funkciu národného tímu CERT. Zástupcovia CSIRT.CZ sa ako súčasť odbornej komisie zúčastnili priamo procesu tvorby návrhu zákona, mali možnosť svoje pripomienky nechať zapracovať priamo do konečného znenia zákona a aj preto nemajú momentálnemu zneniu zákona čo vytknúť. Pavla Baštu napadol jediný podnet k rozšíreniu, a to zákonom definované právomoci členov národného a vládneho tímu CERT. Môžu totiž nastať situácie, kedy by zamestnanec za účelom zachovania dôveryhodnosti tímu mal overiť existenciu nahláseného bezpečnostného incidentu priamo v sieti, ale nemá k tomuto výkonu dostatočné právne kompetencie. Na margo vyhlášok dodávajú, že cieľom oboch vyhlášok a nariadenia vlády, ktoré sprevádzajú Zákon o kybernetickej bezpečnosti je konkretizovať zákonom všeobecne definované postupy a kritéria. Proces schvaľovania zákona je dlhý a náročný, zatiaľ čo vyhláška a nariadenie predstavujú flexibilnejší a rýchlejšie zmeniteľnejší legislatívny rámec. Z tohto dôvodu sa konkrétne požiadavky, hodnoty, kritéria, teda informácie, ktoré sa v stále vyvíjajúcom sa svete informačných systémov a technológií rýchlo menia, stanovujú práve v týchto právnych predpisoch. [40]

Jednoduchým a zreteľným príkladom je vymedzenie pojmu kritická informačná infraštruktúra v Zákone č. 181/2014 Sb., o kybernetickej bezpečnosti, kde sa ním chápe „*prvok alebo systém prvkov kritickej infraštruktúry v odvetví komunikačné a informačné systémy* ([4], § 2)“ s odvolaním na Nariadenie vlády č. 315/2014 Sb., v ktorom je už za prvok kritickej infraštruktúry v oblasti potravinárskej výroby považovaný výrobný závod s výrobou mäsa v hodnote aspoň 200 000 ton za rok. Novinkou v praxi je však sankcionovanie na základe nesplnenia povinností uložených zákonom, ktoré má v rukách NBÚ ako kontrolný orgán. [4] [35]

5 CSIRT.CZ, Národný CSIRT tím ČR

Už pri návrhu zákona bolo nutné zamyslieť sa nad tým, kto bude po nástupe do účinnosti vykonávať rolu prevádzkovateľa. V prípade vládneho CERT tímu sa prevádzkovateľom stalo Národné centrum kybernetickej bezpečnosti zriadené vyslovene pre tieto účely ako súčasť Národného bezpečnostného úradu. Voľbou pre národný CERT tím sa stalo združenie CZ.NIC, ktoré spĺňa podmienky stanovené zákonom a už v tej dobe dlhodobo prevádzkovalo modelový tím pre riešenie bezpečnostných incidentov CSIRT.CZ. Ten ešte pred vstupom zákona do účinnosti, a teda vznikom vládneho CERT tímu, zastupoval v Českej republike funkciu národného aj vládneho CERT tímu. Momentálne združenie CZ.NIC naďalej pôsobí ako prevádzkovateľ národného CERT tímu na základe memoranda podpísaného s Národným bezpečnostným úradom.

Organizácia CZ.NIC je záujmovým združením právnických osôb so sídlom na ulici Milešovská 1136/5, 130 00, Praha 3, figurujúca pod IČO 67985726. Združenie bolo založené v roku 1998 a hlavnou činnosťou je zabezpečenie prevádzky registra najvyšších doménových mien .CZ, rozvoj systémov a technológií správy domén a iných projektov internetovej infraštruktúry v rámci Českej republiky. Momentálne má 113 členov. [41]

Pozornosť nasledujúcej a zároveň poslednej kapitoly tejto bakalárskej práce je upriamená práve na fungovanie a prevádzku CSIRT.CZ, Národného CSIRT tímu Českej republiky. Zo Zákona o kybernetickej bezpečnosti vyplývajú národnému CERT tímu určité povinnosti, rovnako tak zo zmluvy s NBÚ. Taktiež ENISA vo svojej príručke CSIRT Setting up Guide ponúka odporúčania a rady k správne fungujúcemu tímu. Vďaka informáciám zverejnených na webových stránkach národného CERT tímu www.csirt.cz a osobnej komunikácií formou rozhovoru a e-mailu (viz Príloha 8 a Príloha 9) je možné nahliadnuť do prevádzky tímu v skutočnom svete, nie „na papieri“. Kapitola predstaví historický vývoj pracoviska CSIRT.CZ až do role národného CERT tímu, jeho pole pôsobnosti a funkcie, vrátane konkrétneho príkladu koordinácie, ponúkané služby, spôsob financovania, aktivity v oblasti medzinárodnej a národnej spolupráce a technické a organizačné zázemie pracoviska. Záverom kapitoly je porovnanie postavené na týchto informáciách a údajoch z predchádzajúcich kapitol venovaných Zákonu o kybernetickej bezpečnosti a príručke „z pera“ organizácie ENISA.

5.1 Od modelového pracoviska k národnému CERT

Zatiaľ čo Národný bezpečnostný úrad pracoval na návrhu nového zákona vytvárajúceho právny rámec v oblasti kybernetickej bezpečnosti, pracovisko, ktoré sa neskôr stalo národným CERT tímom, sa vyvíjalo svojou vlastnou cestou.

Na úplnom začiatku stál vedecko-výskumný grant Ministerstva vnútra Českej republiky s názvom Kybernetické hrozby z hľadiska bezpečnostných záujmov Českej republiky. Tento grant je označený identifikačným číslom VD20072010B013. V rámci neho malo v Českej republike vzniknúť modelové pracovisko s cieľom „*overenia stavu bezpečnostnej infraštruktúry ČR a overenia realizovateľnosti distribuovanej hierarchie pre systematické plošné riešenie bezpečnostnej problemati-*

ky v počítačových sieťach ČR prostredníctvom CSIRT tímov ([17], s.12)", respektíve overiť, či sú správcovia informačných systémov, poskytovatelia služieb elektronických komunikácií a operátori schopní pri riešení závažného a plošného bezpečnostného incidentu spolupracovať. Takto rozsiahla spolupráca ale vyžaduje dohľad a dávku koordinácie, ktorú malo priniesť práve vybudovanie modelového tímu CSIRT. Keďže išlo o pilotný projekt, Ministerstvo vnútra ČR sa skontaktovalo s jediným združením, ktoré s budovaním a prevádzkovaním CSIRT tímu malo už skúsenosti, združením CESNET. Práve oni vytvorili CESNET-CERTS, prvý svetovou komunitou oficiálne uznaný CSIRT tím v Českej republike. S oficiálnou výstavbou modelového pracoviska CSIRT.CZ sa začalo na jeseň 2007. Do 1. januára 2008 sa za pomoci CSIRT tímu združenia CESNET podarilo vytvoriť kompletné technické a organizačné zázemie, 3. apríla 2008 boli spustené webové stránky tímu a sprístupnené kanály hlásenia bezpečnostných incidentov. Týmto momentom sa modelové pracovisko CSIRT.CZ oficiálne spustilo. Keďže je však pre CERT tímy spolupráca s inými pracoviskami nutnosťou, bolo potrebné nechať tím CSIRT.CZ uznať európskou komunitou, v máji 2008, a neskôr svetovou komunitou tímov CERT, v júni 2009, kedy bolo pracovisko CSIRT.CZ úradom Trusted Introducer oficiálne pripísané na zoznam konštituovaných a svetovo akceptovaných tímov CERT. [17] [20]

Hoci CSIRT.CZ odvtedy zastával rolu vrcholového CERT tímu a plnil jeho funkcie, nebol oficiálne považovaný za národný CERT tím. Zmena nastala podpísaním memoranda medzi združením CZ.NIC a Ministerstvom vnútra Českej republiky na 16. decembra 2010, ktorým bolo pracovisko CSIRT.CZ deklarované Národným CSIRT tímom Českej republiky. Svetovej komunite tímov CERT sa vznik národného CERT tímu CSIRT.CZ oznámil v španielskej Barcelone vo februári 2011. [20]

5.1.1 Memorandum o CERT / CSIRT Českej republiky

Po tom, čo vláda svojím uznesením č. 781 z októbra 2011 rozhodla, že rolu národnej autority pre oblasť kybernetickej bezpečnosti od Ministerstva vnútra preberie Národný bezpečnostný úrad, bolo potrebné uzavrieť nové memorandum práve s NBÚ. Nová zmluva nesie názov Memorandum o Computer Emergency Response Team / Computer Security Incident Response Team české republiky (v práci ďalej len Memorandum) a ide o štvorstranový dokument s účinnosťou od 1. apríla 2012, podpísaný riaditeľom Národného bezpečnostného úradu, Ing. Dušanom Navrátilom a riaditeľom združenia CZ.NIC, Mgr. Ondřejom Filipom MBA. [42]

V ňom sa združenie CZ.NIC zaväzuje k prevádzkovaniu národného CSIRT tímu a plneniu s tým súvisiacich povinností, to znamená, že zabezpečí potrebné akreditácie, plnú funkcionalitu a bezproblémovú prevádzku CSIRT.CZ, ku ktorej musí disponovať dostatočnými technickými a ľudskými zdrojmi. Rovnako sa zaväzuje k spolupráci s NBÚ v súlade s jej pokynmi, napríklad zdieľaniu informácií v prípade bezpečnostného incidentu s vážnym dopadom na siete štátnej správy alebo povinnosti zúčastniť sa medzinárodných akcií na požiadanie NBÚ, či prevedeniu auditu výkonu služby na jeho pokyn. Povinnosťou CZ.NIC je predkladať NBÚ pravidelné správy o činnosti, aspoň raz ročne. [42]

Počas doby, kedy je národný CERT tím prevádzkovaný združením CZ.NIC, ešte nenastala situácia, kvôli ktorej by Národný bezpečnostný úrad bol s činnosťou pracoviska CSIRT.CZ vyslovene

nespokojný. Je nutné si uvedomiť, že CSIRT.CZ bol modelovým pracoviskom a aj z toho dôvodu sa niektoré veci dolaďovali „za pochodu“. NBÚ je za zákonom stanovených podmienok raz za rok predkladaná výročná správa o činnosti národného tímu, ku ktorej má možnosť vyjadriť svoje pripomienky, taktiež nie sú neobvyklé ani neformálne návštevy zástupcov NBÚ na pracovisku CSIRT.CZ či iné neformálne stretnutia. Aj vďaka týmto návštevám, NBÚ vie, čo a ako sa v národnom tíme deje, dohliada nad jeho činnosťou a v prípade potreby má možnosť zakročiť. Keďže podľa Pavla Baštu takáto potreba ešte nenastala, verí, že svoju funkciu národného tímu pracovisko CSIRT.CZ vykonáva maximálne kvalitne a správne. [40]

5.1.2 Výberové riadenie na post prevádzkovateľa národného CERT

Niektoré zmluvy je možné podpísať na dobu neurčitú, no v prípade Memoranda sa jedná o zmluvu podpísanú na konkrétne vymedzený časový úsek. Jeho platnosť by mala končiť s koncom tohto roka. To znamená, že dovtedy musí prebehnúť nové výberové riadenie na post prevádzkovateľa národného tímu CERT. Ten sa vyberá na základe podmienok stanovených zákonom, ktoré sú v práci priblížené v kapitole 4.2.2 Zákon o kybernetickej bezpečnosti (č. 181/2014 Sb.). Podľa Pavla Baštu však Memorandum s týmto faktom počítalo a združenie CZ.NIC sa bude o zisk postu prevádzkovateľa uchádzať znovu. Nie je ale jediné. Rola národného CERT tímu sa stala akousi „značkou kvality“ a o tento post prejavili záujem niektoré komerčné spoločnosti. Zuzana Duračinská dodáva, že zákonné podmienky hovoria jasne a národný CERT musí byť nestranný a nesmie propagovať žiadne konkrétne riešenia a postupy. Rovnako vykonáva túto činnosť bezúplatne, hoci prevádzkovanie a personálne obsadenie má svoje náklady, ktoré znáša CZ.NIC ako prevádzkovateľ, a to si mnohé spoločnosti neuvedomujú. [40]

5.2 Funkcia a služby poskytované CSIRT.CZ

Pracovisko CSIRT.CZ bolo vďaka podpísaniu Memoranda združením CZ.NIC a Národným bezpečnostným úradom menované Národným CSIRT tímom Českej republiky. Zo zmluvy vyplývajú tímu povinnosti, ktoré sú bližšie rozobraté v tejto kapitole.

Základnou podmienkou prevádzkovania národného tímu je podľa zákona jeho bezúplatné prevádzkovanie. To znamená, že všetky náklady spojené s prevádzkovaním pracoviska a jeho služieb nesie prevádzkovateľ, teda združenie CZ.NIC. Rovnako nesmie porušiť podmienku nestrannosti, teda presadzovať konkrétne riešenia a produkty. Pracovisko CSIRT.CZ z postu národného CERT tímu poskytuje mnoho služieb, ktoré sú navzájom prepojené. Pre jednoduchšiu orientáciu sú v tejto práci rozdelené do troch veľkých kategórií a jednej vedľajšej [43]:

- Činnosti súvisiace s riešením bezpečnostných incidentov
- Proaktívna a osvetová činnosť na poli kybernetickej bezpečnosti
- Spolupráca s ostatnými CERT tímami a organizáciami pôsobiacimi v oblasti kybernetickej bezpečnosti na medzinárodnej a národnej úrovni – tejto oblasti sa venuje samostatná kapitola 5.3 Príklady spolupráce pracoviska CSIRT.CZ.

- Činnosti súvisiace s rolou interného bezpečnostného tímu CZ.NIC – činnosti sa nevzťahujú priamo k funkcii národného CERT tímu, preto nie sú v tejto práci bližšie rozobrané.

5.2.1 Činnosti súvisiace s riešením bezpečnostných incidentov

Do tejto kategórie spadajú činnosti vyplývajúce zo zákona a Memoranda. Ide o zriadenie a prevádzku služby na hlásenie bezpečnostných incidentov, ich riešenie a koordináciu riešenia, v prípade CSIRT.CZ je možné ich nahlásiť na telefónnom čísle, e-mailovej adrese aj na webovej stránke pomocou dvoch formulárov. Ako bolo povedané, jeden vhodný pre povinné hlásenie bezpečnostných udalostí osôb a orgánov § 3 písm. a) a b) zákona, pre ktoré pôsobí ako prvotné kontaktné miesto a druhý pre ostatné subjekty. Pole pôsobnosti CSIRT.CZ je totiž celá Česká republika a všetky siete, ich správcovia a všetci užívatelia na jej území, ktorí sa môžu na CSIRT.CZ obrátiť a tím im poskytne pomoc s riešením incidentov alebo radu ohľadom metodického postupu. Národný CERT tím nemá priamy dosah a prostriedky k analýze a priamemu riešeniu každého nahláseného bezpečnostného incidentu, zabezpečuje preto len koordinačnú činnosť potrebnú k odstráneniu problému alebo ochrane ostatných ohrozených subjektov. V prípade potreby poskytne informácie nutné k riešeniu problému národnému CERT tímu, NBÚ, Polícií Českej republiky alebo podá prípad na analýzu forenzným laboratóriám, s ktorými spolupracuje. [43]

Povinnosť triedenia a vyhodnocovania všetkých hlásení prebieha pomocou naimplementovaného ticketovacieho systému OTRS. Kontaktné informácie na správcov sietí sa získavajú z databáze RIPE, prípadne iných databáz RIR. Archivácia a ochrana dát podlieha interným smerniciam združenia. [44]

Úspešnosť riešenia bezpečnostných incidentov

Hoci do kompetencií CSIRT.CZ ako „posledného útočiska“ spadajú všetci užívatelia, v praxi sa s ním do kontaktu dostanú minimálne, napríklad v prípade kedy mu pošlú vzorku nového malwaru, ktorý by mohol byť hrozbou pre ostatných. Bežní užívatelia by mali bezpečnostné incidenty riešiť so správcom svojej siete. Práve správcovia sietí majú incidenty hlásiť. Príklad, spoločnosť dostane podvodný e-mail, ktorý predstavuje potenciálnu hrozbu aj pre ostatné spoločnosti, preto skontaktujú CSIRT.CZ, ktorí následne problém začne riešiť, môže materiál poslať na rozbor forenznému laboratóriu a v prípade potreby varuje pred hrozbou ostatné spoločnosti. V nasledujúcom obrázku (viz Obrázok 5) je možné vidieť štatistiky úspešnosti riešenia bezpečnostných incidentov. Za tento rok sa zatiaľ nepodarilo úspešne vyriešiť 13 incidentov oproti 1063, ktoré boli úspešne vyriešené, nastala pozitívna zmena alebo bol systém varovaný pred prienikom do siete. O 82 incidentov je CSIRT.CZ informovaný a stále v štádiu riešenia. [40]

	2008	2009	2010	2011	2012	2013	2014	2015	sum
Successful	64	149	67	622	4085	180	288	97	5552
IDS Informed						2106	2374	782	5262
Positive change		24	185	119	130	188	413	184	1243
We are informed	164	245	203	20	32	95	176	82	1017
Warning	15	32	158	5					210
Unsuccesful	1	41	20	10	7	47	67	13	206
Admin unable to solve			1						1
sum	244	491	634	776	4254	2616	3318	1158	13491

Obrázok 5: Úspešnosť riešenia nahlásených bezpečnostných incidentov (Zdroj: [45])

Druhy bezpečnostných incidentov a ich trendy

Ticketovací systém, ktorý CSIRT.CZ používa, automaticky triedi nahlásené bezpečnostné incidenty podľa ich druhu. Tento proces umožňuje zaznamenávať a sledovať druh a počet nahlásených bezpečnostných incidentov v jednotlivých rokoch a následne vytvoriť z týchto údajov výstup (viz Obrázok 6), v prípade CSIRT.CZ verejne dostupný na webovej stránke.

	2008	2009	2010	2011	2012	2013	2014	2015	sum
IDS				491	3924	2121	2380	783	9699
Phishing	65	220	209	144	159	175	368	133	1473
Spam	47	28	103	26	43	73	159	37	516
Malware	53	97	42	9	19	44	117	81	462
Other	1	5	8	62	13	75	101	98	363
Virus		121	178	1	1				301
DOS	1	4	2	2	68	72	32	16	197
Trojan	66	6	26	5	5	12	56	17	193
Probe		3	14	25	12	26	86	10	176
Botnet		3	46	5	8	15		1	78
Portscan	10	4	1	6	1	3	2		27
Pharming							18		18
Crack	1		4						5
Copyright			1		1				2
sum	244	491	634	776	4254	2616	3319	1176	13510

Obrázok 6: Štatistika riešených bezpečnostných incidentov – druhy (Zdroj: [45])

Podľa štatistiky sú v tomto roku najčastejšie hlásené bezpečnostné incidenty IDS prieniky, malwary a phishingové pokusy. Tieto čísla sa ale nemôžu reflektovať ako dianie každej bežnej siete v rámci celej republiky. CSIRT.CZ pôsobí ako „posledné útočisko“, a preto sa k nemu dostávajú len informácie o incidentoch, ktoré je zo zákona povinné hlásiť alebo môžu potenciálne ohroziť aj iné subjekty a preto vyžadujú koordináciu viacerých subjektov. Aj podľa Pavla Baštu ide o špičku ľadovca, pretože správcovia sietí si uvedomujú, ktoré incidenty má zmysel hlásiť. Príkladom je

početnosť hlásení phishingu, ktorého identifikácie nie je náročná a teda je správca siete schopný takýto problém rozpoznať. Zároveň je to informácia, ktorá vo väčšine prípadov zaujíma aj iné subjekty, ktoré môžu byť potenciálne ohrozené. Naopak, hoci je skenovanie portov viac ako častou záležitosťou v reálnom živote, nie je tak očividné a nebezpečné, ergo sa k národnému CERT tímu hlásenie o takomto incidente dostane v menšom zastúpení. [40]

Rovnako je v štatistike možné postrehnúť trendy a výkyvy v popularite konkrétnych útokov. Príkladom je vlna DoS útokov, ktorá sa zdvihla v roku 2012 na základe rastúcej popularity skupiny Anonymous. Postupom času aj táto vlna opäť začala klesať a momentálnym trendom sú výrazne personalizované e-maily. Tie sú oproti starším verziám písaným v anglickom jazyku zamerané priamo na českého užívateľa. Okrem textu v českom jazyku obsahujú skutočné mená exekútorov a ich pravé telefónne čísla. Mesačné správy o konkrétnych bezpečnostných incidentoch je možné nájsť aj na webovej stránke vládneho CERT tímu[4], avšak tieto publikácie sú postavené len na správach, ktoré sa už objavili v médiách a na Internete. Ako sa vyjadrila v rozhovore Zuzana Duračinská, ani vládny, ani národný tím CERT nesmú zverejňovať konkrétne informácie o nahlásených bezpečnostných incidentoch a subjektoch, ktoré ich nahlásili a bežný užívateľ sa k nim rozhodne nedostane. Takýto únik informácií by mohol mať negatívny dopad na dobré meno spoločnosti a spôsobiť škody. Pre bežného užívateľa alebo správcu siete majú však tieto mesačné správy informačnú a osvetovú funkciu. [40]

5.2.2 Príklad koordinácie pri riešení bezpečnostného incidentu

Zaťažkávajúca skúška, ktorá otestovala schopnosť tímu CSIRT.CZ koordinovať viaceré subjekty a úspešne vyriešiť bezpečnostný incident celoplošného charakteru prebehla v dňoch 4. až 7. marca 2013, kedy bola prevedená séria doposiaľ najvýraznejších DoS útokov na služby viacerých webových stránok prevádzkovaných v Českej republike. Prípad vďaka svojmu rozsahu priťahoval vysokú pozornosť médií aj obyvateľstva. DoS útoky boli vedené v dvoch časových vlnách, v rannej vlne od 9 do 11 hodiny a v poobednej vlne od 14 do 16 hodiny, každodenne po dobu štyroch dní, pričom boli cielené na vybrané skupiny webových serverov meniace sa každý deň. V prvý deň, 4. marca, boli napadnuté najviac navštevované on-line mediálne zdroje ako iDNES.cz, Lidovky.cz, Csfd.cz či Živě.cz. Druhý deň boli z dôvodu útokov na hodinu a pol nedostupné služby vyhľadávacích www stránok Seznam.cz. Tretí deň útoky v čase 9:30 do 11:00 postihli webové stránky bánk ČSOB, Fio, Komerčnej banky, Českej sporiteľne, Raiffeisen banky a dokonca aj Českej národnej banky. Poobedná vlna bola namierená už len na stránky Českej sporiteľne, u ktorej následkom útokov vypadli služby e-commerce a niektorých platobných terminálov. Posledný deň, 7. marca, prebehli posledné zaznamenané útoky na webové stránky mobilných operátorov Telefónica O2 a T-mobile, rovnako webové stránky dpp.cz. Zdroj útokov pochádzal zo siete RETN, http://www.retn.net/en/, ktorej prevádzkovateľ bol CSIRT.CZ tímom okamžite skontaktovaný, avšak bez reakcie a zablokovania útokov. Hlavnou metódou použitou DoS útokmi bol mechanizmus SYN Flood, ktorý cez podstrčenú falošnú IP adresu vysiela veľké množstvo požiadavkou na

[4] Mesačné správy o bezpečnostných incidentoch v krajine a vo svete tvorené vládnym pracoviskom CERT sú prístupné na webovej stránke, v sekcii Publikace: http://www.govcert.cz/cs/informacni-servis/bulletiny/

konkrétny bod alebo službu siete, následkom čoho sú kapacity a zdroje systému vypotrebované, systém je preťažený a ostatným užívateľom nedostupný. [46]

Prvé žiadosti o informácie a pomoc v prípade útokov CSIRT.CZ tím obdržal od prevádzkovateľov sietí už poobede prvého dňa, na prípade začal tím pracovať, kontaktoval správcu siete RETN a 6. marca, kedy prebiehali DoS útoky na sieť Českej sporiteľne majúce najvážnejší charakter, formou videokonferenčného hovoru vytvoril pracovnú skupinu pozostávajúcu zo špecialistov z tímu CSIRT.CZ, CESNET, GTS a odborníkov priamo z Českej sporiteľne. Cieľom bolo pomocou diskusie a analýzy dôjsť k najúčinnejšej forme ochrany, pričom z preventívnych dôvodov bola v pohotovosti aj počas nasledujúcich dvoch dní. Paralelne s touto pracovnou skupinou bola v priestoroch združenia CZ.NIC vytvorená skupina z pracovníkov CSIRT.CZ, CZ.NIC a PR špecialistov, ktorej úlohou bola koordinácia všetkých zložiek zapojených v riešení útokov, koncentrácia dát a informácií o útokoch, ich šírenie a komunikácia s prevádzkovateľmi napadnutých sietí, Národným centrom pre kybernetickú bezpečnosť, médiami a subjektmi, ktoré sa mohli stať potenciálnym nasledujúcim cieľom útoku. Im a im sieťovým správcom boli poskytnuté informácie o útoku a zabezpečeniu ochrany, rovnako ako o postupe v prípade napadnutia. [46]

5.2.3 Proaktívna a osvetová činnosť na poli kybernetickej bezpečnosti

Hlavným cieľom služieb v kategórii proaktívna a osvetová činnosť je zdvihnúť povedomie v oblasti kybernetickej bezpečnosti, šíriť informovanosť medzi užívateľmi a poskytnúť služby v oblasti prevencie bezpečnostných incidentov.

Zákon stanovuje národnému CERT tímu povinnosť šíriť informácie nadobudnuté na medzinárodnej a národnej úrovni, to znamená zverejňovať nové správy a trendy zo sveta získané na medzinárodných konferenciách či informácie z domácej sféry kybernetickej bezpečnosti prevzaté z hlásení bezpečnostných incidentov alebo vzájomnej komunikácie medzi ostatnými CERT tímami v rámci Českej republiky, vrátane vládneho tímu GovCERT.CZ. Najrýchlejším a širokému publiku najdostupnejším spôsobom komunikácie a predávania informácií je ich zverejňovanie na webových stránkach www.csirt.cz v rubrike Aktuálne z bezpečnosti, v ktorej sa formou stručných správ užívateľ dozvie o dianí a novinkách zo sveta aj domova, napríklad varovanie klientov Českej sporiteľne pred prebiehajúcimi podvodmi na sociálnej sieti Facebook z dňa 9. apríla 2015 alebo upozornenie na chybu v programe BitTorrent Sync z dňa 8. apríla 2015. [47]

Hoci cieľovou skupinou týchto správ sú správcovia a administrátori sietí, ktorí majú možnosť informácie predať ďalej, správy sú určené aj pre bežných užívateľov, ktorí sú podľa Zuzany Duračinskej a Pavla Baštu, pôsobiacich v CSIRT.CZ ako špecialisti počítačovej bezpečnosti, počítačovo gramotní a vedia s počítačmi zachádzať a využívať ich na vysokej úrovni, ale potenciálne hrozby stále podceňujú. Pritom hrozby sa časom stali sofistikovanejšie a stále sa vyvíjajú. Podcenenie rizika aj pri každodenných činnostiach ako je prihlasovanie sa k Facebook kontu, môže viesť k získaniu prihlasovacích a následne osobných údajov a ohrozeniu ľudí vo vašich kontaktoch. Aj z tohto dôvodu CSIRT.CZ ponúka služby v oblasti osvety vo forme prednášok, seminárov, školení a stretnutí, o ktoré môže požiadať prakticky ktokoľvek s úmyslom zdvihnúť bezpečnostné povedomie, pričom nemusí ísť o vyslovene technické publikum. Tím CSIRT.CZ v minulosti spolupracoval s viacerými vzdelávacími inštitúciami, súkromnými organizáciami,

štátnou správou či dokonca s Políciou ČR, pre ktorú zorganizoval úspešné školenie s účasťou cez 100 ľudí. Školenie malo tri časti. Prvá zameraná na využitie Internetu všeobecne, druhá na vyťaženie informácií o vyšetrovanom pomocou Internetu, napríklad ako nájsť jeho väzby na sociálnych sieťach. Posledná časť patrila forenznej analýze a očakávaniam, ktoré Polícia môže mať v tejto oblasti, napríklad zisk informácií o navštevovaných stránkach. Školenie dokáže prispôsobiť na mieru ako v prípade školenia pre České technické učení alebo pri momentálne prebiehajúcom projekte, ktorí bude patriť učiteľom informatiky na konkrétnej škole. [40]

Na pravidelnej báze prebieha v spolupráci s Akadémiou CZ.NIC dvojdňové školenie Počítačová bezpečnosť prakticky, vedené lektorom Pavlom Baštom. Platené školenie je určené predovšetkým správcom a administrátorom sietí, ktorým sú predstavené kybernetické útoky z teoretickej aj praktickej stránky, vrátane metód prevencie a obrany[5]. [48]

Projekt Lovci záhad, televízny program, bol zameraný na šírenie osvety medzi deťmi. Iný televízny projekt, Ako na Internet, mal vďaka odvysielaniu pred hlavnými správami veľký dosah, čo bolo jeho zámerom. [40] Išlo o osvetový projekt v spolupráci so združením CZ.NIC, ktorý sa vo forme dvojminútových videí snažil divákom priblížiť problematiku Internetu a bezpečnosti na ňom. Videami sprevádzal Roman Zach, pričom ku každému videu je možné získať bližšie informácie o téme v podobe sprievodného textu. Oblasti, ktorým sa projekt venoval je osem, každá skupina obsahuje 8 až 14 videí, rozoberajúca témy od autorského práva, cez internetové zoznamovacie služby, po šifrovanie. [49]

Služby z oblasti proaktívnej činnosti sú zamerané na prevenciu a včasnú ochranu siete a systémov pred napadnutím a predídenie bezpečnostným incidentom. Príkladom je Skener webov, bezplatná služba poskytovaná na objednávku tímom CSIRT.CZ, ktorá sa pomocou automatických aj ručných testov snaží odhaliť bezpečnostné slabiny aplikácií na webových stránkach objednávateľa, ktorého následne informuje o náleze a miere rizika, ktoré so sebou prináša, rovnako ako o vhodnom spôsobe jeho odstránenia. S cieľom sledovania, kontroly a riešenia hrozieb v doméne .CZ bola vyvinutá open-source aplikácia Malicious Domain Manager, ktorá zbiera a vyhodnocuje informácie o rizikových URL adresách v doméne, ukladá ich do histórie a vlastníka konkrétnej domény informuje o hrozbe pomocou e-mailovej správy. Záujemcovia pri splnení určitých podmienok môžu požiadať Laboratórium CZ.NIC o rovnako záťažové testy, ktoré svojou silou a intenzitou napodobujú DoS útoky z marca roku 2013. Táto služba je bezplatne poskytovaná v spolupráci s CSIRT.CZ tímom. V oblasti neoprávneného a rizikového prieniku do systému CSIRT.CZ za spoluúčasti združenia CESNET poskytuje službu detekcie a zaznamenávania takýchto pripojení v rámci siete Internet. Intrusion Detection System po spozorovaní podozrivej IP adresy alebo pripojenia kontaktuje administrátora siete pomocou e-mailovej správy s detailnejšími informáciami o potenciálnom útoku. Poslednou preventívnou službou, ktorú národný tím CERT ponúka v rámci spolupráce s Laboratóriom CZ.NIC je projekt Honeynet, ktorý na webovej stránke https://honeymap.cz/ zobrazuje sieť nastražených honeypotov a prebiehajúce útoky. V prípade spozorovania ešte nepreskúmaného malwaru je podrobený bližšej analýze. [43]

---

[5] Na školenie Počítačová bezpečnosť prakticky je nutné sa vopred prihlásiť na stránkach Akadémie CZ.NIC: https://akademie.nic.cz/akademie/course/79/detail/.

Pracovisko CSIRT.CZ momentálne pripravuje vlastný dlhodobý výskumný projekt zameraný na získavanie dát z hlásení bezpečnostných incidentov a vybudovanie systému umožňujúceho osloviť užívateľov zapojených do starých botnetov, o ktorých je možné získať informácie zatiaľ len sprostredkovanou cestou cez zdroje ako je tím Cymru alebo ShadowServer. Rovnako je cieľom takto získané údaje systémom analyzovať a zistiť trendy v oblasti bezpečnostných incidentov. [40]

5.2.4 Financovanie prevádzky CSIRT.CZ

Ako bolo povedané pri téme potenciálnych záujemcov o post národného CERT tímu, pozícia národného CERT tímu je vyslovene lukratívna z komerčného hľadiska. Odhliadnuc od povinnosti byť nestranným orgánom a teda nezneužívať situáciu k propagácií svojich produktov, je v Zákone o kybernetickej bezpečnosti povinnosť vykonávať prevádzkovanie národného CERT tímu bezúplatne.

Taktiež z memoranda medzi CZ.NIC a NBÚ, podpísaného ešte pred vstupom zákona do účinnosti, vyplýva, že združenie CZ.NIC nesie všetky náklady spojené s prevádzkou CSIRT.CZ a NBÚ sa financovania nepodieľa. Výnimkou je získanie grantu za splnených podmienok alebo pomoc pri žiadaní o finančnú podporu z Európskych fondov. [42]

Napriek faktoru bezúplatného vykonávania činnosti môže byť post prevádzkovateľa lákavý zo spomínaného reklamného hľadiska, prevádzkovateľ získa štatút najvyššieho odborníka v oblasti zabezpečenia a ochrany informačných systémov, čo mu pridáva na dôveryhodnosti, získa možnosť účasti na konferenciách a cvičeniach s čím prichádza rozšírenie kontaktov v krajine aj celosvetovo a v neposlednom rade získa príležitosť rozvíjať a uplatniť svoje nápady a myšlienky v oblasti kybernetickej bezpečnosti.

5.3 Príklady spolupráce pracoviska CSIRT.CZ

Keďže vzájomná spolupráca CERT tímov či už na medzinárodnej, alebo národnej úrovni je základom budovania väzieb pre zdieľanie informácií a následný rozvoj tímov, táto kapitola bakalárskej práce sa venuje práve projektom spolupráce, v ktorých je zapojený národný tím CSIRT.CZ.

5.3.1 Spolupráca na medzinárodnej úrovni

Prvým úradom, ktorý CSIRT.CZ oficiálne akreditoval na medzinárodnej úrovni bol úrad Trusted Introducer pôsobiaci v rámci organizácie TERENA, ktorá zastrešuje prevažne európske tímy spĺňajúce členské predpoklady. Poskytuje priestor na prezentovanie CERT tímov, konkrétnych prípadov a skúseností, s ktorými sa stretli, pričom všetko prebieha v rámci uzavretých fór umožňujúcich rozbor, ich analyzovanie a diskusiu. Trusted Introducer usporadúva pravidelné spoločné stretnutia tímov 2 až 3-krát za rok so samozrejmou účasťou pracoviska CSIRT.CZ. Druhou medzinárodnou organizáciou fungujúcou ako celosvetové fórum je organizácia FIRST. Spoločné stretnutie organizuje raz za rok a národný tím CSIRT.CZ sa ho zúčastňuje aj napriek tomu, že momentálne nie je

oficiálnym členom. O zisk členstva sa však snaží a dúfa, že sa stane oficiálnou súčasťou ešte v priebehu tohto roka. CERT tímy pôsobiace v Českej republike, ktorá je súčasťou Európskej únie, získavajú možnosť účasti na cvičeniach, seminároch a konferenciách organizovaných agentúrou ENISA. V rámci spolupráce s agentúrou ENISA je CISRT.CZ momentálne koordinátorom celoeurópskych cvičení za Českú republiku, ktoré nesú názov CYBER Europe, prebiehajú každé dva roky a tímy si vďaka nim môžu precvičiť a otestovať svoje schopnosti spolupráce pri simuláciách kybernetických útokov. [40]

Pred dvoma rokmi, v máji 2013, na podnet Národného bezpečnostného úradu vznikla platforma CECSP, Central Europe Cyber Security Platform, ktorej členmi sú tímy z krajín Vyšegráckej štvorky a Rakúska, vrátane CSIRT.CZ. Hlavným dôvodom bolo vytvorenie medzinárodnej organizácie s menším počtom tímov, ktoré dovoľuje nadviazať bližšie vzťahy medzi tímami, budovať dôveru a hlbšiu spoluprácu formou spoločných projektov. Bezpečnostní technici CSIRT.CZ tímu sa rovnako pravidelne zúčastňujú neverejných konferencií zameraných na bezpečnostnú komunitu CSIRT tímov, ktoré si CSIRT tímy organizujú samé. Prebiehajú v Estónsku v rovnakých dňoch ako konferencia FIRST, ale sústreďuje sa na technické aspekty kybernetických útokov a ich detaily. [35]

Najnovším medzinárodným projektom, v ktorého čele stojí CSIRT.CZ je jeden rok trvajúci projekt vzájomného zdieľania informácií a budovania spolupráce CS DANUBE, Kybernetická bezpečnosť v Podunají, ktorého účastníkmi sú CERT tímy zo Slovenska, Rakúska, Chorvátska, Srbska a Moldavska. [50]

5.3.2 Spolupráca na národnej úrovni

Spolupráca medzi národným CERT tímom, vládnym CERT tímom a Národným bezpečnostným úradom je upravená v Zákone o kybernetickej bezpečnosti, ergo bližšie rozobraná bola v kapitole zameranej na zákon a jeho obsah. Tím CSIRT.CZ ale prichádza s NBÚ do styku aj v roli spoluorganizátora cvičnej akcie CyberCzech orientovanej na testovanie znalostí zástupcov z rôznych štátnych orgánov v oblasti kybernetickej bezpečnosti formou riešenia simulovaných situácií. [40]

Pod záštitu tímu CSIRT.CZ od 15. apríla 2008 taktiež patrí pravidelná organizácia pracovnej skupiny CSIRT.CZ, v podobe otvoreného fóra pre bezpečnostných analytikov a iných odborníkov z oblasti kybernetickej bezpečnosti ako sú operátori, správcovia sietí či zástupcovia organizácií spadajúcich do kategórie významných informačných systémov , ktorí sa stretávajú 2 až 3-krát do roka, aby prediskutovali súčasné bezpečnostné problémy, aktuálne hrozby, spôsoby riešenia a možnosti spolupráce. Účasť na stretnutí je možné dohodnúť po skontaktovaní tímu CSIRT.CZ na e-mailovej adrese info@csirt.cz. Pracovná skupina sa stretávala aj počas príprav nového Zákona o kybernetickej bezpečnosti, kedy cieľom schôdzí bolo komentovať a pripomienkovať návrh zákona, identifikovať a odstrániť prípadné nedostatky. [40] [43]

K najvýraznejším projektom za poslednú dobu, pri ktorých vzniku CSIRT.CZ stál, patrí projekt FENIX vytvorený ako reakcia na DoS útoky z marca 2013. FENIX predstavuje platformu, bezpečnú VLAN sieť, ktorá v prípade opätovného ohrozenia a výpadku webových služieb jej členov

umožní ich sprevádzkovanie a dostupnosť českým užívateľom. Prísne podmienky[6] vstupu organizácií do projektu, medzi ktoré patrí napríklad existencia vlastného CERT tímu či získanie doporučení od dvoch už aktívnych členov, zachovávajú integritu a bezpečnosť siete. Medzi momentálmomentálnych členov okrem zakladajúcich CZ.NIC a NIX.CZ patria Seznam.cz, Telefónica O2 či Dial Telecom. [51]

Tým, že Česká republika patrí medzi menšie krajiny s menším počtom CERT tímov, vzťahy medzi tímami na národnej úrovni sú oproti úrovni medzinárodnej omnoho bližšie a spolupráca tesnejšia. Rovnako CSIRT.CZ ako národný CERT tím ponúka pomoc pri zakladaní nových CERT tímov a ich integrácií do medzinárodnej infraštruktúry. Platí totiž podmienka, že tím, ktorí sa pokúša o zaradenie do zoznamu napríklad úradu Trusted Introducer, musí byť podporovaný iným už akreditovaným tímom pôsobiacim v organizácií. Členovia tímu sa teda častokrát poznajú na osobnej báze, preto nie je problém získať názor na konkrétny problém aj z iných pracovísk. Práve tak je sám oslovovaný s otázkami týkajúcich sa bezpečnostných incidentov ostatnými tímami a poskytuje konzultačné služby kriminálnemu oddeleniu Polície ČR. Keďže CSIRT.CZ sa nevenuje priamo forenznému vyšetrovaniu bezpečnostných incidentov, naviazal po oslovení spoluprácu s forenzným laboratóriom spoločnosti Avast, ktorému posiela na analýzu vzorky nových, ešte nepreskúmaných škodlivých softwarov, prípadne pri incidente väčších rozmerov skontaktuje viaceré forenzné laboratória. [40][43]

Spolupráca s ostatnými subjektmi z oblasti kybernetickej bezpečnosti je v prípade CSIRT.CZ ako koordinačného strediska pre Českú republiku, kľúčová. S ponukou ho však môže osloviť ktokoľvek aj mimo komunitu CERT tímov, pričom tieto projekty väčšinou spadajú pod služby tímu CSIRT.CZ v osvetovej činnosti ako sú prednášky alebo školenia. Za všetky je možné spomenúť spoluprácu s organizáciou Safer Internet, zameranú primárne na dvíhanie bezpečnostného povedomia u detí. [40]

5.4 Technické a organizačné zázemie tímu CSIRT.CZ

Aby bolo pracovisko schopné vykonávať všetky svoje role a plniť všetky svoje povinnosti a funkcie, musí stáť na kvalitných základoch. Tie sú v prípade CERT tímu tvorené okrem technologického zázemia, vrátane komunikačných kanálov, aj ľudskými zdrojmi.

5.4.1 Komunikačné kanály

Komunikačnými kanálmi sa rozumejú cesty, pomocou ktorých je možné sa s tímom CSIRT.CZ skontaktovať či ide o prípad hlásenia bezpečnostného incidentu, komunikáciu medzi viacerými tímami, alebo snahu skontaktovať prevádzkovateľa národného tímu.

---

[6] Všetky podmienky potrebné k vstupu organizácie do projektu FENIX sú dostupné v on-line PDF dokumente: http://nix.cz/cs/file/NIX_PRAVIDLA_FENIX

Hlásenie bezpečnostných incidentov

Kontakty na národný tím je možné vyhľadať priamo na ich webovej stránke www.csirt.cz, ktorá je rovnako formou komunikačného kanálu distribuujúceho informácie. Podstránka Kontaktné informácie obsahuje telefónne číslo (+420 910 101 010) , prípadne telefónne číslo pre urgentné prípady (+420 222 745 111), e-mailovú adresu na zasielanie hlásení (abuse@csirt.cz**)** a pracovnú dobu, počas ktorej sa bezpečnostné incidenty riešia. Tá je pre CSIRT.CZ konkrétne od 09:00 – 17:00, každý pracovný deň. V prípade, že dôvodom kontaktu nie je hlásenie bezpečnostných incidentov, webová stránka ponúka všeobecnú e-mailovú adresu, kontakt na prevádzkovateľa alebo PR manažéra. [52]

Webová stránka taktiež obsahuje dva formuláre umožňujúce nahlásiť bezpečnostný incident, plus návod a pokyny ako postupovať pri hlásení incidentu. Jeden sa vzťahuje priamo k Zákonu o kybernetickej bezpečnosti a vyplňovať ho majú orgány a osoby vymedzené zákonom. Druhý patrí ostatným subjektom a bezpečnostným incidentom, ktoré sa netýkajú zákona, ide napríklad o bežných užívateľov či poskytovateľov služieb. Rozdelenie je dôležité z toho dôvodu, že každý formulár spadá do inej fronty v ticketovacom systéme, na základe ktorej sa s ním pracuje. Prípady, kedy by sa k tímu dostali hlásenia, ktoré im reálne nepatria, nie sú časté. Ide o číslo v jednotkách za rok. Nový zákon presne vymedzil kritéria a rozdelenie subjektov na prvky kritickej informačnej infraštruktúry a významné informačné systémy, ktorým dáva povinnosť hlásiť bezpečnostné incidenty národnému alebo vládnemu CERT tímu. Vďaka tomu majú organizácie jasný prehľad a nesprávne hlásené incidenty nie sú bežné. Neznamená to však, že prvky kritickej infraštruktúry spadajúce pod vládny CERT nesmú podávať žiadny informácie národnému CERT tímu. Ak považujú bezpečnostný incident potenciálnou plošnou hrozbou, môžu skontaktovať CSIRT.CZ, aby o hrozbe informoval ostatné subjekty. [40]

Chatovacia miestnosť

Ako bolo už povedané, spolupráca je základom dobrej kooperácie medzi tímami pri riešení bezpečnostného incidentu. Okrem tradične využívaných prostriedkov ako je e-mail alebo telefón, CSIRT.CZ komunikuje s ostatnými tímami pomocou privátnej „chatovacej miestnosti“, ako ju nazval Pavel Bašta. Vznikla za účelom rýchlejšej komunikácie v rámci malej skupiny CERT tímov Českej republiky, ktoré do nej patria. Keďže ide o službu len pre vybrané subjekty, nie je možné poskytnúť bližšie informácie o jej lokalite. [40]

5.4.2 Základné softwarové vybavenie CSIRT.CZ

Zo zákona vyplýva národnému CERT tímu povinnosť spracovávať a uchovávať informácie o nahlásených bezpečnostných incidentoch, neurčuje však konkrétne aký systém majú za týmto účelom používať. Softwarovým jadrom celého procesu hlásenia bezpečnostných incidentov v prípade CSIRT.CZ je ticketovací systém OTRS. Nástroj automaticky spravujúci informácie o všetkých nahlásených incidentoch patrí k open-source systémom, to znamená, že každý užívateľ má možnosť si ho prispôsobiť. Takéto úpravy má aj OTRS tímu CSIRT.CZ. Prvou úpravou je rozdelenie hlásení systémom do dvoch front, hlásenia vyplývajúce zo zákonnej povinnosti a ostatné hlásenia, podľa druhu vyplneného formulára. Pri každom hlásení zároveň systém automaticky zobrazí IP

adresu odosielateľa, kontaktné údaje na správcu siete, základné informácie o napadnutej sieti a pravdepodobný druh problému, respektíve bezpečnostného incidentu. Systém všetky informácie spracováva a vyhodnocuje, výstupom môže byť napríklad aj štatistika o najčastejších druhoch hlásených incidentov. Systém je navrhnutý tak, aby sa dokázal z prípadných ručných opráv jeho zaradenia učiť a v identifikácií zlepšovať. [40]

V situáciách, kedy treba informácie o internetových sieťach, ich správcoch a údaje o doménach TLD dohľadať, sa na dennej báze využíva databáza RIPE, jedna z organizáciou ENISA odporúčaných informačných zdrojov. Zaznamenané dáta sú archivované a zálohované podľa interných smerníc pracoviska. Všetky systémy pracujú na platforme operačného systému Linux, ktorý je pokladaný za všestranne použiteľný. K dispozícií je na pracovisku dostupný aj software VMware, používaný pri forenznej analýze alebo iných účeloch. [44]

Pokiaľ ide o bezpečnosť informácií, e-mailová komunikácia v rámci tímu CSIRT.CZ aj v rámci komunikácie s ostatnými tímami je šifrovaná pomocou PGP kľúčov. Na webovej stránke je zverejnený PGP kľúč pre centrálnu e-mailovú adresu abuse@csirt.cz [52]:

- User ID: CSIRT.CZ Abuse team abuse@csirt.cz
- KeyID: 46A050CA
- Key size: 1024
- Key fingerprint = 22E9 699B 099E 2226 000A 00A5 013F F6B9 46A0 50CA

Rovnako každý člen tímu má vytvorený svoj vlastný PGP kľúč k svojej e-mailovej adrese. Samozrejmosťou je ochrana firewallom a využitie iných bezpečnostných softwarov ako sú antivírové scanery a pod. [44] [53]

5.4.3 Organizačný tím CSIRT.CZ

Momentálne tvorí tím CSIRT.CZ osem členov, čo je podľa ENISA štandardu optimálny počet. Vedúcim bezpečnostného tímu CSIRT.CZ je Martin Peterka, ktorý pôsobí súčasne ako prevádzkový riaditeľ CZ.NIC. Reprezentáciu tímu na medzinárodnej aj národnej úrovni, komunikáciu a strategický rozvoj zabezpečuje Andrea Kropáčová, ktorá pôsobí v tíme už od jeho založenia. Ako bezpečnostný špecialista v tíme pracuje Pavel Bašta, Michal Prokop, Zuzana Duračinská, Katarína Ďurechová, Edvard Rejthar a najnovšie Robert Šefr. Každý z nich má v tíme špecifickú úlohu či ide o prípravu kybernetických cvičení a prevádzkovanie služby Skener webov Zuzanou Duračinskou, alebo analýzu škodlivých kódov na českých doménach v prípade Edvarda Rejthara, ale vzájomná spolupráca funguje aj v rámci tímu, hlavne ak je kvôli rozsahu bezpečnostného incidentu nutné koordinovať celoplošné a rozsiahle akcie. [54]

Pokiaľ ide o prijímanie nových členov, väčšinou sa najímajú skúsení technici, ktorí sa v téme kybernetickej bezpečnosti následne doškolia. Správny správca siete alebo administrátor sa v oblasti orientuje, základy a skúsenosti s ňou teda má. [40]

5.5 Záverečné porovnanie formou tabuľky

Všetky dôležité informácie, ktoré boli doteraz v tejto bakalárskej práci prezentované či už pri rozbore Zákona o kybernetickej bezpečnosti č. 181/2014 Sb. a jeho sprievodných dokumentov, alebo odporúčaní z príručky CSIRT Setting up Guide vytvorenej agentúrou ENISA ako pomôcku pri zakladaní tímu, je možné zhrnúť v komplexný celok podkladových informácií a následne porovnať s konkrétnymi údajmi z pracoviska Národného CSIRT tímu Českej republiky, CSIRT.CZ, v podobe prehľadnej tabuľky. Ľavý stĺpec Kategória pomenúva oblasť, z ktorej pochádza konkrétne odporúčanie alebo povinnosť prezentovaná v prostrednom stĺpci Návrh. Reálne aplikované riešenie alebo forma spracovania pracoviskom CSIRT.CZ je predložená v poslednom stĺpci tabuľky, Národný CERT tím CSIRT.CZ.

Pri bližšom pohľade do tabuľky je viditeľné, že Národný CSIRT tím Českej republiky CSIRT.CZ, momentálne prevádzkovaný združením CZ.NIC, vykonáva svoju funkciu plne v súlade zo zákonom aj odporúčaniami agentúry ENISA vo všetkých smeroch a oblastiach, ktoré súvisia s jeho podstatou. Združenie spĺňa všetkých sedem podmienok pre získanie postu prevádzkovateľa národného CERT tímu. CSIRT.CZ vykonáva všetky povinnosti uložené zákonom či navrhované agentúrou ENISA, predovšetkým v oblasti koordinácie a riešenia bezpečnostných incidentov, ako v prípade DoS útokov v marci 2013, vlastného plánovaného výskumu a vývoja nástrojov ochrany, spolupráce medzi CERT tímami a inými subjektmi pôsobiacimi v kybernetickej bezpečnosti na medzinárodnej aj národnej úrovni v podobe účasti na konferenciách, spolupráce na projektoch ako FENIX alebo osvetovej a proaktívnej činnosti zameranej na dvíhanie bezpečnostného povedomia v organizáciách aj medzi bežnými obyvateľmi poskytovanými školeniami a prednáškami. Neplatené služby skenovania webov alebo testovania bezpečnosti voči DoS útokom sú poskytované v rámci preventívnych opatrení a zabezpečenia ochrany sietí. Medzi kľúčové povinnosti patria jednoznačne prijímanie a spracovávanie hlásení o bezpečnostných incidentoch či už cez vyvesený on-line formulár na webových stránkach alebo inou komunikačnou formou na základe zverejnených kontaktných informácií. Zhoda nastáva aj v technickej oblasti. Výnimkou v tabuľke sú dva atribúty, v ktorých sa CSIRT.CZ od návrhu odlišuje, vyplývajú však z podstaty národného CERT tímu, ktorý nepôsobí ako komerčný CERT tím, a preto jeho zložky nie je možné vnímať ako platiacich zákazníkov, ergo nevyvstáva potreba využívať CRM software riadenia starostlivosti o zákazníkov. Rovnako zákon neukladá národnému tímu povinnosť analyzovať bezpečnostné incidenty na forenznej úrovni, preto CSIRT.CZ spolupracuje s externými forenznými laboratóriami.

Tabuľka 1: Porovnanie požiadaviek zákona a odporúčaní ENISA s pracoviskom CSIRT.CZ

Kategória	Návrh	Národný CERT tím CSIRT.CZ
Podmienky postu prevádzkovateľa národného CERT tímu	Právnická osoba [4]	Prevádzkovateľ CZ.NIC je Záujmovým združením právnických osôb [41]
	Uzavretie verejnoprávnej zmluvy s NBÚ [4]	Podpis Memoranda o CERT / CSIRT České republiky s nástupom účinnosti 1. apríla 2012 [20]

Kategória	Návrh	Národný CERT tím CSIRT.CZ
	Predchádzajúce skúsenosti s prevádzkou alebo správou informačných systémov v rozsahu min. 5 rokov [4]	Založenie CSIRT tímu 3. apríla 2008 a následné prevádzkovanie činnosti v oblasti [20]
	Členstvo v nadnárodnej organizácií zameranej na kybernetickú bezpečnosť [4]	Zápis CSIRT.CZ do zoznamu akreditovaných CERT tímov úradu Trusted Introducer, organizácie TERENA, v júni 2009 [20]
	Výkon činnosti národného CERT tímu bezúplatne voči štátu [4]	Všetci náklady na prevádzkovanie nesie podľa klauzule Memoranda združenie CZ.NIC [42]
	Technické predpoklady [4]	Operačný systém, ticketovací systém, bezpečnostné softwary a zabezpečenie elektronickej komunikácie, dostupné komunikačné kanály [40]
	Zverejnenie kontaktných údajov na prevádzkovateľa na webových stránkach národného tímu [4]	Odkaz Kontakt na prevádzkovateľa na webovej stránke https://www.csirt.cz/page/887/kontakt/ [52]
Povinnosti národného CERT tímu	Budovanie a rozvíjanie agendy národného CERT tímu [42]	Spolupráca pri tvorbe a pripomienkovaní návrhu Zákona o kybernetickej bezpečnosti a organizácia schôdzí pracovnej skupiny za týmto účelom [40]
	Príjem hlásení o bezpečnostných incidentov a kontaktných údajov od orgánov § 3 písm. a) a b) podľa zákona č. 181/2014 Sb. (viz Príloha 3) [4]	K dispozícií webová stránka s on-line formulárom na hlásenie bezpečnostného incidentu podľa zákona (viz Príloha 5), e-mailová adresa, telefónne číslo a poštová adresa [52] [55]
	Príjem hlásení o bezpečnostných incidentov a kontaktných údajov od orgánov (viz Príloha 1) [18]	K dispozícií webová stránka s on-line formulárom na hlásenie bezpečnostného incidentu (viz Príloha 4), e-mailová adresa, telefónne číslo a poštová adresa[56]
	Evidovať informácie o bezpečnostných incidentoch a kontaktné údaje [4]	Nahláseným bezpečnostným incidentom je pridelené ticketovacím systémom identifikačné číslo a následne sú systémom triedené podľa druhu a spracovávané [40]
	Uchovávať informácie o bezpečnostných incidentoch a kontaktné údaje [4]	Všetky informácie sú uchovávané a zálohované podľa interných smerníc združenia CZ.NIC [44]
	Vyhodnocovať nahlásené bezpečnostné incidenty [4]	Ticketovací systém spracováva a vyhodnocuje informácie o bezpečnostných incidentoch, ich druhoch a stave riešenia, ktoré sú následne zverejnené na webovej stránke v rubrike Štatistiky riešených incidentov [45]

Kategória	Návrh	Národný CERT tím CSIRT.CZ
	Zdieľanie informácií v oblasti kybernetickej bezpečnosti [42]	Publikovanie najnovších informácií a varovaní o potenciálnych hrozbách na webovej stránke v rubrike Aktuálne z bezpečnosti [47]
	Ponúknuť koordinačnú a poradenskú pomoc pri riešení a podporu orgánom postihnutým bezpečnostným incidentom [4]	Vytvorenie pracovnej skupiny pri DoS útokoch v marci 2013a komunikácia s potenciálne ohrozenými organizáciami [46]
	Zabezpečovať osvetovú a vzdelávaciu činnosť dvíhajúcu povedomie o kybernetickej bezpečnosti [42]	Vytvorenie projektov Ako na Internet a Lovci záhad, spolupráca s organizáciou Safer Internet a osvetová činnosť formou prednášok a seminárov [40]
	Výmena informácií s NBÚ a vládnym CERT tímom [4]	Výročné správy podávané NBÚ, neformálne stretnutia so zástupcami NBÚ a vzájomná komunikácia s vládnym CERT tímom aj formou súkromnej siete [40]
	Poskytnúť pomoc pri zriaďovaní CERT tímu v sieti na území ČR a jeho akreditovaní [42]	Poskytovanie pomoci pri zriaďovaní CERT tímu po skontaktovaní na e-mailovej adrese infor@csirt.cz [43]
Ostatné služby ponúkané národným CERT tímom	Analýza bezpečnostných incidentov [18]	Pracovisko CSIRT.CZ z kapacitných dôvodov neposkytuje službu analýzy bezpečnostného incidentu na forenznej úrovni, ale spolupracuje s forenzným laboratóriom Avast, ktorému na rozbor posiela vzorky [40]
	Audity a hodnotenia bezpečnosti [18]	Ponuka bezplatnej služby na objednávku Skener webov a testovanie webových stránok na výdrž DoS útokov záťažovými testami [43]
	Snaha o zachovanie bezpečnosti na sieťach [18]	Spravovanie a kontrola honeypotov, vyhodnotenie zachytených malwarov a ich odoslanie na rozbor, prípadné vydanie varovania [43]
	Výskum a tvorba nových nástrojov v oblasti kybernetickej bezpečnosti [18]	Momentálne aktivity a plánovanie vlastného výskumného projektu na prepojenie informačných zdrojov s údajmi o správcoch sietí [40]
	Detekcia prieniku a narušenia informačných systémov [18]	Prevádzkovanie služby na odhaľovanie prienikov do siete Intrusion Detection System, v spolupráci s CESNET [43]
	Odstránenie problému a oprava systému po narušení [18]	CSIRT.CZ sa fyzicky nepodieľa na riešení problému, zaisťuje koordinačnú činnosť a pomoc pri kontaktovaní orgánov a subjektov [42]
Formy spolupráce	Účasť na medzinárodných konferenciách [42]	Pravidelná účasť na medzinárodnom fóre FIRST, konferenciách usporiadaných organizáciou ENISA a TERENA [40]

Kategória	Návrh	Národný CERT tím CSIRT.CZ
	Tvorba spoločných projektov a spolupráca s ostatnými CERT tímami na národnej úrovni [42]	Spoluúčasť na projekte Danube, FENIX, spolupráca so Safer Internet, forenzným laboratóriom Avast [40]
	Vzájomná komunikácia a zdieľanie informácií medzi tímami na národnej úrovni [4]	Usporadúvanie stretnutí pracovnej skupiny, šifrovaná e-mailová komunikácia, telefonáty a komunikácia na vlastnej súkromnej chatovacej platforme [40]
Technické a organizačné predpoklady	Organizačná štruktúra vo forme generálny riaditeľ, 6 – 8 členov prevádzkovo-technického časti tímu a pracovná časť tímu (vrátane PR) [18]	Martin Peterka ako vedúci bezpečnostného tímu, 6 bezpečnostných špecialistov a Andrea Kropáčová ako reprezentantka CSIRT.CZ na domácej a medzinárodnej scéne [54]
	Komunikačné kanály – internetové stránky, on-line formulár na hlásenie bezpečnostných incidentov, e-mailová adresa, telefónne a faxové číslo, adresa [18]	Webová stránka www.csirt.cz, na ktorej sú zverejnené oba druhy on-line formulárov, telefónne číslo, adresa pracoviska, e-mailová adresa abuse@csirt.cz, kontakt na prevádzkovateľa a otváracie hodiny pracoviska [52]
	Operačný systém – Linux, Windows NT 4.0, XP, 2003 a vyššie, MacOS X [23]	Operačný systém Linux [44]
	Virtualizačný software VMware, VirtualPC, VirtualServer [23]	Dostupný virtuálny software VMware [44]
	Ticketovací systém AIRT, RTIR alebo OTRS [23]	Ticketovací systém OTRS s vlastnými úpravami na triedenie nahlásených bezpečnostných incidentov a tvorbu štatistík [40]
	Využitie CRM softwaru riadenia starostlivosti o zákazníkov, SugarCRM alebo Sugarforce [18]	CSIRT.CZ nepoužíva CRM software, pretože nevystupuje ako komerčný CERT tím poskytujúci platené služby, ergo nemá zákazníkov v pravom slova zmysle [44]
	Využitie databázy organizácie RIPE, TI a IRT [18]	Čerpanie informácií o sieťach a ich správcoch z databázy RIPE [44]
	Šifrovanie elektronickej pošty a využitie digitálneho podpisu PGP, GnuPG alebo S/MIME [18]	E-mailová adresa abuse@csirt.cz aj každý z členov tímu má vlastný PGP kľúč [53]
Skúšobná doba pracoviska	18 – 24 mesiacov [22]	Od založenia v apríli 2008 po menovanie národným tímom v decembri 2010 CSIRT.CZ fungoval ako modelové pracovisko [20]

6 Záver práce

Na začiatku písania tejto bakalárskej práce bol stanovený jej hlavný cieľ v podobe popisu súčasnej úlohy národného tímu CERT v oblasti ochrany kritickej informačnej štruktúry na základe uvedenia Zákona o kybernetickej bezpečnosti do účinnosti a porovnanie teoretických prístupov s ich uplatnením v praxi. Pred samotným porovnaním však bolo nutné položiť základy teoretické, a to v oblasti kybernetickej bezpečnosti a bezpečnostných incidentov so zameraním na CERT / CSIRT tímy v historickej, technickej a funkčnej oblasti a medzinárodné aj národné možnosti spolupráce. Následne sa práca mohla venovať legislatívnemu rámcu kybernetickej bezpečnosti a kriminality v Českej republike, vrátane procesu schvaľovania, obsahovej analýze a vyhodnoteniu nového Zákona č. 181/2014 Sb., o kybernetickej bezpečnosti.

Dopady schválenia a vstupu zákona do účinnosti je možné rozdeliť na dve časti. Prvou je vytvorenie opory pre národný a vládny tím CERT, zakotvenej v legislatíve krajiny, druhou uloženie zákonnej povinnosti hlásenia bezpečnostných incidentov orgánom a osobám konkrétne vymedzeným zákonom. Pokým Zákon o kybernetickej bezpečnosti nebol Parlamentom Českej republiky schválený, zastávalo úlohu oboch, to znamená vládneho aj národného CERT tímu, modelové pracovisko CSIRT.CZ, neskôr oficiálne menované Národným CSIRT tímom Českej republiky. Vznik vládneho CERT tímu GovCERT.CZ, pod hlavičkou Národného centra pre kybernetickú bezpečnosť, bol jedným z výrazných dopadov zákona. Hoci pracoviská stále fungujú v tesnej spolupráci a v niektorých prípadoch zdieľajú informácie o bezpečnostných incidentoch, ich povinnosti boli zákonom rozdelené. Od 1. januára 2015 pod GovCERT.CZ patria hlásenia správcov informačného alebo komunikačného systému kritickej informačnej infraštruktúry a správcov významných informačných infraštruktúr, zatiaľ čo CSIRT.CZ ako národný CERT tím krajiny sa stará o hlásenia orgánov a osôb zaisťujúcich významný informačný systém (ak nezastávajú úlohu správcu), poskytovateľom služieb elektronickej komunikácie a zaisťovateľom sietí elektronických komunikácií. Keďže jednou z povinností národného CERT tímu je taktiež starostlivosť a koordinácia riešenia bezpečnostných incidentov, ktoré predstavujú potenciálnu širokoplošnú hrozbu pre organizácie v krajine, pričom môžu byť nahlásené ktorýmkoľvek subjektom, formálnym dopadom zákona bolo rozdelenie hlásení na úrovni prijímania vo verzii dvoch rozdielnych formulárov na webovej stránke a na úrovni triedenia, ktoré zabezpečuje ticketovací systém CSIRT.CZ.

Okrem zakotvenia povinností vládneho a národného CERT tímu v legislatíve, zákon určil podmienky, ktoré musí spĺňať subjekt vykonávajúci rolu prevádzkovateľa národného CERT tímu. Navzdory tomu, že národný tím vykonával svoju oficiálnu funkciu už od roku 2010 a orgány a osoby mali možnosť bezpečnostné incidenty hlásiť, možnosť sa prijatím zákona zmenila na právnu povinnosť v rozsahu určenom rozdelením podľa významnosti infraštruktúry. Taktiež pribudli prostriedky kontroly a sankcie udeľované Národným bezpečnostným úradom pri nesplnení týchto povinností. Pokiaľ ide o konkrétne dopady v kontexte organizácií a ich zabezpečenia, okrem oficiálnej povinnosti hlásenia incidentov by dopady nemali byť veľké. Organizácie kritickej či významnej infraštruktúry by totiž mali spĺňať bezpečnostné štandardy ISO/IEC 27000, z ktorých vychádza samotný zákon. Veľké zmeny a s nimi súvisiace investície a problémy môžu nastať hlavne v prípade, kedy organizácia kybernetickú bezpečnosť a bezpečnosť informácií zanedbávala.

Stručným zhrnutím dopadov schválenia Zákona o kybernetickej bezpečnosti je vytvorenie všeobecného právneho rámca v oblasti kybernetickej bezpečnosti konkretizovaného trojicou sprievodných dokumentov obsahujúcich špecifické a technické detaily, definovanie rolí a povinností vládneho a národného tímu CERT a rozdelenie subjektov podľa významnosti siete vrátane spresnenia procesu hlásenia bezpečnostných incidentov.

Ako je zrejmé z predchádzajúcich riadkov, národný CERT tím bol jedným zo subjektov v Českej republike, ktorých sa schválenie zákona dotýkalo výraznou mierou. Preto som sa rozhodla ďalej v práci zamerať na ich povinností a fungovania podľa zákona a odporúčaní európskej agentúry ENISA a následné porovnanie s informáciami z praxe, získanými počas osobného rozhovoru, e-mailovej komunikácie alebo webových stránok CSIRT.CZ, ktoré sú spracované formou samostatných podkapitol zameraných na konkrétne povinnosti, činnosti a vlastnosti. Záverečné porovnanie je vytvorené vo forme tabuľky (viz Tabuľka 1: Porovnanie požiadaviek zákona a odporúčaní ENISA s pracoviskom CSIRT.CZ), ktorá najprehľadnejším spôsobom poskytuje možnosť porovnať získané informácie zo všetkých zdrojov.

Zákon o kybernetickej bezpečnosti a odporúčania agentúry ENISA, ktoré sú prezentované v príručke CSIRT Setting up Guide, sú natoľko kompatibilné a voči sebe obsahujú len minimálne rozdiely, že je možné ich zhrnúť v jeden celok, ako je tomu v priloženej tabuľke. Jediné dve odlišnosti vyplývajú zo samotnej podstaty národného CERT tímu, ktorý nepôsobí ako komerčný CERT tím, a preto jeho zložky nie je možné vnímať ako platiacich zákazníkov, ergo nevyvstáva potreba využívať CRM software riadenia starostlivosti o zákazníkov. Rovnako zákon neukladá národnému tímu povinnosť analyzovať bezpečnostné incidenty na forenznej úrovni, preto CSIRT.CZ spolupracuje s externými forenznými laboratóriami. Inak pri samotnom porovnávaní vyplynulo, že Národný CSIRT tím Českej republiky CSIRT.CZ, momentálne prevádzkovaný združením CZ.NIC, vykonáva svoju funkciu plne v súlade zo zákonom aj odporúčaniami agentúry ENISA či ide o oblasť koordinácie a riešenia bezpečnostných incidentov, vlastného výskumu a vývoja nástrojov ochrany, spolupráce medzi CERT tímami a inými subjektmi pôsobiacimi v kybernetickej bezpečnosti na medzinárodnej aj národnej úrovni alebo osvetovej a proaktívnej činnosti zameranej na dvíhanie bezpečnostného povedomia v organizáciách aj medzi bežnými obyvateľmi. Už Jean-Jacques Rousseau totiž vedel, že : „*Hlupák, ktorý porúča, môže ako ktokoľvek iný zločiny trestať, skutočný štátnik im však dokáže predísť.* [57]“

Postupným naplnením dieľčích cieľov a následne splnením primárneho cieľa vo forme porovnania teoretických a praktických informácií prináša táto bakalárska práca prínos v rovine nadobudnutia nových teoretických poznatkov v oblasti kybernetickej bezpečnosti a kybernetickej kriminality, pochopenia role, ktorú v nej hrajú CERT / CSIRT tímy, porozumenia novo účinného Zákona o kybernetickej bezpečnosti a dôsledkov, ktoré z neho vyplývajú a praktickej orientácie v tejto problematike, ktorá vysvetľuje funkciu a fungovanie národného CSIRT tímu voči organizáciám aj bežnému užívateľovi, vrátane konkrétnej ukážky koordinácie riešenia bezpečnostného incidentu a to v prípade DoS útokov z marca 2013.

Najväčším prínosom sa nakoniec stalo práve zdvihnutie povedomia o tímoch pre riešenie bezpečnostných incidentov. Sama som pred písaním tejto bakalárskej práce o CERT tímoch nevedela veľa, ľudia z môjho okolia, hoci sa venujú informatike, tiež o tímoch takmer nepočuli. Nakoniec však vďaka všetkým zozbieraným informáciám vyplynulo, že navzdory tomu, že ako bežný užívateľ prídem do styku s národným CERT tímom len skrz osvetovú činnosť, oplatí sa sledovať ich

webové stránky a činnosť, pretože práve ako človek, bežný užívateľ som najnáchylnejším cieľom útokov a zraniteľností. Varovania a výstrahy, ktoré CSIRT.CZ aj GovCERT.CZ zverejňujú na svojich webových stránkach môžu pôsobiť ako preventívne a ochranné opatrenie.

Samotná bakalárska práca, výsledky a prínosy z nej plynúce, sú v reálnom svete využiteľné okrem zdvihnutia povedomia o CSIRT.CZ tíme a predstavenia nového Zákona o kybernetickej bezpečnosti aj ako orientačná pomôcka pri hlásení bezpečnostných incidentov pre organizácie alebo zakladaní CERT tímu, prípadne ako teoretický podklad pre rozšírenie práce v budúcnosti.

6.1 Potenciálne smery prehĺbenia analýzy

Moja bakalárska práca bola zameraná na pochopenie teoretického fungovania národného CERT tímu postaveného na právnom rámci nového Zákona č. 181/2014 Sb., o kybernetickej bezpečnosti a dvojstrannej zmluve s Národným bezpečnostným úradom, po čom následne bolo možné previesť porovnanie s informáciami z praxe. Na začiatku ale bolo potrebné zmapovať legislatívnu oblasť kybernetickej kriminality a kybernetickej bezpečnosti s hlavným dôrazom na nový komplexný Zákon o kybernetickej bezpečnosti, ktorého schválenie by mohlo inšpirovať aj ostatné krajiny Európskej únie, rovnako ako prezentovať základné informácie o tímoch pre riešenie bezpečnostných incidentoch, o ktorých, ako som počas písania bakalárskej práce zistila, široká verejnosť nemá vysoké povedomie.

Samotná bakalárska práca by mohla byť rozšírená či využitá ako podklad pre tri tematické smery:

- Analýza pracoviska vládneho CERT tímu GovCERT.CZ, jeho funkcie a povinností, praktického fungovania a kompetencií. Následnou hlavnou témou a zameraním práce by mohla byť otázkou či je potrebné oddeľovať pracoviská národného a vládneho tímu, či takéto rozdelenie prináša väčší úžitok a nie je systémovo, finančne a funkčne jednoduchšie ich spojiť ich v jeden tím, ako tomu bolo pred nástupom Zákona o kybernetickej bezpečnosti do praxe.
- Zameranie sa na následnú forenznú analýzu bezpečnostných incidentov prebiehajúcu vo forenzných laboratóriách, napríklad spomenutej spoločnosti Avast, najčastejšie používaných postupov a softwarových nástrojov, vyhodnocovania výsledkov a proces ich implementácie do konečných ochranných prostriedkov.
- Hlbšia analýza legislatívneho rámca krajín Európskej únie, rozbor Európskou radou pripravovanej Direktívy v oblasti kybernetickej bezpečnosti a jej následkov pre členské štáty a analýza opatrení, ktoré by museli byť prijaté či prípadných kolízií s ich doterajšími legislatívami.

Terminologický slovník

Termín	Skratka	Význam [zdroj]
Advanced Research Projects Agency Network	ARPANET	Prvá počítačová sieť zdieľajúca informácie navrhnutá a zostrojená v roku 1969 pod záštitou Advanced Research Projects Agency, Ministerstva obrany Spojených štátov amerických. [8]
Application for Incident Response Teams	AIRT	Online aplikácia zaznamenávajúca informácie o priebehu a stave riešenia bezpečnostného incidentu. [23]
Bezpečné viacúčelové rozšírenie pošty Internetu (angl. Secure Multimedia Internet Mail Extentions)	S/MIME	Software používaný na šifrovanie a podpisovanie elektronickej pošty za účelom ochrany a zabezpečenia. [18]
Bezpečnostná udalosť (angl. information security event)		Nečakaná situácia alebo stav informačného systému, ktorý predstavuje možnosť narušenia, ovplyvnenia alebo zlyhania kybernetickej bezpečnosti, jej zadefinovaných postupov a pravidiel. [17]
Bezpečnostný incident (angl. security incident)		Bezprostredné „*narušenie bezpečnosti IS/ICT a pravidiel definovaných k jeho ochrane ..., ktoré je obvykle spojené s výpadkom služby alebo zhoršením jej kvality* ([17], s.12)“
Citlivé informácie (angl. sensitive data)		Chránené informácie o zamestnancoch a klientoch, firemné know-how a pracovné postupy, používaný sofware a iné dáta, ktoré majú dôverný charakter a sú určené len na interné použitie v rámci organizácie, pretože ich únik alebo strata môže spôsobiť citeľnú škodu. [vlastná definícia autorky]
Česká pobočka AFCEA (angl. The Armed Forces Communication & Electronics Association)	ČP AFCEA	Vzdelávacia organizácia podporujúca rozvoj informačných a komunikačných technológií ozbrojených síl. [58]
Distribuované odmietnutie služby (angl. Distributed Denial of Service)	DoS (DDoS)	Technika útoku, ktorá spôsobuje nedostupnosť internetovej služby jej zahltením mnohými požiadavkami útočníka. [5]
Európska agentúra pre bezpečnosť sietí a informácií (angl. European Network and Information Security Agency)	ENISA	Organizácia zastrešujúca tímy CERT z krajín Európskej únie za účelom zdieľania informácií, znalostí a praktík v oblasti informačnej bezpečnosti. [59]
Fórum tímov pre reakciu na bezpečnostné incidenty a pre bezpečnosť (angl. Forum of Incident Response and Security Teams)	FIRST	Celosvetová organizácia združujúca tímy pre riešenie bezpečnostných incidentov, podporujúca ich vzájomnú spoluprácu. [18]

Termín	Skratka	Význam [zdroj]
Hacker		Pomenovanie pre osobu zaoberajúcu sa štúdium kódu a preniknutia do programovateľných systémov za účelom intelektuálnej zvedavosti alebo jeho následného zneužitia. [5]
Hacking		Použitie v zmysle crack, „*neoprávnené narušenie zabezpečenia ochrany programu alebo systému*“. ([5], s.28)
Honeypot		Informačný systém nastražený ako návnada za účelom prilákania a zachytenia škodlivého softwaru, malware, ktorý je následne analyzovaný. [5]
Informačné centrum nástrojov pre riešenie bezpečnostných incidentov (angl. Clearing House for Incident Handling Tools)	CHIHT	Pilotný webový projekt poskytujúci tímom riešiacim bezpečnostné incidenty nástroje a príručky. [23]
Informačný systém/ informačné a komunikačné technológie (angl. Information System/ Information and Communication Technology)	IS/ICT	Skrátené slovné spojenie používané pre označenie všetkých informačných systémov a technológií v organizácií. [vlastná definícia autorky]
Internet		„*Globálny systém prepojených počítačových sietí, ktoré používajú štandardný internetový protokol (TCP/IP)*.“ ([5], s.49)
Internetový červ (angl. internet worm)		Druh škodlivého programu so schopnosťou klonovania sa a preposielania.[5]
Intranet		„*Privátna (interná) počítačová sieť využívajúca klasické technológie Internetu, ktorá umožňuje zamestnancom organizácie efektívne vzájomne komunikovať a zdieľať informácie*.“ ([5], s.50)
Kybernetická bezpečnosť (angl. cyber security)		„*Súhrn právnych, organizačných, technických a vzdelávacích prostriedkov smerujúcich k zaisteniu ochrany kybernetického priestoru.“* ([5], s.57)
Kybernetická kriminalita (angl. cyber crime)	kybernalita	„*Trestná činnosť, v ktorej figuruje určitým spôsobom počítač ako súhrn technického a programového vybavenia (vrátane dát) alebo iba niektorá z jeho komponent, prípadne väčšie množstvo počítačov samostatných alebo prepojených do počítačovej siete a to buď ako predmet záujmu tejto trestnej činnosti ... alebo ako nástroj trestnej činnosti.*“ ([5], s.57)
Kybernetický priestor (angl. cyberspace)	kyberpriestor	„*Digitálne prostredie umožňujúce vznik, spracovanie a výmenu informácií, tvorenú informačnými systémami, a službami a sieťami elektronických komunikácií.*“ ([5], s.59)

Termín	Skratka	Význam [zdroj]
Kyberterorizmus (angl. cyber terrorism)		Politicky alebo extrémisticky motivovaná trestná činnosť vyvolávajúca negatívnu reakciu alebo strach využívajúca alebo mierená na informačné technológie. [5]
Národné centrum pre kybernetickú bezpečnosť	NCKB	Súčasť NBÚ vytvorená za účelom prevádzkovania vládneho CERT tímu a činností s tým súvisiacimi. [30]
Národný bezpečnostný úrad	NBÚ	Gestor ČR pre kybernetickú bezpečnosť a najvyšší vládny orgán zabezpečujúci ochranu informácií a bezpečnostné overenia. [28]
Národný tím CERT Českej republiky	CSIRT.CZ	Tím CERT preberajúci na základe Memoranda o CERT/CSIRT tímoch v ČR úlohu národného tímu CERT. [21]
Ochrana kritických informácií (angl. Critical Information Protection)	CIP	Ochrana informácií, ktorých strata alebo únik by mohli vážne ohroziť alebo poškodiť normálne fungovanie štátu a jeho bezpečnosť. [5]
Ochrana kritických informácií a infraštruktúry (angl. Critical Information and Infrastructure Protection)	CIIP	Ochrana systémov a služieb, ktorých nedostatočná alebo žiadna funkčnosť by spôsobila problémy výrazne ovplyvňujúce normálny chod štátu a jeho bezpečnosť. [5]
Ochrana súkromnia GNU (angl. GNU Privacy Guard)	GnuPG	Bezplatný software umožňujúci šifrovanie a ochranu elektronickej pošty. [18]
Open-source Ticket Request System	OTRS	Open-source softwarový nástroj používaný na správu hlásení bezpečnostných incidentov. [40]
Phishing		Zločinecká metóda získavania prístupových hesiel, mien a platobných údajov s cieľom ich zneužitia. [5]
Plan – Do – Check – Act Model	PDCA	Manažérsky koncept zachycujúci životný cyklus procesu v organizácií zameraný na jeho vylepšovanie. [16]
Rada pre kybernetickú bezpečnosť	RKB	Poradný vládny orgán vytvorený za účelom pomoci NBÚ pri jej dohľadovej a koordinačnej činnosti ako aj tvorbe správ o aktuálnom stave v oblasti kybernetickej bezpečnosti. [29].
Rovný s rovným (angl. Peer-to-peer)	P2P	Model počítačovej siete, pri ktorom komunikujú klienti navzájom, najčastejšie v podobe výmenných sietí, kde s dvíhajúcim sa množstvom klientov stúpa prenosová kapacita. [5]
Sledovač žiadostí o reakci na bezpečnostné incidenty (angl. Request Tracker for Incident Response)	RTIR	Bezplatný systém riadenia a uchovávania informácií o bezpečnostných incidentoch fungujúci na báze open-source. [23]
Sociálne inžinierstvo (angl. social engineering)		Techniky manipulácie a zneužívania ľudských zdrojov za účelom páchania nelegálnej činnosti. [3]

Termín	Skratka	Význam [zdroj]
Systém detekovania prieniku (angl. Intrusion Detection System)	IDS	Systém využívaný k overeniu pokusu o prienik do siete, prípadne reakcie na uskutočnený prienik. [5]
Systém zvládania bezpečnostných incidentov (angl. Security Incident Management System)	SIMS	Aplikácia založená na modeli PDCA modifikovaného na použitie pri riešení bezpečnostných incidentov a ich vylepšovaní. [16]
Škodlivý software (angl. malicious software)	malware	Všeobecné pomenovanie škodlivých programov ako sú vírusy, červy a pod. [5]
Tím riešenia bezpečnostných incidentov (angl. Information Security Incident Response Team)	ISIRT	Tím profesionálov so zameraním na kybernetickú bezpečnosť a riešenie bezpečnostných incidentov. Synonymum tímu CERT. [18]
Tím pre reakciu na bezpečnostné incidenty počítačov (angl. Computer Security Incident Response Team)	CSIRT	Tím profesionálov so zameraním na kybernetickú bezpečnosť a riešenie bezpečnostných incidentov. Synonymum tímu CERT. [18]
Tím pre reakciu na počítačové útoky (angl. Computer Emergency Response Team)	CERT	Tím profesionálov so zameraním na kybernetickú bezpečnosť a riešenie bezpečnostných incidentov. Synonymum tímu CSIRT. [18]
Trans-európske združenie pre výskum a vytváranie vzdelávacích síl (angl. Trans-European Research and Education Networking Association)	TERENA	Organizácia podporujúca spoluprácu technických špecialistov, manažérov a iných pracovníkov v oblasti CERT tímov a informačnej bezpečnosti z európskych a okolitých krajín. [60]
Transmission Control Protocol/ Internet Protocol	TCP/IP	Sústava, sada protokolov, zabezpečujúca komunikáciu a vzájomné prepojenie počítačových systémov v sieťach, figurujúca ako primárny komunikačný protokol internetu. [61]
Vládny tím CERT Českej republiky	GovCERT.CZ	Tím CERT Zákonom o kybernetickej bezpečnosti (181/2014 Sb.) určený ako vládny CERT dohliadajúci na ochranu kritickej infraštruktúry a prvotný zdroj informácií z oblasti kybernetickej bezpečnosti. [21]
Veľmi dobré súkromie (angl. Pretty Good Privacy)	PGP	„*Software pre šifrovanie elektronických elektronickej pošty a správ*.“ ([18], s.54)
World Wide Web	WWW	Jedna zo služieb Internetu fungujúca na princípe prepojenia hypertextových stránok. [5]
Zložka		V kontexte fungovania CERT tímov označenie pre klienta, zákazníka. [18]

Zoznam použitej literatúry

[1] Internet World Stats : Usage and Population Statistics. *Internet Usage Statistics: World Internet Users Statistics 2014 Population Stats* [online]. © 2001-2015 Miniwatts Marketing Group [vid. 9. březen 2015]. Dostupné z: http://www.internetworldstats.com/stats.htm

[2] ELLIS, Juanita a Tim SPEED. *The Internet Security Guidebook: From Planning to Deployment*. B.m.: Academic Press, 2001. 348 s. ISBN 0-12-237471-1.

[3] JIROVSKÝ, Václav. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. 1. vyd. Praha: Grada, 2007. 284 s. ISBN 978-80-247-1561-2.

[4] *Zákon č. 181/2014 Sb,. o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti)* [online]. 29. srpen 2014 [vid. 21. březen 2015]. Dostupné z: http://www.zakonyprolidi.cz/cs/2014-181

[5] JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti = Cyber security glossary*. 2. vyd. Praha: Policejní akademie ČR v Praze : Česká pobočka AFCEA, 2013. 200 s. ISBN 978-80-7251-397-0.

[6] MATĚJKA, Michal. *Počítačová kriminalita*. 1. vyd. Praha: Computer Press, 2002. 106 s. ISBN 80-7226-419-2.

[7] PLOUG, Thomas. *Ethics in Cyberspace: How Cyberspace May Influence Interpersonal Interaction*. B.m.: Springer Science & Business Media, 2009. 223 s. ISBN 978-90-481-2370-4.

[8] GILSTER, Paul. *The Internet navigator: The essential guide to network exploration for the individual dial-up user*. New York: Wiley & Sons, 1993. 470 s. ISBN 0-471-59782-1.

[9] CHON, Margaret. Learning Cyberlaw in Cyberspace: Introduction to Cyberspace. *Learning Cyberlaw in Cyberspace* [online]. [vid. 23. březen 2015]. Dostupné z: http://www.cyberspacelaw.org/chon/

[10] GHERNAOUTI-HELIE, Solange. *Cyber Power: Crime, Conflict and Security in Cyberspace*. Lausanne: EPFL Press, 2013. 468 s. ISBN 978-1-4665-7304-8.

[11] Slovenské slovníky. *Jazykovedný ústav Ľudovíta Štúra Slovenskej akadémie vied* [online]. © Jazykovedný ústav Ľ. Štúra SAV [vid. 22. březen 2015]. Dostupné z: http://slovniky.juls.savba.sk/?w=u%C5%BE%C3%ADvate%C4%BE&s=exact&c=h91d&d=kssj4&d=psp&d=scs&d=sss&d=peciar&d=ma&ie=utf-8&oe=utf-8#

[12] Urban Dictionary: Catfishing. *Urban Dictionary* [online]. [vid. 22. březen 2015]. Dostupné z: http://www.urbandictionary.com/define.php?term=Catfishing

[13] Internet addiction: Stanford study seeks to define whether it's a problem. *Stanford Medicine: News Center* [online]. 17. říjen 2006, ©2015 Stanford Medicine [vid. 22. březen 2015]. Dostupné z: http://med.stanford.edu/news/all-news/2006/10/internet-addiction-stanford-study-seeks-to-define-whether-its-a-problem.html

[14] BOSWORTH, Seymour, Michel E. KABAY a Eric WHYNE, ed. *Computer security handbook*. 6. vyd. Hoboken, New Jersey: John Wiley & Sons, Inc, 2014. 2207 s. ISBN 978-1-118-13410-8.

[15] JULIAN, Ted. Defining Moments in the History of Cyber-Security. *Infosecurity Magazine* [online]. © 2015 Reed Exhibitions Ltd. [vid. 10. březen 2015]. Dostupné z: http://www.infosecurity-magazine.com/opinions/the-history-of-cybersecurity/

[16] DOUCEK, Petr, Luděk NOVÁK, Lea NEDOMOVÁ a Vlasta SVATÁ. *Řízení bezpečnosti informací: 2. rozšířené vydání o BCM*. 2. přeprac. vyd. Praha: Professional Publishing, 2011. 286 s. ISBN 978-80-7431-050-8.

[17] KROPÁČOVÁ, Andrea. *CERT/CSIRT: týmová práce pro zajištění bezpečnosti komunikačních sítí*. In: Connect, Computer Press, 2010, roč. 15, č. 6, s. 12–13. ISSN 1234-5678.

[18] ENISA. *CSIRT Setting up Guide* [online]. 22. prosinec 2010, © 2005-2015 ENISA. 87 s. [vid. 1. duben 2015]. Dostupné z: https://www.enisa.europa.eu/activities/cert/support/guide/files/csirt-setting-up-guide-in-czech

[19] ENISA. *CERT Inventory : Inventory of CERT teams and activities in Europe* [online]. verze 2.14. 2015, © 2005-2015 ENISA. 47 s. ISBN 978-92-79-00077-5. Dostupné z: http://www.enisa.europa.eu/activities/cert/background/inv/files/inventory-of-cert-activities-in-europe

[20] CSIRT - Historie. *CSIRT.CZ* [online]. [vid. 7. duben 2015]. Dostupné z: https://www.csirt.cz/page/889/historie/

[21] Vládní CERT / Národní centrum kybernetické bezpečnosti ČR. *Národní centrum kybernetické bezpečnosti ČR* [online]. [vid. 1. duben 2015]. Dostupné z: http://www.govcert.cz/cs/vladni-cert/

[22] ROBERTS, Paul. CSIRT groups take on new roles. *Network World*. 2005, roč. 22, č. 4, s. 45. ISSN 0887-7661.

[23] PENEDO, David. Technical Infrastructure of a CSIRT. In: *International Conference on Internet Surveillance and Protection, 2006. ICISP '06*: *International Conference on Internet Surveillance and Protection, 2006. ICISP '06* [online]. B.m.: IEEE, 2006, s. 27–27. ISBN 0-7695-2649-7. Dostupné z: doi:10.1109/ICISP.2006.32

[24] ENISA. *Detect, SHARE, Protect - Solutions for Improving Threat Data Exchange among CERTs* [online]. 20. listopad 2013, © 2005-2015 ENISA. 43 s. [vid. 4. duben 2015]. Dostupné z: https://www.enisa.europa.eu/activities/cert/support/information-sharing/detect-share-protect-solutions-for-improving-threat-data-exchange-among-certs

[25] EU Cybersecurity plan to protect open internet and online freedom and opportunity - Cyber Security strategy and Proposal for a Directive. *Digital Agenda for Europe* [online]. 7. únor 2013 [vid. 4. duben 2015]. Dostupné z: ec.europa.eu//digital-agenda/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security

[26] KRATOCHVÍL, David. *Kybernetická bezpečnost a legislativa ČR*. Praha, 2013. Diplomová práce. Fakulta informatiky a statistiky, Vysoká škola ekonomická v Praze, Katedra systémové analýzy. Vedoucí práce Petr Doucek. [online]. 30. červen 2013. Dostupné z: http://www.vse.cz/vskp/eid/38486

[27] Legislativa / Legislativa / Národní centrum kybernetické bezpečnosti ČR. *Národní centrum kybernetické bezpečnosti ČR* [online]. [vid. 5. duben 2015]. Dostupné z: http://www.govcert.cz/cs/legislativa/legislativa/

[28] Národní bezpečnostní úřad. *Národní bezpečnostní úřad* [online]. © Národní bezpečnostní úřad [vid. 19. duben 2015]. Dostupné z: http://www.nbu.cz/cs/

[29] Rada pro kybernetickou bezpečnost / RKB / Národní centrum kybernetické bezpečnosti ČR. *Národní centrum kybernetické bezpečnosti ČR* [online]. [vid. 5. duben 2015]. Dostupné z: http://www.govcert.cz/cs/rkb/rada-pro-kybernetickou-bezpecnost/

[30] Úvod / Národní centrum kybernetické bezpečnosti ČR. *Národní centrum kybernetické bezpečnosti ČR* [online]. [vid. 5. duben 2015]. Dostupné z: http://www.govcert.cz/cs/

[31] Zranitelnosti / Informační servis / Národní centrum kybernetické bezpečnosti ČR. *Národní centrum kybernetické bezpečnosti ČR* [online]. [vid. 5. duben 2015]. Dostupné z: http://www.govcert.cz/cs/informacni-servis/zranitelnosti/

[32] MongoDB - oprava chyby umožňující vzdálené odmítnutí služby / Zranitelnosti / Informační servis / Národní centrum kybernetické bezpečnosti ČR. *Národní centrum kybernetické bezpečnosti ČR* [online]. [vid. 5. duben 2015]. Dostupné z: http://www.govcert.cz/cs/informacni-servis/zranitelnosti/mongodb---oprava-chyby-umoznujici-vzdalene-odmitnuti-sluzby/

[33] Národní odkazy / Odkazy / Národní centrum kybernetické bezpečnosti ČR. *Národní centrum kybernetické bezpečnosti ČR* [online]. [vid. 19. duben 2015]. Dostupné z: http://www.govcert.cz/cs/odkazy/narodni-odkazy/

[34] Předpis 181/2014 Sb. *Poslanecká sněmovna Parlamentu České republiky* [online]. [vid. 5. duben 2015]. Dostupné z: http://www.psp.cz/sqw/sbirka.sqw?cz=181&r=2014

[35] *Nařízení vlády č. 315/2014, kterým se mění nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury* [online]. 8. prosinec 2014 [vid. 5. duben 2015]. Dostupné z: http://www.nbu.cz/cs/pravni-predpisy/provadeci-pravni-predpisy/provadeci-pravni-predpisy-k-zakonu-c-1812014-sb-o-kyberneticke-bezpecnosti-a-o-zmene-souvisejicich-zakonu/

[36] Nový kybernetický zákon: Jak se připravit? In: *BusinessInfo.cz* [online]. 18. prosinec 2014, © 1997-2015 CzechTrade [vid. 6. duben 2015]. Dostupné z: http://www.businessinfo.cz/cs/clanky/novy-kyberneticky-zakon-jak-se-pripravit-59504.html

[37] KII / VIS / KII / VIS / Národní centrum kybernetické bezpečnosti ČR. *Národní centrum kybernetické bezpečnosti ČR* [online]. [vid. 5. duben 2015]. Dostupné z: http://www.govcert.cz/cs/kii--vis/kii--vis/

[38] *Vyhláška č. 317/2014, o významných informačních systémech a jejich určujících kritériích* [online]. 15. prosinec 2014 [vid. 5. duben 2015]. Dostupné z: http://www.nbu.cz/cs/pravni-predpisy/provadeci-pravni-predpisy/provadeci-pravni-predpisy-k-zakonu-c-1812014-sb-o-kyberneticke-bezpecnosti-a-o-zmene-souvisejicich-zakonu/

[39] *Vyhláška č. 316/2014, o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti* [online]. 15. prosinec 2014 [vid. 5. duben 2015]. Dostupné z: http://www.nbu.cz/cs/pravni-predpisy/provadeci-pravni-predpisy/provadeci-pravni-predpisy-k-zakonu-c-1812014-sb-o-kyberneticke-bezpecnosti-a-o-zmene-souvisejicich-zakonu/

[40] BAŠTA, Pavel a Zuzana DURAČINSKÁ. Osobný rozhovor so zamestnancami CSIRT.CZ. 25. březen 2015

[41] CZ.NIC - O sdružení. *CZ.NIC Správce domény CZ* [online]. © 2015 CZ.NIC, z. s. p. o. [vid. 10. duben 2015]. Dostupné z: http://www.nic.cz/page/351/o-sdruzeni/

[42] *Memorandum o Computer Emergency Response Team / Computer Security Incident Response Team České republiky* [online]. 28. únor 2012. Dostupné z: https://www.govcert.cz/cs/legislativa/smlouvy-a-memoranda/

[43] CSIRT - Služby. *CSIRT.CZ* [online]. [vid. 10. duben 2015]. Dostupné z: https://www.csirt.cz/page/2764/sluzby/

[44] DURAČINSKÁ, Zuzana. *Doplňujúce otázky k bakalárskej práci* [online]. 7. duben 2015. Dostupné z: http://mail.azet.sk//inbox/dorucene?utm_source=azet.sk&utm_medium=box-po-prihlaseni&utm_content=email&utm_campaign=HP-new2&i9=d2b5637e0e94#/inbox/dorucene/msg/1428478892679361?i9=d2b5637e0e94&_=1428586844883

[45] CSIRT - Statistiky řešených incidentů. *CSIRT.CZ* [online]. [vid. 7. duben 2015]. Dostupné z: https://www.csirt.cz/page/2635/statistiky-resenych-incidentu/

[46] *Rekapitulace (D)DoS útoků ze dnů 4. 3. - 7. 3.* [online]. B.m.: CSIRT.CZ. Dostupné z: https://www.csirt.cz/files/csirt/Rekapitulace-utoky-20120311.pdf

[47] CSIRT - Aktuálně z bezpečnosti. *CSIRT.CZ* [online]. [vid. 11. duben 2015]. Dostupné z: https://www.csirt.cz/news/security/

[48] Akademie - Detail kurzu. *Akademie CZ.NIC* [online]. © 2015 CZ.NIC, z. s. p. o. [vid. 11. duben 2015]. Dostupné z: https://akademie.nic.cz/akademie/course/79/detail/

[49] CZ.NIC. Jak na Internet. *Jak na Internet* [online]. © 2012 - 2014 CZ.NIC, z. s. p. o. [vid. 11. duben 2015]. Dostupné z: http://www.jaknainternet.cz/

[50] CSIRT - Novinky. *CSIRT.CZ* [online]. 1. duben 2015 [vid. 12. duben 2015]. Dostupné z: https://www.csirt.cz/news/

[51] O Fenixu. *Fenix* [online]. [vid. 13. duben 2015]. Dostupné z: http://fe.nix.cz/#about

[52] CSIRT - Kontakt. *CSIRT.CZ* [online]. [vid. 8. duben 2015]. Dostupné z: https://www.csirt.cz/page/887/kontakt/

[53] *CSIRT description for CSIRT.CZ, National CSIRT of The Czech Republic* [online]. 23. březen 2015. Dostupné z: https://www.nic.cz/files/csirt/rfc2350_CSIRT.CZ.20150323.pdf

[54] CSIRT - Členové týmu. *CSIRT.CZ* [online]. [vid. 8. duben 2015]. Dostupné z: https://www.csirt.cz/page/2633/clenove-tymu/

[55] CSIRT - Formulář hlášení kybernetického bezpečnostního incidentu podle Zákona o kybernetické bezpečnosti. *CSIRT.CZ* [online]. [vid. 12. duben 2015]. Dostupné z: https://www.csirt.cz/stateincidentreport/

[56] CSIRT - Hlášení incidentu. *CSIRT.CZ* [online]. [vid. 12. duben 2015]. Dostupné z: https://www.csirt.cz/incidentreport/

[57] Vybraný citát autora - Jean-Jacques Rousseau [#14693]. *CITÁTY SLÁVNYCH osobností* [online]. © 2010 citaty-slavnych.cz [vid. 14. duben 2015]. Dostupné z: http://www.citaty-slavnych.cz/citat/14693

[58] Česká pobočka AFCEA | AFCEA. *Česká pobočka AFCEA* [online]. © AFCEA [vid. 4. duben 2015]. Dostupné z: http://afcea.cz/ceska-pobocka-afcea/

[59] HELMBRECHT, Udo. About ENISA — ENISA. *ENISA: European Union Agency for Network and Information Security* [online]. © 2005-2015 ENISA [vid. 4. duben 2015]. Dostupné z: http://www.enisa.europa.eu/about-enisa

[60] About TERENA (GÉANT Association as of 7 October 2014). *TERENA* [online]. 25. listopad 2014 [vid. 4. duben 2015]. Dostupné z: https://www.terena.org/about/

[61] BURIAN, Pavel. *Internet inteligentních aktivit*. Edice Průvodce. Praha: Grada, 2014. 1. vyd. 332 s. ISBN 978-80-247-5137-5.

Zoznam obrázkov a tabuliek

Zoznam obrázkov

Zoznam tabuliek

Prílohy

Zoznam príloh

Príloha 1: Formulár hlásenia bezpečnostných incidentov ENISA

FORMULÁŘ HLÁŠENÍ BEZPEČNOSTNÍHO INCIDENTU

Vyplňte tento formulář a zašlete ho faxem nebo elektronickou poštou na: ……..
*Řádky označené hvězdičkou * jsou povinné.*

Jméno a organizace

1. Jméno*:
2. Název organizace*:
3. Druh sektoru:
4. Země*:
5. Město:
6. Elektronická adresa*:
7. Telefonní číslo*:
8. Jiné:

Postižený hostitel (postižení hostitelé)

9. Počet hostitelů:
10. Jméno hostitele a internetový protokol – IP *(Internet Protocol)**:
11. Funkce hostitele*:
12. Časové pásmo:
13. Hardware:
14. Operační systém:
15. Postižený software:
16. Postižené soubory:
17. Bezpečnost:
18. Jméno hostitele a IP:
19. Protokol/port:

Bezpečnostní incident

20. Referenční číslo ref #:
21. Druh bezpečnostního incidentu:
22. Bezpečnostní incident začal:
23. Jedná se o pokračující bezpečnostní incident: ANO NE
24. Doba a způsob zjištění:
25. Známá zranitelnost:
26. Podezřelé soubory:
27. Protiopatření:
28. Podrobný popis*:

(Zdroj: [18], s.48)

Príloha 2: Stručný zoznam zákonov a noriem ovplyvňujúcich bezpečnosť informácií

Vnitrostátní

- Různé zákony o informačních technologiích, telekomunikacích, médiích
- Zákony o ochraně údajů a soukromí
- Zákony a předpisy o uchovávání údajů
- Legislativa o finančnictví, účetnictví a podnikovém řízení
- Kodexy chování pro podnikové řízení a řízení IT

Evropské

- Směrnice o elektronických podpisech (1993/93/ES)
- Směrnice o ochraně údajů (1995/46/ES) a soukromí v elektronických komunikacích (č. 2002/58/ES)
- Směrnice o sítích a službách elektronické komunikace (2002/19/ES – 2002/22/ES)
- Směrnice o právu obchodních společností (např. 8. směrnice o právu obchodních společností).

Mezinárodní

- Basilejská smlouva II (zejména pokud jde o řízení provozního rizika)
- Úmluva Rady Evropy o internetové kriminalitě
- Úmluva Rady Evropy o lidských právech (čl. 8 o soukromí)
- Mezinárodní účetní normy – IAS *(International Accounting Standards;* do určité míry nařizují kontroly IT).

Normy

- Britská norma BS 7799 (Bezpečnost informací)
- Mezinárodní normy ISO 2700x (Systémy managementu bezpečnosti informací)
- Německá IT-Grundschutzbuch (kniha o hlavní ochraně IT), francouzský EBIOS a jiné národní varianty.

(Zdroj: [18], s.29)

Príloha 3: Formulár hlásenia kybernetického bezpečnostného incidentu podľa Vyhlášky č.316/2014 Sb.

Příloha č. 5 k vyhlášce č. 316/2014 Sb

Formulář hlášení kybernetického bezpečnostního incidentu

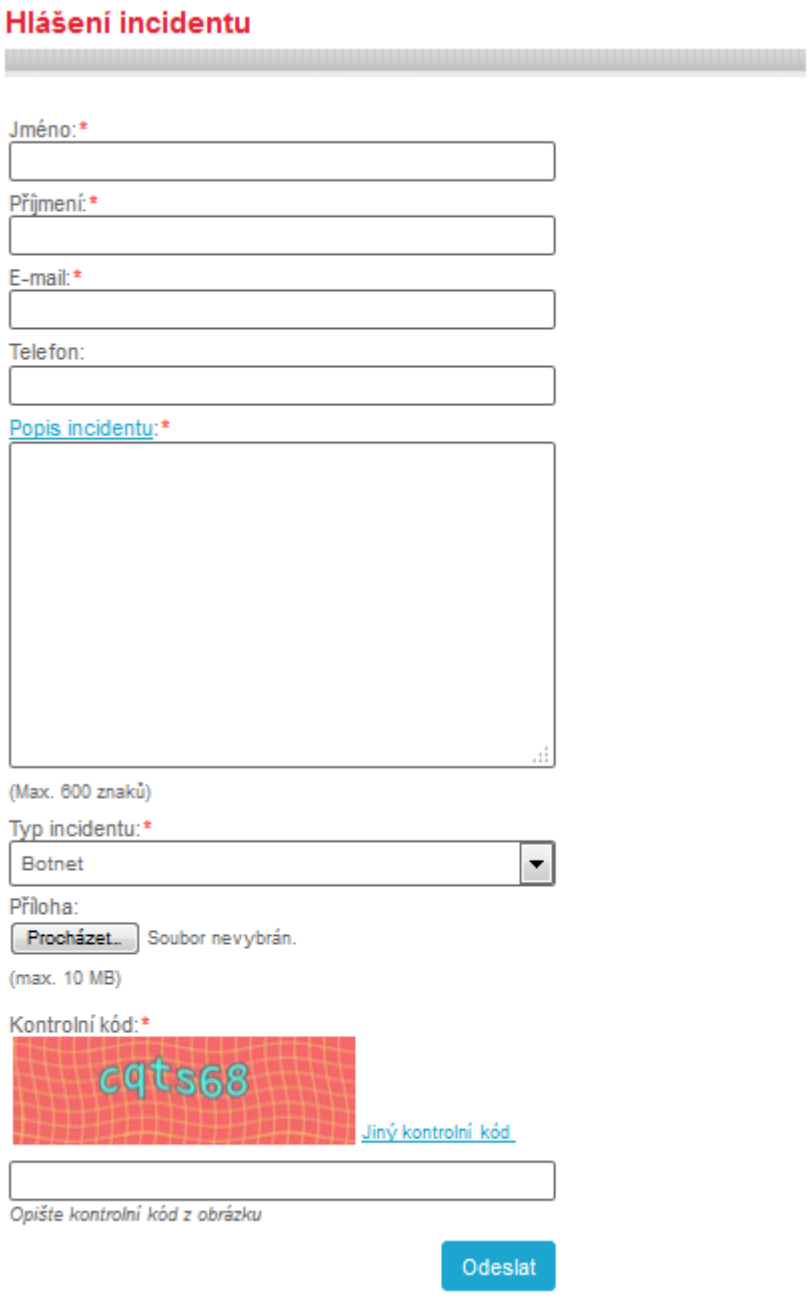
HLÁŠENÍ KYBERNETICKÉHO BEZPEČNOSTNÍHO INCIDENTU	
MÍRA OCHRANY INFORMACE	
Úroveň ochrany	
	Osobní – seznam příjemců Omezená distribuce Neomezeno
KONTAKTNÍ ÚDAJE	
Orgán a osoba uvedená v § 3 písm. c) až e) zákona	
Email	
Telefon	
DETAILY INCIDENTU	
Datum a čas zjištění	
Časová zóna	
Kategorie incidentu	Kategorie III – velmi závažný kybernetický bezpečnostní incident Kategorie II – závažný kybernetický bezpečnostní incident Kategorie I – méně závažný kybernetický bezpečnostní incident
Typ incidentu	Kybernetický bezpečnostní incident způsobený kybernetickým útokem nebo jinou událostí vedoucí k průniku do systému nebo k omezení dostupnosti služeb. Kybernetický bezpečnostní incident způsobený škodlivým kódem. Kybernetický bezpečnostní incident způsobený překonáním technických opatření. Kybernetický bezpečnostní incident způsobený porušením organizačních opatření. Kybernetický bezpečnostní incident spojený s projevem trvale působících hrozeb. Ostatní kybernetické bezpečnostní incidenty způsobené kybernetickým útokem. Kybernetický bezpečnostní incident způsobující narušení důvěrnosti primárních aktiv. Kybernetický bezpečnostní incident způsobující narušení integrity primárních aktiv.

(Zdroj: [39], s. 4003)

	Kybernetický bezpečnostní incident způsobující narušení dostupnosti primárních aktiv. Kybernetický bezpečnostní incident způsobující kombinaci dopadů uvedených shora.
Současný stav zvládání kybernetického bezpečnostního incidentu	Probíhá analýza a šetření kybernetického incidentu Kybernetický bezpečnostní incident je pod kontrolou Dotčené funkce obnoveny Neznámý
Počet zasažených systémů (odhad)	
Odhad počtu dotčených uživatelů	
Popis incidentu	
SYSTÉMOVÉ DETAILY	
Host nebo IP	
Funkce hosta (DNS server, stanice atd.)	
Pokračování	Iniciační oznámení CERTu Pokračování dříve oznámených

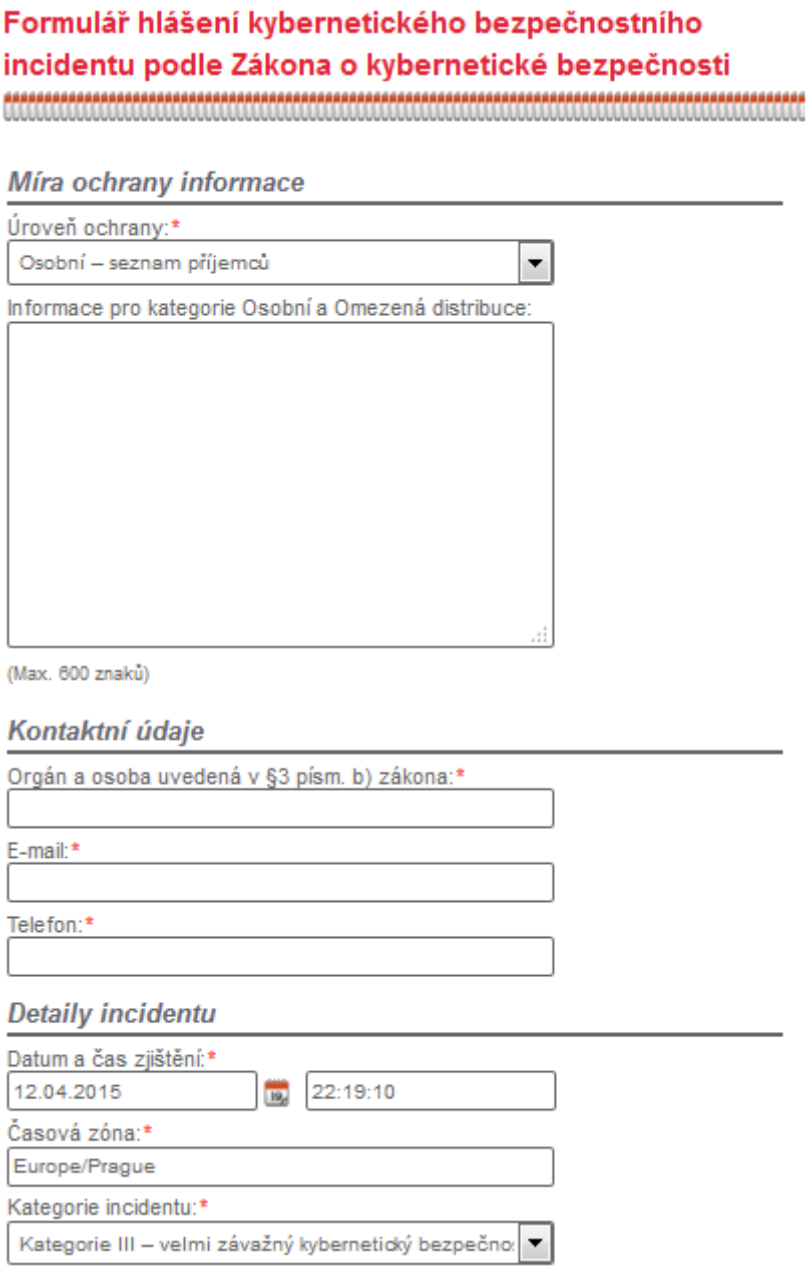
(Zdroj: [39], s. 4004)

Príloha 4: Formulár hlásenia bezpečnostných incidentov CSIRT.CZ



(Zdroj: [56])

Príloha 5: Formulár hlásenia kybernetického bezpečnostného incidentu CSIRT.CZ podľa Vyhlášky č. 316/2014 Sb.



Formulář hlášení kybernetického bezpečnostního incidentu podle Zákona o kybernetické bezpečnosti

Míra ochrany informace

Úroveň ochrany:*

Osobní – seznam příjemců

Informace pro kategorie Osobní a Omezená distribuce:

(Max. 600 znaků)

Kontaktní údaje

Orgán a osoba uvedená v §3 písm. b) zákona:*

E-mail:*

Telefon:*

Detaily incidentu

Datum a čas zjištění:*

12.04.2015 22:19:10

Časová zóna:*

Europe/Prague

Kategorie incidentu:*

Kategorie III – velmi závažný kybernetický bezpečno

(Zdroj:[55])


Typ incidentu:*
Kybernetický bezpečnostní incident způsobený kyber
Současný stav zvládání kybernetického bezpečnostního incidentu:*
Probíhá analýza a šetření kybernetického incidentu
Počet zasažených systémů (odhad):*
Odhad počtu dotčených uživatelů:*
Popis incidentu:*
(Max. 600 znaků)
Příloha:
Procházet...
Soubor nevybrán.
(max. 10 MB)
Systémové detaily
Host nebo IP:*
Funkce hosta (DNS server, stanice atd.):*
Pokračování:*
Iniciační oznámení CERTu
Kontrolní kód:*
28qyhe
Jiný kontrolní kód
Opište kontrolní kód z obrázku
Odeslat

(Zdroj:[55])

Príloha 6: Súhlas s použitím informácií – Bašta Pavel

Súhlas s použitím poskytnutých informácií

Meno a priezvisko: Dominika Rezníčková
Adresa trvalého pobytu: Fatranská 3103/20, Žilina, Slovenská republika

CZ.NIC, z.s.p.o.
Milešovská 1136/5
130 00, Praha 3
Česká republika

Svojím podpisom udeľujem súhlas Dominike Rezníčkovej so spracovaním a následným použitím informácií získaných pri osobnom rozhovore v spoločnosti CZ.NIC, z.s.p.o. za účelom vypracovania bakalárskej práce. Súhlas platí do jeho odvolania. Tento súhlas je možné kedykoľvek písomne odvolať.

V Prahe, dňa 25.3.2015

.....

Pavel Bašta
(špecialista počítačovej bezpečnosti CSIRT.CZ)

Príloha 7: Súhlas s použitím informácií – Duračinská Zuzana

Súhlas s použitím poskytnutých informácií

Meno a priezvisko: Dominika Rezníčková
Adresa trvalého pobytu: Fatranská 3103/20, Žilina, Slovenská republika

CZ.NIC, z.s.p.o.
Milešovská 1136/5
130 00, Praha 3
Česká republika

Svojím podpisom udeľujem súhlas Dominike Rezníčkovej so spracovaním a následným použitím informácií získaných pri osobnom rozhovore v spoločnosti CZ.NIC, z.s.p.o. za účelom vypracovania bakalárskej práce. Súhlas platí do jeho odvolania. Tento súhlas je možné kedykoľvek písomne odvolať.

V Prahe, dňa 25.3.2015

.....
Mgr. Zuzana Duračinská
(špecialista počítačovej bezpečnosti CSIRT.CZ)

Príloha 8: Prepis osobného rozhovoru

ÚČEL: Zisk podkladov k bakalárskej práci na tému národný CERT ČR

STOPÁŽ: 67 minút 50 sekúnd

FORMÁT: audio nahrávka mp4

DÁTUM ROZHOVORU: 25. 3. 2015

MIESTO: CZ.NIC, z.s.p.o, Milešovská 1136/5, 130 00 Praha 3

ÚČASTNÍCI:

DR = Dominika Rezníčková, moderátor;

ZD = Mgr. Zuzana Duračinská, špecialista počítačovej bezpečnosti CSIRT.CZ;

PB = Pavel Bašta, špecialista počítačovej bezpečnosti CSIRT.CZ;

DR: V prvom rade sa Vám chcem poďakovať, že ste boli ochotní a našli si čas na naše stretnutie. Na začiatok sa môžem opýtať, ako to tu u vás teda funguje. Dočítala som sa, že bezpečnostný incident vám nahlasujú pomocou formulára, ktorý máte zverejnený na internete (pozn. https://www.csirt.cz/). Našla som dva. Tak môžeme začať tým, aký je rozdiel medzi týmito dvoma formulármi?

ZD: Tak jeden sa vzťahuje k zákonu (pozn. Zákonu o kybernetickej bezpečnosti 181/2014 Sb.) priamo, pretože podľa tohto zákona nám vyplýva povinnosť, aby nám subjekty, ktoré spadajú do našej kompetencie, podľa paragrafu 3, hlásili incidenty a iba pre tieto účely je na našich stránkach zverejnený prvý formulár. S tým, že ten formulár sa zároveň odosiela na iný e-mail a spadá nám do inej fronty v ticketovacom systéme. Ten je rozdelený do niekoľkých front, práve aby sme vedeli rozlíšiť, ktoré incidenty sú hlásené podľa zákona, respektíve ktoré kontakty sú hlásené podľa zákona. Takže na kontakty a incidenty tam máme dva formuláre. A potom tam je formulár, ktorý slúži na hlásenie incidentov, ktoré sa netýkajú priamo toho zákona, ale hlásenia sú od nejakých poskytovateľov alebo bežných užívateľov a podobne.

DR: Takže vy prijímate hlásenia o bezpečnostných incidentov v podstate aj od bežných ľudí, užívateľov?

PB: Možno by stálo za reč na začiatok povedať, že ako národný CSIRT sme zodpovedný za všetky siete a užívateľov v Českej republike. To znamená, že k nám naozaj môže reportovať každý, každá IP adresa, každá doména v Českej republike. My riešime incidenty, ktoré sa ich nejakým spôsobom dotýkajú. Takto to je, ale zákon priniesol tú novinku, že časť z týchto sietí to musí robiť povinne. Doteraz bolo všetko dobrovoľné, dialo sa to na dobrovoľnej báze, ale teraz zákon vymedzil nejakú časť, ktorá je považovaná za tak dôležitú, že je potreba, aby nejakým spôsobom reportovala bezpečnostné incidenty vždy. Alebo aby s nami nejakým spôsobom spolupracovala.

DR: Jasné, tam je potom rozdiel, respektíve zákonom sú vyslovene dané organizácie, ktoré to majú hlásiť vám a ktoré majú hlásiť vládnemu CERT tímu, s ktorým máte následne spolupracovať. Čiže predpokladám, že sa niekedy stáva, že k vám hlásia incidenty, ktoré v skutočnosti patria vládnemu CERT tímu? Stávajú sa prípady, že sa k vám dostanú hlásenia, ktoré k vám reálne nepatria?

PB: Minimálne teraz, v poslednej dobe, by som povedal, že ani nie. Ako vyšiel ten zákon, urobilo sa v tom viac jasno. Niekedy sa k nám hlásenie môže dostať ako vedľajší efekt, že je to napríklad nejaký veľký útok a veľký problém, dostaneme zoznam IP adries a sami zistíme, že by niektorá z nich mala patriť k vládnemu CSIRT-u. A tak ju predáme vládnemu CSIRT-u, alebo sa s nimi dohodneme či k nim naozaj patrí, alebo nie. Keď je to napríklad v nejakom väčšom balíku dát, keď nám toho príde naozaj veľa alebo keď je to napríklad hlásenie zo zahraničia, ktoré to nerozlišuje úplne detailne, tak si to medzi sebou nejakým spôsobom rozdelíme sami.

ZD: Možno len aby ste si to vedeli predstaviť, ako kolega hovoril, v prípade väčších hlásení môže byť zoznam IP adries, ktoré pošlú priamo nám a pritom patria do vládneho sektoru a podobne.

V tom prípade to predáme ďalej. V tomto prípade sa môže stať, že dostaneme aj informácie, ktoré sa týkajú aj iných organizácií.
DR: Tak ako často, napríklad za rok, sa takéto niečo stane?
PB: To nedokážeme povedať, ale sú to jednotky.
ZD: Ešte by bolo dobré povedať, ako kolega hovoril, to, čo zákon hovorí, nezakazuje subjektom, ktoré patria pod kritickú infraštruktúru alebo podobne, spolupracovať aj s nami. To znamená, že pokiaľ oni nahlásia nejaký incident priamo vládnemu CERT-u, môžu kľudne nejaké informácie podať aj nám, ak majú pocit, že by to malo rozsiahlejší dopad a podobne, alebo môžu s nami spolupracovať na inej báze. Tým, že orgány podľa zákona spadli pod vládny CERT, iné pod národný, neznamená, že sa pred nimi pri druhom CERT-e zatvorili dvere.
DR: Stávajú sa teda prípady, že jeden incident riešite oba CERT-y?
PB: Incidenty nie, incidentov sa to netýka. Kolegyňa skôr myslela, všeobecne spoluprácu. My napríklad organizujeme pracovnú skupinu CSIRT.CZ, kam môže prísť každý. Ešte nie je konkrétne vymedzené, ale predpokladám, že ČTÚ pravdepodobne spadne pod vládny CSIRT. Napriek tomu zástupcovia ČTÚ chodia na našu pracovnú skupinu, kde sa riešia bezpečnostné otázky a podobne. Kolegyňa tým chcela teda povedať, že sa spadnutím pod konkrétny CERT podľa zákonu nezatvárajú dvere pre inú spoluprácu s druhým CERT-om. Rovnako si viem predstaviť, že pokiaľ by organizácia zaznamenala nejaký incident, ktorý by sa týkal ich a mal by širší dopad, typicky by to mohol byť spam. Dostali by nejaký nebezpečný e-mail, ako teraz chodí stále, že niekto niekomu dlží peniaze a podobne. Zaznamenali by takýto incident, týka sa ich a spadajú pod vládny CSIRT, budú ho hlásiť vládnemu CSIRT-u. Ale kľudne sa môže stať, že v rámci spolupráce ho vládny CSIRT nahlási nám, pretože to je vec, ktorá zaujíma všetkých užívateľov v Českej republike a mohla by sa šíriť ďalej. Takže tá spolupráca tam je, ale čo sa týka incidentov, tam sa nám nestáva, že pracujeme na rovnakom incidente. My máme navyše medzi sebou nejaké komunikačné kanály, rýchle, takže ak je potreba, dokážeme sa rýchlo opýtať „Robíte na tom? Viete o tomto? K nám to nepatrí. “.
DR: K tej spolupráci sa ešte dostaneme. Ale ak to chápem správne, vy sa staráte o bežných užívateľov, ale ako konečný last resort, posledné útočisko. Čiže ja, ak som dostala e-mail o tom, že som súdne trestaná a určite to nie je pravda, ako bežný užívateľ to mám nahlásiť správcovi siete, ktorý by s tým mal niečo urobiť. A ak to neurobí, tak vtedy sa mám obrátiť na vás?
PB: V tomto konkrétnom prípade my asi nemôžeme správcom povedať, že majú niečo robiť. Toto nie je úplne dobrý príklad. Neviem si predstaviť nejakého správcu siete, ktorý by na takýto e-mail nezareagoval a nenastavil na jeho serveri nejakú blokáciu. Takže tento prípad by sa k nám ani dostať nemal a skôr funguje v opačnom smere. Keď je to v rámci organizácie, ťažko do toho budeme zasahovať. Popravde sme sa s takýmto prípadom ani nestretli. Vždy je to tak, že sú dve organizácie, a jedna má zavírovaný počítač, z ktorého ide útok na iného užívateľa tu a ten si sťažuje u svojho správcu. Správca sa následne sťažuje u organizácie a v prípade, ak by s tým nič nerobili, správa ide za nami. Koncový užívatelia s nami bežne nekomunikujú. Samozrejme posielajú nám nejaké vzorky, to áno, malware, to k nám občas dorazí. Ale malo by sa to riešiť cez ich správcov.
ZD: V tomto prípade by som doplnila, že koncový užívateľ, napríklad vy, keď vám príde spam, už tú situáciu nevrátite. Nijak ten e-mail neodpošlete späť. Ide skôr o to, že technici, ktorí vidia, že ide o malware nový, ešte sa s ním nestretli a sú zároveň koncový užívatelia, tak nás o ňom informujú. „Našiel som niečo nové, neviem či ste sa s tým už stretli,“ ide skôr o informačnú službu, aby sme to my distribuovali ďalej v prípade hrozby, pretože tieto informácie musíme odniekiaľ zbierať.
DR: V prípade, že je vám niečo nahlásené, ako si to vy v tíme podelíte? Máte každý svoju vlastnú špecializáciu, zameranie?
PB: V podstate by sa dalo povedať, že áno, že každý máme nejakú svoju rolu v tom tíme. Niekto napríklad triedi hlásenia, stará sa o ne, niekto robí bežnú agendu a dokáže vyriešiť problém rovno. Ak je to väčší problém konzultuje sa s niekým na analytickej pozícií. Ale to býva minimálne. Tým ako sa človek stále učí, čím ďalej tým viac sa vyvíjajú rôzne nástroje, niekto robí rutinnú činnosť. Napríklad Zuzka má na starosti zastupovanie tímu navonok, komunikuje so zahraničnými partnermi alebo partnermi v Čechách, zároveň má na starosť prevádzku jednej služby, ktorú máme, skenovanie webov, ktoré poskytujeme ako službu zadarmo. Máme to rozdelené, ale viac-menej každý robí všetko.
DR: Spomínali ste nástroje, aké máte technické vybavenie? Konkrétne systémy, niektoré sú totiž odporúčané ENISOU, príkladom je ticketovací systém RTIR a podobne.

PB: Máme ticketovací systém, používame OTRS. Je upravený tak, aby nám niektoré veci robil automaticky. To znamená, že napríklad pri prijatom e-maily nám rovno ukáže IP adresu, ktorej sa problém týka a aký je to pravdepodobne druh problému. Pretože my to máme rozdelené podľa druhov. Na našich stránkach sú štatistiky o najčastejších druhoch problému. Tie sa berú práve z tohto delenia. My to samozrejme môžeme ručne zmeniť, ale v systéme existuje softwarový nástroj, ktorý sa učí. Takže čím viac krát ja nastavím, že nejaký druh mailu je phishing, tak s tým väčšou pravdepodobnosťou to on nabudúce vyhodnotí ako hlásenie o phishingovom útoku. Rovno sú predvyplnené kontaktné údaje na zodpovedných správcov, ktorým by sa to malo hlásiť a základné informácie o akú sieť sa jedná.
DR: A konkrétne, priame vyšetrovanie, napríklad toho malwaru alebo iného bezpečnostného incidentu, si vykonávate sami alebo spolupracujete s inými forenznými laboratóriami?
PB: Toto je zložitejšie, my to moc nerobíme, pretože na to nemáme kapacity. To robia antivírové spoločnosti. My máme nadviazanú spoluprácu napríklad s Avastom, ktorý napríklad, keď zaznamenáme novú vzorku malwaru, tak im ho pošleme, nech ho môžu zaradiť medzi svoje zdroje. Pokiaľ ide o niečo väčšie, oslovíme viaceré antivírové spoločnosti a pošleme im vzorky. Ale Avast bol vyslovene ten, ktorý prejavil záujem o spoluprácu, takže na základe toho im my posielame získané informácie a vzorky, keď sa niečo nové objaví.
DR: Rozumiem. Vy už ste spomenuli najčastejšie bezpečnostné incidenty, ktoré riešite. Ja som si túto štatistickú tabuľku stiahla. Na nej vidno, že najčastejšie sú phishingy, spamy a malwary. Vy ste založený od roku 2008, postrehli ste nejaké trendy?
PB: Čo bolo zaujímavé a teraz to už opadlo, v predchádzajúcich dvoch rokov, vlastne od tej doby čo boli útoky Anonymous, dosť výrazne narástli DoS útoky. Teraz to už nie je také výrazné. Na začiatku bolo vidieť ako to rástlo, ako sa stali populárnymi, je to pekne vidieť aj v tej tabuľke. Už to ale zase kleslo. Bolo vidieť ako to naraz vyskočilo, je to môj pocit, ale povedal by som, že je to práve spopularizovaním Anonymous. Z toho sa inak nedajú robiť nejaké závery, lebo ako sme last resort, tak sa k nám naozaj dostane iba špička ľadovca a nie všetko k nám hlásia. Ja si myslím, že sami správcovia si uvedomujú, čo sa k nám hlásiť má a čo nemá. A preto je v tabuľkách veľa phishingu, ktorý zmysel má. Poprvé, sme jasne schopní vidieť či to phishing je alebo nie je, podruhé je to vec, ktorá nie je sporná a na ktorú väčšina spoločností bude reagovať, v zmysle: My im napíšeme, že vás server niekto „hackol“, máte phishingovú stránku na banku v Južnej Amerike, tak na to zareagujú hneď. Potom sú ale veci, ktoré veľa správcov považuje za mimo ich rozpoznávacie schopnosti, ako napríklad skenovanie portov a podobne. Takže tomu odpovedajú hlásenia a následne štatistiky. Skenovanie portov sa deje masovo, ale hlási ho ďaleko menšia časť správcov než hlásia phishing. A zároveň to skenovanie nie je tak ohrozujúce pre systémy ako práve phishing, ktorý ohrozí veľa užívateľov.
DR: Ja som si na stránkach GovCERT.CZ našla mesačné správy o bezpečnostných incidentoch. Všimla som si, že prevažne sú napadnutými organizáciami banky a že po Novom roku, v lednu a únoru, sa hlásenia ako keby zvýšili. Neviem či je to práve dôsledok ich povinnosti to hlásiť alebo náhoda?
ZD: Inštitúcie majú zo zákona povinnosť incidenty hlásiť, ale my ani vládny CERT nemáme prístup do siete, aby sme mali možnosť overiť, čo z toho ohlásili a čo nie. Zároveň si ale vďaka zákonu uvedomili, že majú určitú zodpovednosť a počet hlásení bude stúpať.
PB: Pokiaľ sa nemýlim, otázka bola, či to, že je tam za posledné mesiace viac incidentov, je dopad zákona. To ja si nemyslím. Preto aj tak nemôžeme o tých incidentoch, ktoré nám nahlásili písať, ani NCKB (pozn. Národné centrum kybernetickej bezpečnosti). To čo je na stránkach sú obecné veci, ktoré preplávali internetom alebo o ktorých sa už vie. Napríklad správa, že minulý mesiac sme zaznamenali phishingový útok na klientov Českej sporiteľne, to sú všetko články, ktoré sú verejné.
DR: Dokumenty, ktoré mám na mysli, nie sú konkrétne články, ale mesačné správy.
PB: Áno, áno. To mám na mysli, to sú len veci verejné.
DR: Takže tie mesačné správy nie sú štatistiky, ktoré sú na niečom podložené. Na reálnych hláseniach.
PB: Nie, sú to veci verejné, také zhrnutia toho, čo sa stalo, aby tí užívatelia vedeli. Ak by ich zaujímalo čo sa v ktorom mesiaci dialo, to si myslím, že je užitočné.
DR: Takže reálne sa bežný užívateľ alebo ja nedozvie, nedostane k informáciám, ktoré incidenty boli nahlásené?
PB: To podľa mňa nie.

ZD: Nie.
PB: Jedine v nejakej všeobecnej štatistike, všeobecného typu. Konkrétne my ale nemôžeme vôbec hovoriť o tých incidentoch.
DR: Osobne som postrehla kauzu tzv. policajný vírus, ransomware, ktorý prebehol pár mesiacov dozadu. Viem, že vy ste ho konkrétne neriešili, ale postrehli ste?
PB: Neriešil to náhodou CESNET? Viem, že oni majú forenzné laboratórium a robili rozbor tohto ransomwaru. My sme sa s tým však prakticky nestretli.
DR: A zaujala vás nejaká kauza v poslednom období?
ZD: Napríklad marcové útoky 2013 na Českú republiku, DoS. Bolo zverejnených niekoľko článkov.
PB: Mňa osobne zaujalo, že sa začali objavovať e-maily dobre zamerané na užívateľov v českom prostredí. Že sú čím ďalej, tým viac zamerané. Napríklad oproti prvej vlne e-mailov s tým, že dlžíte peniaze, som bol až prekvapený a doteraz slýcham nielen pracovne ale aj súkromne, koľko ľudí ich otvorilo. Predtým to nebývalo, predtým chodili hlavne e-maily buď anglicky, alebo v mizernej češtine a boli to všeobecné veci, ktoré sa objavujú po celom svete. A teraz sú vyložene zamerané na naše prostredie, sú tam české mobilné telefóny, podpísaní českí užívatelia, mená skutočných exekútorov. Skutočne si dal niekto tú námahu, že tu niekto vyslovene operuje z Českého územia alebo tu majú minimálne niekoho, kto s nimi odtiaľto spolupracuje.
ZD: Je to také cielenejšie. To isté napríklad sa stalo s Českou poštou. Chodili obdobné e-maily. Myslím, že ESET robil analýzu toho víru. Aj my sme o ňom na blogu písali. Tam z mapky sveta, keď sa pozriete, je pôsobenie v Českej republike násobne vyššie ako v ostatných štátoch. Tento vírus bol práve v e-mailoch Českej pošty a tuším aj exekučných príkazoch.
DR: Tiež s tým mám osobné skúsenosti. Teraz sa môžem opýtať na spoluprácu. Ako fungujete s ostatnými tímami na českej a medzinárodnej úrovni? Ja som sa dočítala, že napríklad prvýkrát tento rok ste sa zúčastnili ako spoluorganizátor s NBÚ CyberCzech 2014. Akcie zameranej na testovanie znalostí zástupcov z rôznych štátnych orgánov v oblasti kybernetickej bezpečnosti. Zúčastnili ste sa niektorí z vás?
ZD: Nie, to bola práve kolegyňa.
DR: A neviete aké výsledky z tej akcie boli? K tým som sa nedopátrala.
ZD: Ja si myslím, že tie výsledky nebudú zverejnené, že išlo o cvičnú akciu. Išlo o cvičenie, počas ktorého si účastníci mali reálne vyskúšať ako by reagovali na konkrétne situácie. Ale k tej spolupráci. Ako už kolega povedal, organizujeme niekoľko rokov pracovnú skupinu CSIRT.CZ, informácie sú aj na našom webe, s tým, že je to otvorené fórum pre všetkých bezpečnostných analytikov alebo ľudí, ktorí sa zaoberajú bezpečnosťou, operátorov a pod. Poskytuje možnosť na to, aby sa stretli a diskutovali o súčasných bezpečnostných problémoch. Predtým, ako zákon vstúpil do platnosti, vo fáze kedy sa pripravoval, sa často táto skupina stretávala s cieľom, aby sa komentoval ten zákon, aby sa vylepšoval, aby nedošlo k tomu, že po nadobudnutí účinnosti sa zistí, že niektoré organizácie do neho nespadajú alebo sa v ňom nevedia identifikovať.
DR: Môžem do toho len jednu otázku? V akej miere vaše pripomienky do zákona vzali?
ZD: Pomerne vo vysokej.
PB: Ja myslím, že áno.
ZD: K tomu zákonu sa vyjadrovalo niekoľko organizácií, operátorov a najväčších poskytovateľov v Čechách. Ja myslím, že ten zákon ...
DR: ... je postavený na skutočných pripomienkach skutočných ľudí.
ZD: Aspoň v tej prvej verzii, čo som videla.
PB: Áno, ja som počul, že veľa z pripomienok skutočne do zákona zapracovali.
ZD: Takže tá pracovná skupina. Tá figuruje na tej českej úrovni. Rovnako konferencie a iná spolupráca.
DR: Napríklad Kriminálne oddelenie Polície, prichádzate s ním do styku?
PB: Áno. Spolupracujeme, buď tak, že my ich na niečo upozorníme, čo ale úplne nie je bežné. Alebo sa nás na niečo pýtajú, väčšinou sa nás pýtajú či sme sa s niečím nestretli. To znamená, že my napríklad publikujeme nejakú správu, ako boli napríklad tie exekútorské e-maily, na základe čoho sa nám začali ozývať z rôznych kútov, že majú niekoho kto bol postihnutý, či nemáme k tomu nejaké údaje.
DR: Dá sa teda povedať, že Polícia vás spája s tými bežnými užívateľmi? Oni im niečo nahlásia a Polícia skontaktuje vás?
ZD: Skôr by som povedala, že tak ako v každom prípade, ktorý Polícia vyšetruje, potrebuje dôkazy z viacerých strán.

PB: My ale väčšinou neposkytujeme dôkazy, tie nemáme, skôr im poskytujeme konzultačnú činnosť. Oni sa napríklad opýtajú „Nemôžete nám poradiť, čo si myslíte o tomto? Neviete o niekom, kto vie?“, pretože my vďaka fungovaniu v tej centrálnej rovine máme veľa kontaktov, dokážeme im povedať na koho sa obrátiť. „My vám k tomu nič nepovieme, ale skúste sa opýtať toho a tam, oni by vám mohli poradiť a niečo k tomu mať.“
ZD: Takisto spolupracujeme so Safer Internetom. V podstate každý, kto nás osloví so žiadosťou o nejakú prednášku či už k zákonu alebo k bežnej operatíve CSIRT tímu a podobne. A nemusí to byť zrovna technické publikum. Prednášali sme učiteľom na Akadémií, škála užívateľov, pre ktorých sme prednášali je naozaj široká.
DR: To je tá osvetová činnosť, ktorú máte v povinnostiach. Pravda?
ZD: Presne tak. Je to nejaká forma spolupráce. Teraz napríklad pripravujeme školenie pre jednu konkrétnu školu, pre učiteľov, ktorí učia informatiku. Skutočne kto nás osloví... Napríklad aj televízia.
PB: Teraz sme robili detský televízny program.
ZD: Lovci záhad. Takisto aktivity, ktoré má naše združenie CZ.NIC, napríklad seriál Ako na internet. Tam, kde sú otázky bezpečnosti a týka sa to bezpečnosti, tam navrhneme nejaký diel.
PB: Ešte k tej Polícií. Robili sme školenie napríklad pre Políciu, celkom úspešne. Pôvodne malo byť pre 40 ľudí a nakoniec ich prišlo naozaj veľa, cez 100 ľudí určite.
DR: To školenie bolo zamerané na...
PB: To školenie bolo zamerané na Internet všeobecne, aby mali nejakú predstavu o tom, ako vyťažiť z Internetu informácie, ako sa o niekom niečo dozvedieť. Napríklad o vyšetrovaných, niečo najviac, ako nájsť väzby v sociálnych sieťach a podobne. Tá tretia časť bola forenzná analýza, to znamená, taký všeobecný prehľad o tom, čo môžu čakať od tých „ajťákov“, aby vedeli, že sa dá napríklad zistiť, že niečo bolo vytlačené na nejakej tlačiarni alebo sa dá zistiť, na ktoré stránky ten človek išiel. Všeobecný prehľad o tom, čo sa dá očakávať. Robili sme aj pre štátnu správu, ČTÚ školenie na mieru.
DR: S tým trochu súvisí aj výskum. Zúčastňujete sa aj nejakých výskumov?
ZD: To ani nie.
DR: Napríklad so školami, Masarykova univerzita alebo ...
ZD: Napríklad IT14 sme robili v spolupráci s ČVÚT.
PB: To skôr v rámci prednášok v tom projekte. Ale že by sme sa zapojili priamo do nejakého výskumu, to aktuálne nie. Pripravujeme momentálne svoj výskumný projekt, ale to je naše. Výsledky budú ale verejné.
DR: Čiže mi zatiaľ nemôžete povedať, na čo bude ten výskum zameraný?
PB: Všeobecne aj áno. Chceme vybudovať systém, ktorý nám umožní z dát, ktoré máme momentálne, ono tých zdrojov dát je totiž obrovské množstvo. Okrem toho, že nám chodia incidenty, ktoré sú nám hlásené, tak odoberáme, respektíve máme možnosť odoberať informácie o rôznych problémoch tu v českej sietí z rôznych zdrojov, ktorí sa tým zaoberajú. Skupiny ako tím Cymru, ShadowServer a podobne. Človek sa ale musí vždy sám pozrieť na tie zdroje, odkiaľ to ShadowServer a tímy berú. Oni majú prístup k nejakému starému botnetu a dokážu identifikovať užívateľov, ktorí sú v ňom zapojení. Majú teda napríklad zoznam IP adries pre Českú republiku, ktoré sú zapojené k nejakému starému botnetu. Tie by stálo za to nejako kontaktovať, v tejto chvíli to ale nie je možné nejako jednoducho analyzovať. Takže by sme chceli urobiť systém, ktorý nám pomôže toto urobiť, osloviť tých užívateľov a zároveň nám pomôže urobiť tie analýzy, ktoré by nám ukázali nejaké trendy alebo nám pomohli identifikovať nové udalosti, alebo nové incidenty, ktoré sa v sieti dejú. Ale to je beh na dlhú trať, to nepostavíme za týždeň ani za mesiac.
DR: Samozrejme, ale niečo chystáte. Ak sa môžeme vrátiť k tej spolupráci s ostatnými CERT a CSIRT tímami.
ZD: Ak myslíte na českej úrovni, tak je dobré spomenúť projekt Fénix, v ktorom je združených, v súčasnosti asi 10 CSIRT tímov. Mnoho operátorov svoje CSIRT tímy má, takže tá spolupráca prebieha často aj bilaterálne. Nie je to vyslovene spolupráca, ktorá by bola spísaná formou memoranda. Tým, že Česká republika je pomerne malá a tých tímov nie je veľa, je tam mnoho osobných kontaktov. To znamená, že často sa na nás obrátia neformálne či sme niečo také riešili, či im nevieme pomôcť s riešením toho a onoho problému, Občas sa obrátime my na nich. Je to skutočne aj na tých osobných vzťahoch.

PB: My máme práve zriadenú aj takú chatovaciu miestnosť, práve pre tie CSIRT tímy. Je to také rýchle, ako som hovoril, keď potrebujeme rýchlo niečo vyriešiť, niekto niečo nové objaví a chce na to upozorniť ostatných, tak iba napíše, že si všimol to a ono, a niekto zareaguje.
DR: Je to niečo verejné alebo?
PB: Nie, je to vyslovene interné. Preto ani nehovorím, kde to je.
DR: Interná sieť. Teda na tej medzinárodnej úrovni ste členom ENISY, prispievate na FIRST...
ZD: Aby som to vzala z druhej strany. V súčasnosti vo svete existujú dva také, my to voláme telefónne zoznamy CERT / CSIRT tímov. A my sme členom Trusted Introducer, keď sa pozriete na ich stránky, sa tam väčšinou objavujú európske tímy. Často tam aj prezentujeme, pretože sú to uzatvorené fóra a väčšinou sa tam prezentujú konkrétne prípady, ktoré sme napríklad v Čechách riešili, ako sme to riešili a výsledky. Druhé medzinárodné fórum je práve FIRST, kde je v podstate celosvetové členstvo, a tam by sme sa chceli stať členmi v priebehu tohto roku. Jeho fór sa samozrejme zúčastňujeme pravidelne.
DR: Dá sa určiť ako často, koľkokrát za rok vycestujete a zúčastnite sa takýchto medzinárodných konferencií?
ZD: Ten Trusted Introducer usporadúva spoločné stretnutia 2-3x za rok, FIRST raz ročne. V ENISE nie sme členmi, to je Európska agentúra...
DR: Myslela som skôr, že keď usporadúvajú stretnutia, ste na nich zúčastnení.
ZD: To áno. Členstvo ako také sa vzťahuje k TI a FIRST, kde tím musí mať formálne predpoklady k tomu, aby sa stal členom. Pri ENISE platí, že pokiaľ pôsobíte v členskom štáte EÚ, patríte k nej. K jej cvičeniam, ktoré usporadúva ENISA, sme v súčasnosti koordinátori za Českú republiku, sú to cvičenia CyberEurope a myslím, že sa budú konať každé dva roky. S ENISOU spolupracujeme nielen na cvičeniach, ale aj rôzne workshopy, stretnutia národných a vládnych CSIRT tímov. Rovnako sú konferencie nielen pre CSIRT tímy ale aj bezpečnostných analytikov, kam skôr chodia kolegovia, takže v podstate vycestujeme... Dosť.
DR: Takže desiatky.
PB: Ak by sa to sčítalo, tak áno. My sa často zúčastňujeme konferencií, ktoré si robia CSIRT tímy sami pre seba. Napríklad v Estónsku je raz za rok konferencia zameraná na ľudí z CSIRT tímov, práve v dobe, kedy prebieha FIRST. Tá v Estónsku je zameraná viac na technikov, tam sa riešia technické veci, detaily rôznych útokov a je to len na pozvánku. Takže sa tam dostanú len členovia z komunity, aby bolo overené, že neuniknú nejaké informácie. Zraz bezpečnostnej komunity etablovaných CSIRT tímov. Tiež ma napadlo, že sme členmi V4 komunity.
ZD: Minulý rok alebo už to budú dva roky, práve NBÚ inicioval spoluprácu V4 a jej CSIRT tímov s tým, aby vznikla platforma, trošku menšia ako Trusted Introducer. Pretože v tých veľkých organizáciách je problém, že tých tímov je skutočne veľa a tie bilaterálne vzťahy sú náročnejšie na nadväzovanie. Vznikla teda platforma CECSP – Central Europe Cyber Security Platform. Práve s ňou sa uskutočnilo už niekoľko stretnutí. Je potrebné si uvedomiť, že tie CERT tímy, CSIRT tímy sú pomerne nová záležitosť a každý ten tím je trošku iný, každý funguje trošku inak. Napríklad na Slovensku je v súčasnosti jeden tím, ktorá zastupuje národný aj vládny tím. Takže každý ten tím má aj trošku inú agendu, používa trošku iné nástroje, ako sme spomínali tie ticketovacie systémy, každý ich má prispôsobené trošku inak, používa iné funkcie, zbiera iné zdroje. Práve na takýchto platformách ako je CECSP a podobne sa tieto skúsenosti zdieľajú. Práve na týchto stretnutiach sa o projektoch ako je tím Cymru, ShadowServer dozvedáme a máme možnosť sa na nich podieľať a zapojiť do spolupráce odoberať dáta a podobne.
DR: Keď ste spomínali tie vlastné úpravy nástrojov a funkcií, aké máte vy?
PB: Niektoré sme už spomínali, ale rozmýšľam, aké tam ešte sú. Hovorí nám to veci, ktoré potrebujeme pre tú našu prácu, úpravy ako vyhodnocovanie ticketov, že nám to rovno povie či je to phishing a podobne.
ZD: Práve to OTRS aj RTIR sú open-source systémy, takže sú otvorené práve na to, aby si ich tí administrátori, respektíve ľudia, ktorí ich budú využívať, prispôsobili na svoje požiadavky. Takže nám tam napríklad spadajú hlásenia incidentov podľa zákona. Každý ten ticketovací systém pracuje trochu inak ale plní rovnakú funkciu.
DR: V podkladoch mám vypísané konkrétne vízie, ku ktorým by som chcela počuť vaše, kľudne aj osobné, vyjadrenie. Zaujala ma jedna vec, ako hrozbu vníma Česká republika, že môže byť testovacím objektom pre napadnutie zvyšku Európskej únie. Myslíte si, že váš informačný systém je nejako slabší oproti ostatným krajinám alebo náchylnejší na nebezpečenstvo?

ZD: Ja by som sa nad tým problémom zamyslela trochu inak. Je potrebné si uvedomiť, že hrozby, ktoré sú, napríklad ako minulý rok „heartbleed bug“ a podobne, vnikajú do systému cez nejakú chybu, dieru. V OpenSSL sa na to prišlo po 15 rokoch a ohrozilo to takmer každý štát na svete, s tým, že OpenSSL používajú vládne inštitúcie aj súkromné inštitúcie. Je dôležité preto definovať najskôr tú hrozbu a následne sa zamyslieť nad tým, či by sme byť nejaký takýto testovací panáčik.
DR: Mňa len prekvapilo, že sami seba a svoj systém dehonestujú na úroveň najslabšieho článku.
PB: Ja si myslím, že to takto nebolo myslené, že tým, že máme malé množstvo užívateľov, to znamená, že keby si chcel nejaký štát či organizácia vyskúšať či dokáže položiť nejakú krajinu v oblasti kybernetickej bezpečnosti, tak je lepšie vybrať si nejaký menší štát, kde tých systémov nie je toľko a môže na ne zaútočiť väčšou silou. Ja si myslím, že je to myslené takto. Takto sa to stalo vtedy v Estónsku, kde to bolo dosť veľké. Nepamätám si detaily, ale určite sa to dá niekde dohľadať. Bolo by určite zložitejšie zaútočiť napríklad na Nemecko, ktoré ma väčšie množstvo užívateľov a informačných systémov a ten dopad sa určite ľahšie rozptýli v porovnaní s menšou krajinou ako sme my.
DR: Tým, že vy sa stretávate na prednáškach a podobne aj s bežnými užívateľmi, viete povedať ako veľmi počítačovo negramotní alebo gramotní sú tí ľudia?
PB: Povedal by som, že sú počítačovo gramotní, že to sa zlepšuje, ale hrozby stále podceňujú.
ZD: Hlavne tie hrozby sú stále sofistikovanejšie.
PB: Stále sa vyvíjajú. Sú stále múdrejšie. Pred pár rokmi nikoho ani len nenapadlo, že ak vy budeme mať zlé heslo do Facebooku, tak to ohrozí všetkých vašich kamarátov, lebo niekto sa k nim dostane a požiada ich o preposlanie napríklad SMS kódu. Takéto technológie tu pred pár rokmi rozhodne neboli a dnes je to úplne bežná vec, platiť cez mobil. Tie hrozby sa stále posúvajú a tí užívatelia na to nie sú dostatočne pripravení, hoci sú počítačovo gramotní, že to s počítačom vedia. Podcenia riziko, napríklad pri e-maily sa nezamyslia a automaticky na odkaz kliknú.
DR: Predpokladám, že aj vďaka vašej osvete sa stav zlepšuje. Ste ale jediný, ktorí robia takúto činnosť?
ZD: Práve Safer Internet sa to zameriava. On má ale cieľovú skupiny na deti. My ju máme všeobecnú.
PB: Pre nás asi najviac cieľová skupina sú asi správcovia v tých firmách, pretože práve tí, by mali svojich užívateľov ďalej edukovať nejakým spôsobom. My pôsobíme na nich, snažíme sa im dať rôzne návody ako si zabezpečiť serveri, oni potom následne môžu poslať do svojej siete e-mail, že CSIRT.CZ zverejnil nejakú hrozbu. Nemyslím si, že bežní užívatelia chodia čítať naše stránky, tak naivný nie som. Myslím si, že to čítajú administrátori, správcovia a tí, ktorí sú za sieť zodpovední a je na nich, aby varovali svojich zamestnancov, aby si dali pozor. Celá osveta ale záleží na tom, aké médium človek použije a koľko ľudí sa mu podarí osloviť.
ZD: Presne aj vďaka tomu, že sme v združení CZ.NIC, tak napríklad aj ten seriál mal pomerne veľký dosah, lebo bol odvysielaný pred hlavnými správami. Samozrejme, že by sme tou osvetou chceli dosiahnuť na čo najviac cieľových skupín, ale treba si uvedomiť, že to nie je úplne reálne. Osloviť úplne všetkých. Ono aj kybernetická bezpečnosť sa nejakým spôsobom vyvíja a zároveň s ňou aj my postupujeme. Keď však užívateľ nemá záujem, nejakým spôsobom sa o to nezaujíma, tak sa k nemu nedostaneme. Pokiaľ tam je ten záujem, tak sme nápomocní, urobíme kurz, tých činností je skutočne veľa. Rovnako skutočnosť, že sme last resort, tak najskôr by mali ísť za svojim správcom.
DR: Túto osvetovú činnosť a prednášky máte na starosť konkrétne vy?
PB: To záleží napríklad na tom, ako moc je to technické. Väčšinou si to nejako rozdelíme, kto kedy môže. Záleží od témy, kde to je, pre aké publikum a podobne.
DR: Jednou z hrozieb je nedostatok odborníkov na kybernetickú bezpečnosť. Ako to vnímate vy napríklad s prijímaním nových členov k vám? Máte problém s tým nájsť naozaj niekoho špecializovaného?
PB: Ono je to tak, že väčšinou si vezmeme nejakého skúseného technika a my si ho doškolíme na oblasť bezpečnosti. Väčšinou tí ľudia, ktorí sú dobrí administrátori, skúsenosti s tou bezpečnosťou majú. Ide potom o to doplniť si znalosti z tých častí, ktoré bežne človek nerobil alebo nespravoval. Takže takto.
DR: Takže na školách sa takéto odbory vôbec neučia?
PB: Oni sa práve začali otvárať. Predtým si nemyslím, že existovali.

ZD: Je potrebné si uvedomiť, že každý správca alebo administrátor sa tou bezpečnosťou zaoberá. Respektíve by mal. Pár rokov dozadu kybernetická bezpečnosť pomaly neexistovala a bola braná ako súčasť programovania alebo súčasť správy. Ale teraz sa na tom bazíruje čoraz viac.
DR: Ďalej ma zaujala jedna informácia, že sa plánuje zmeniť prevádzkar národného CERT tímu.
PB: Ono je to tak, že národný tím CERT sa vyberá na základe zákona. My z dôvodu, že sme to robili historicky, tak po dobu, kým dôjde k výberovému riadeniu, tak tá pozícia prevádzkovateľa pretrváva u nás a my to do tej doby spravujeme. Ale o tom, že bude výberové riadenie vieme, to má prebehnúť tento rok.
DR: Takže vy ste túto funkciu dostali na základe toho, že ste to už predtým robili.
ZD: Dobré je si uvedomiť, že národný CSIRT tím, keď vznikol na základe memoranda (pozn. Memorandum o Computer Emergency Response Team / Computer Security Incident Response Team České republiky) s Ministerstvom vnútra ČR, dostal nejaké povinnosti, napríklad rozvíjať agendu národného CSIRT tímu a podobne. Ale keďže to tu nikdy predtým nebolo, tak je procesom budovania myslené hlavne definovanie kompetencií, čo by mal národný CSIRT tím robiť. To sa vyvíjalo a vyvíja doteraz. Po prechode problematiky kybernetickej bezpečnosti pod NBÚ, sme uzavreli memorandum s nimi. Na základe tohto memoranda vykonávame funkciu prevádzkovateľa.
PB: To memorandum je napísané rovno s tým, že sa počítalo, že na základe toho zákona sa vyberie niekto nový. Že to memorandum platí do konca tohto roku, myslím. Behom tohto roku teda musí prebehnúť výberové riadenie, kedy na jeho základe bude vybraný nový prevádzkovateľ.
DR: Predpokladám, že vy sa o túto pozíciu stále uchádzať budete. Viete aj o iných konkurenčných tímoch, ktoré by túto pozíciu oficiálne chceli získať?
PB: Nevieme. Oficiálne ani neoficiálne. Nepočul som o nikom konkrétnom.
ZD: Čo by som spomenula je, že v tom zákone je niekoľko podmienok, za ktorých môže niekto vykonávať túto pozíciu. Ja som práve počula, že nejakí záujemcovia sú, ale málokto vie, že to robíme bezúplatne.
PB: Áno, to je pravda.
ZD: To je dôležité povedať, že od štátu za to nič nedostávame.
PB: Ja som teda počul takú vec, myslím, že to hovorila Andrea (pozn. Andrea Kropáčová, jedna zo zakladajúcich členov CSIRT.CZ), že z toho národného CSIRT-u sa stala trochu značka. Že aj komerčná firma, ktorá vyrába komerčný produkt, by mohla mať teoreticky záujem, pretože by si to dala ako punc „my robíme národný CSIRT“. Ale myslím si, že si neuvedomujú, čo to obnáša, aké je to personálne obsadenie. Neznamená to, že na to vyčlenia jedného človeka, ktorý sa tomu bude venovať. Tak uvidíme.
ZD: Potom je tam riziko, keby národný CSIRT spadal pod nejakú konkrétnu komerčnú spoločnosť, ktorá by presadzovala nejaké konkrétne riešenia. My sa snažíme byť vo všetkom čo robíme neutrálny, nepresadzovať nejaké konkrétne riešenia. Takže ten záujem u súkromných spoločností tam je. Ale tam je skutočne náročné zabezpečiť to, aby ich riešenia alebo to, čo odporučia bolo neutrálne.
DR: Jasné. Myslím, že k tejto téme stačí, aby som do toho nezasahovala príliš veľa. Keďže ste spolupracovali pri tvorbe zákona a teraz viete ako vyzerá, chýba vám tam niečo? Myslíte si, že sú ešte potrebné nejaké ďalšie obmedzenia?
PB: Ja si myslím, že by tam malo byť niečo o tom, že tí členovia CSIRT tímov, aspoň týchto dvoch, by mali byť nejakým spôsobom, ako to povedať, riešené, za čo sú trestno-právne zodpovední. Občas sa musí človek presvedčiť o tom, že ten problém tam naozaj je. Pretože my si musíme udržovať nejakú dôveryhodnosť a nemôžeme preposlať všetko, čo nám niekto pošle. Takže občas sa musíme pozrieť, že ten problém reálne existuje a nie na každý problém sa dá pozrieť bez toho, aby mal človek nejaké oficiálne právomoci. Snažíme sa tomu vyhnúť, ale sú situácie, kedy nám toto robí problém. Keby tam bolo ošetrené to, že ľudia ktorí pracujú v týchto tímoch za určitých okolností, jasne daných, sa môžu pozrieť, či v tom systéme tá chyba naozaj existuje. Toto by tým ľuďom určite pomohlo. Ono ale sa asi ten dotyčný, keď ho upozorníme, že má bezpečnostný problém, sťažovať nebude.
DR: Takže toto ešte nie je ošetrené. Lebo ono je problém s tým, že kým sa parlament „rozhýbe“ a kým je návrh schválený, tak medzitým sa celá tá móda, celý ten smer, ktorým sa kriminalita uberá, zmení.
ZD: No ja si myslím, že práve tam je ten problém, že ono sa to vyvíja a my sami nevieme čo bude o pol roka, čo bude o rok, ako to bude fungovať. Ja som v tíme dva roky a vidím, že sa to skutoč-

ne mení, stále sa tvorí niečo nové. Takže definovať nejaký konkrétny zákon, je pre mňa nepredstaviteľné.
DR: Čiže si myslíte, že tie definície pre kritickú infraštruktúru, pre kyberpriestor, pre všetky tie záležitosti sú dostačujúce? Lebo niektorí ľudia sa sťažujú, že je to také vágne, také neurčité.
ZD: Ono práve to, aby ten zákon prešiel, tak sa muselo, je potrebné si uvedomiť, že sa muselo prijať strašne veľa kompromisov. Čo je to kybernetický priestor. Keby sme to chceli opísať, tak by sa mohlo stať, že o rok by to už neplatilo alebo by sa to zmenilo. Takže si myslím, že to bolo cieľ, aby to bolo také vágne.
DR: Aby sa to dalo prispôsobiť na každý prípad, K tomu ma napadlo, že by mal byť vytvorený nejaký koordinovaný postup, ktorý by mali pri tých bezpečnostných incidentoch alebo vyšetrovaní, alebo pri tých hláseniach CERT tímy dodržiavať. Je niečo také, čo by malo platiť naozaj pre všetky tímy? Ako by sa mali správať?
ZD: Konkrétne, napríklad ak si pozriete RFC 2350, máme to na stránkach, je to dokument prijatý od IETF. To je taký nejaký návod na to, ako by mal taký CSIRT tím fungovať, čo by o sebe mal zverejniť, aké informácie, aké úlohy by mal plniť, ako by mal tie incidenty riešiť, ako si ich zaznamenávať a podobne. To je taká nejaká všeobecná brožúrka.
DR: A používa sa aj v praxi? Je to tak, že dostanete hlásenie, tak si nalistujete?
ZD: My to už vieme. To sú také postupy, ktoré CSIRT tímy aj bez toho, aby si to museli prečítať, tak logicky k tomu dospejú. Že aby sme sa vedeli napríklad k nemu (pozn. bezpečnostnému incidentu) dostať, tak je potrebné mu prideliť číslo. To je skôr taká bežná prax.
DR: Rozmýšľam, že som vyčerpala všetky svoje podklady. Úprimne som bola prekvapená, že je to prvý zákon o kybernetickej bezpečnosti, ktorý bol vytvorený, že predtým asi nič kvôli technológiám nebolo potrebné. A myslím si, že na Slovensku asi ani žiadny taký nemáme.
ZD: Nemáme.
DR: A z tej V4 ste jediný, keď Slovensko nemá? O Maďarsku a Rakúsku teda neviem, úprimne.
ZD: Zákon? Ja myslím, že celkovo v Európe sme buď jediný alebo jedny z mála, no.
DR: Až takto, že v podstate na európskom formáte je to výnimka.
ZD: Čo je dobré spomenúť je ale direktíva Európskej komisie. Aj ten zákon bol v podstate robený k tomu, ak by sa tá direktíva schválila a tie podmienky by platili pre všetky členské štáty, tak sú len minimálne rozdiely s tým zákonom. Nemuseli by sme prijať nijaké riešenia a ten zákon by to „pohltil“ sám.
DR: Tá je ale ešte stále v rokovaní?
ZD: Áno, tá ešte nie je schválená.
DR: Takže zatiaľ Európska únia nemá žiadny zákon, ktorý by to ošetroval?
ZD: Zatiaľ nie a aj toto by bola len direktíva a nie zákon. Ono veľa tých členských štátov má svoje podmienky definované pre CERT tímy, ale nie je to riešené vyslovene zákonom. Môže to byť formou nariadenia, vyhlášky alebo niečoho takého. Napríklad tá vyhláška (pozn. Vyhláška č. 316/2014 Sb. a Vyhláška č. 317/2014 Sb.) je už celkom konkrétna. Ten zákon, ako ste hovorili, je skutočne vágny, tak práve tá vyhláška už definuje konkrétne technické požiadavky na zabezpečenie tých systémov a podobne.
PB: Ale to, ako hovorila Zuzka, bol zámer. Aby sa to tou vyhláškou dalo korigovať, podľa toho čo sa ukáže ako aktuálny problém, lebo ono ako sa to veľmi vyvíja, tak sa to dá ťažko dopredu napasovať. Myslím, že to práve urobili dobre, že urobili zákon vágny a vyhláškami to budú...
ZD: Oni ten zákon nebudú moc meniť. V prípade ak by ho chceli zmeniť, je to pomerne náročný proces, kým vyhláška...
DR: ... sa dá meniť oveľa rýchlejšie.
ZD: Presne tak.
DR: A stáva sa napríklad to, že s vami niekto nesúhlasí? A môže vám váš postup, ako tímu, zatrhnúť?
PB: My nerobíme nikdy nič také, čo by mohol niekto zatrhnúť. Naša rola je naozaj len taká koordinačná. My tie incidenty nikdy neriešime, ani nemôžeme na nikoho tlačiť, aby ich vyriešil. My ich môžeme požiadať, ponúknuť im pomoc. Tie CSIRT tímy vznikli aj z toho dôvodu, že tam často býva komunikačná bariéra, že napríklad ten správca nevie dobre anglicky, príde mu nejaký e-mail a on ho hodí do koša, pretože si myslí, že je to spam, príde mu to dvakrát, trikrát, urobí to znova, ten človek na druhej strane sa naštve a napíše to národnému CSIRT-u a vyrieši to. Takže to nie je tak, hoci nemôžeme vylúčiť, že by taká situácia nenastane, ale zatiaľ nenastala. My pre NBÚ re-

portujeme, robíme pre nich raz za rok výročnú správu, ale nedokážem si predstaviť, že by sa niekto na náš postup sťažoval.
ZD: Ono v podstate áno, NBÚ nás kontroluje, ono je xy iných neformálnych stretnutí, kedy sa stretneme na nejakej návšteve alebo podobne. Oni tu už niekoľkokrát boli, takže NBÚ vie, čo robíme, vie, ako to robíme.
PB: Ale nemá k tomu výhrady. Asi keby mal, tak by zasiahol a oficiálne by nám povedali, že to máme robiť inak. Ale táto situácia zatiaľ ešte nenastala a dúfam, že nenastane. Že to robíme dobre.
ZD: Je potrebné si uvedomiť, že ako som hovorila, ten CSIRT tím vznikol v 2008 ešte na akademickej pôde. Ku nám (pozn. združeniu CZ.NIC) prišiel v 2011, kedy sa o národnom CSIRT tíme ani nechyrovalo, takže on musel odniekiaľ čerpať informácie, o tom ako ten tím funguje, čo rieši, takže tá komunikácia s NBÚ tam bola od začiatku. Takže keby mali nejaké výhrady, určite nám dajú vedieť.
PB: Navyše sme plnili rolu aj vládneho CERT-u, kým ešte neexistoval a nikdy nebola žiadna výhrada k tomu akým spôsobom sme to riešili alebo tak.
DR: Takže ste boli modelová situácia, ale zároveň ste boli inšpiráciou pre rozvoj.
ZD: Ja myslím, že áno. Určite áno.
DR: Takže som priamo pri zdroje, to je super. Tak rozmýšľam, že Vás už nechcem dlhšie zdržiavať, myslím, že mám naozaj všetko, ale chcem Vám poďakovať za spoluprácu.
ZD: Nemáte začo.
PB: Nie je začo.

Príloha 9: E-mail

PREDMET: Doplňujúce otázky k bakalárskej práci
ODOSIELATEĽ: Zuzana Duračinská
PRIJÍMATEĽ: Dominika Rezníčková
DÁTUM ODOSLANIA: 8.4.2015

Dobrý deň,

Dňa 7.4.2015 o 10:36 d.reznickova napísal(a):
Dobrý deň,
dostala som sa k poslednej časti svojej bakalárskej práce, to jest predstaveniu CSIRT.CZ. Na základe informácií z webových stránok a nášho interview mám dosť podkladov, ale predsa len ma napadlo pár dodatočných otázok hlavne technického charakteru. Bola si bol vďačná, ak by ste mi na ne mohli odpovedať:

1) Používate pri e-mailovej komunikácií s organizáciami či inými tímami na národnej či medzinárodnej úrovni digitálne podpísané alebo šifrované e-maily? Napr. systémom PGP, S/MIME, GnuPG...
Áno, každý člen týmu má svoj PGP kľúč a zároveň je PGP kľúč dostupný aj na abuse@csirt.cz kde sa zasielajú incidenty. Každý tím má povinnosť mať PGP kľúč, takže túto formu komunikácie využívame takisto s ostatnými tímami.
2) Na akom operačnom systéme fungujete? Linux, Windows XP, Windows 2007 atď. alebo software umožňujúci striedať rôzne operačné systémy VMware, VirtualPC/VirtualServer?
Všetci využívame distribúciu Linuxu. K forenznej analýze a na rôzne iné účely máme dostupné aj virtuály (VMWare).
3) Používate nejaký konkrétny bezpečnostný software, napríklad antivírové scanery, firewally, programy proti spywaru? (Kľudne konkrétne názvy)
Firewally samozrejme využívame. Čo konkrétne si predstavujete pod pojmom bezpečnostný software?
4) Aký systém používate na zálohovanie dát? (Fyzické zálohovanie na DVD ... alebo ukladanie na online storage?) Kontrolujete tieto zálohované dáta na pravidelnej báze, ako často?
Všetky dáta zálohujeme podľa interných smerníc združenia.
5) Používate nejaký CRM software určený pre riadenie starostlivosť o zákazníkov? SugarCRM, Sugarforce, prípadne iný?
Žiadnych zákaznikov nemáme. Pokiaľ sa niekto dotaze na csirt.cz, jeho požiadavky sa riešia cez ticketovací systém.
6) V prípade vyhľadávania kontaktných informácií (ak ich nedostane priamo z hlásenia alebo ich nedohľadá váš ticketovací systém) využívate informačné zdroje, napríklad RIPE Network Coordination Centre?
RIPE databázu, ako aj databázy ostatných RIRov využívame na dennej báze.
7) ENISA ponúka v dokumente CSIRT Setting up Guide obrázok s kompletným výčtom možných služieb poskytovaných CSIRT tímom. (pripojený v prílohe) Dokážete z nich vybrať konkrétne tie, ktoré poskytujete vy?

Ako Národny CSIRT tím poskytujeme takmer všetky zo spomenutých služieb. Služby ako napr. "řešení zranitelnosti" nieje možné vzťahovať na tím na národnej úrovni. Tam by bolo nutné definovať, čo sa pod riešením zranitelností všetko myslí. Služba ako je táto, je skôr službou interných tímov a to vykonávame v rámci združenia pod havičkou bezpečnostného tímu CZ.NIC-CSIRT. Čo sa týka kategórii "Management jakosti bezpečnosti", tam ide takisto o služby, ktoré spravidla poskytujú tímy interného typu.

Veľmi pekne ďakujem za odpovede. Je možné získať špecifické informácie, napríklad keďže pôsobíte pre ENISu ako koordinátor za Českú republiku alebo v prípade väčšej hrozby máte skoordinovať spoluprácu viacerých tímov? Naozaj potrebujem konkrétne informácie typu: "Dňa XY nám prišiel e-mail/nás oslovila ENISA/nám bol nahlásený incident, obsahoval novú hrozbu, vírus XY, ktorý sme ešte nevideli, tak sme touto a touto cestou skontaktovali tím XY... Odpoveďou bola dňa ... správa / dňa XY sme zaslali pozvánku na ENISA konferenciu/cvičenie tým a tým tímom... Samozrejme napríklad v prípade bezpečnostného incidentu mi nemôžete poskytnúť informácie o organizácií, skôr mi ide o vašu úlohu a vašu koordinačnú činnosť. Ak by sa Vám podarilo niečo také konkrétne napísať, bola by som Vám vďačná.

Pre ENISU pôsobíme iba ako koordinátor pre oblasť cvičení Cyber Europe. Koordinácia tohto cvičenia prebehla postupne s všetkými tímami, ktoré sme pre účasť na cvičenie oslovili. Viac info k tomuto cvičeniu a jeho priebehu nájdete napr. tu:
https://blog.nic.cz/2015/03/19/uspesne-ukoncenie-cvicenia-cyber-europe-2014/
a
https://blog.nic.cz/2014/05/06/bezpecnostne-tymy-testovali-svoje-schopnosti/.

ENISA členských štátom incidenty nehlási (vo výnimočných situáciach sa tak však stať môže). Rola ENISY je iná a pôsobí skôr v oblasti vzdelávania CSIRT tímov, vytvára reporty týkajúce sa aktuálnych trendov, má politickú úlohu a podobne.

Ako príklad koordinácie môžete využiť DDoS útoky z marca 2013. Info ako
sa postupovalo najdete tu:
https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/conference/2nd-enisa-conference/presentations/andrea-kropacova-cesnet-ddos-attacks-against-www-server-providers-in-the-czech-republic

Kolegyňa k týmto útokom a našej koordinácii spísala dobrý článok, skúsim to od nej získať a poslať vám to. Vzhľadom k tomu, že to bol zatiaľ najväčší plošný útok, myslím, že by bol ideálny na pochopenie role tímu.
Ako reakcia na tieto útoky vznikol tiež bezpečnostný projekt FENIX, takže to malo aj pomerne veľkú odozvu po samotných útokoch.

Ostávam s pozdravom a prajem pekný deň,

Zuzana Duračinská