Zpráva o činnosti

CSIRT.CZ

(Národního CSIRT ČR)

za rok 2014

Vypracoval:

Dne:

Úvod

Tým CSIRT.CZ

*plní od 1. ledna 2011 roli Národního CSIRT České republiky. Stalo se tak rozhodnutím Ministerstva vnitra ČR a uzavřením Memoranda o provozu Národního CSIRT ČR, které MV ČR a sdružení CZ.NIC podepsali v prosinci 2010. Dne 19. října 2011 přijala vláda České republiky usnesení č. 781 o ustavení **N**árodního **B**ezpečnostního **Ú**řadu gestorem problematiky kybernetické bezpečnosti a zároveň národní autoritou pro tuto oblast. Na jaře 2012 proto došlo k revokaci Memoranda o provozování Národního CSIRT ČR, které uzavřeli sdružení CZ.NIC a MV ČR v prosinci 2010, a bylo podepsáno nové Memorandum mezi sdružením CZ.NIC a Národním Bezpečnostním úřadem. Toto Memorandum mělo platnost do konce roku 2012. Dne 19. prosince 2012 pak bylo uzavřeno nové Memorandum mezi sdružením CZ.NIC a Národním Bezpečnostním Úřadem o provozování Národního CSIRT ČR s platností od 1. ledna 2013 do konce roku 2015.*

Rok 2014 v kostce

Rok 2014 byl velice zajímavý především z hlediska rozvoje základních schopností týmu a jeho služeb, kterými jsou – řešení bezpečnostních incidentů, Skener webu, nekonečný tutoriál Aktuálně z bezpečnosti, služba MDM (Malicious Domain Manager), školení, osvětové akce atd. Potěšující je především to, že se nám podařilo prohloubit symbiósu jednotlivých služeb a lépe využít získaných informací k akcím preventivního charakteru, např. varování uživatelů před další vlnou phishingových kampaní, získání a distribuce informací o infikovaných strojích a uživatelských identitách apod. Každá z poskytovaných služeb prošla také interním vývojem, který danou službu zefektivnil, zjednodušil její obsluhu a zpřesnil výsledky.

V oblasti osvěty, národní a mezinárodní spolupráce jsme pokračovali v udržování již navázané spolupráce v rámci Pracovní skupiny CSIRT.CZ, Pracovní skupiny E-CRIME, v pracovních skupinách organizací ENISA a TERENA, s Bankovní asociací, NCBI (Národní Centrum Bezpečnějšího Internetu), s lokálními bezpečnostními týmy, které působí v sítích významných ISP, registrátorů, bank, s bezpečnostními složkami, akademickou sférou atd. Těší nás, že CERT/CSIRT infrastruktura v České

republice zaznamenává v posledních letech velký rozvoj, jen v roce 2014 se v České republice etablovalo sedm nových CERT/CSIRT týmů.

Absolvovali jsme také několik cvičení – dvě fáze (technické a organizační) cvičení **Cyber Europe 2014**, cvičení **NATO Cyber Coalition 2014**, cvičení **CECSP** a **národní cvičení** pořádané NBÚ.

V průběhu roku jsme se nadále průběžně zapojovali do připomínkování různých strategických dokumentů, např. vyhlášek k zákonu o kybernetické bezpečnosti, direktivě NIS, ale také ke strategii evropské infrastruktury CERT/CSIRT týmů v platformě TF-CSIRT, jejímiž jsme členy.

Závěr roku 2014 byl věnován přípravě týmu CSIRT.CZ na nabytí účinnosti zákona č. 181/2014 Sb., o kybernetické bezpečnosti, který Národnímu CSIRT týmu ukládá řadu povinností.

Služby poskytované týmem CSIRT.CZ

Incident handling a incident response

Služba *incident handling* a *incident response* (řešení a koordinace řešení bezpečnostních incidentů) je základní službou, kterou týmy nazývající se CERT/CSIRT plní a musí plnit v rámci svého definovaného pole působnosti. V případě CSIRT.CZ se jedná o řešení a koordinaci řešení bezpečnostních incidentů, které mají původ nebo cíl v sítích provozovaných v České republice, nebo se obecně dotýkají kyberprostoru České republiky.

Týmu CSIRT.CZ jsou adresovány problémy (tzn. reportovány incidenty a události) několika typů:

- problémy, u kterých se už vyčerpaly veškeré možné způsoby řešení, ale problém přesto přetrvává,
- problémy, u kterých není jednoduché identifikovat, kdo je původcem incidentu, nebo kdo by se jeho řešením měl zabývat,
- problémy, které mají závažný dopad na infrastrukturu v ČR, problémy, které mají plošný charakter a mohou negativně ovlivňovat mnoho sítí, služeb a uživatelů, a je tedy žádoucí, aby se informace co nejrychleji dostaly k těm, kdo mohou zasáhnout a nastavit vhodné metody obrany apod.

V roce 2014 jsme v oblasti řešení nahlášených bezpečnostních incidentů zaznamenali významný nárůst. Zatímco v roce 2013 bylo týmu CSIRT.CZ nahlášeno cca 495 incidentů, **v roce 2014** to byl téměř dvojnásobek – **939 incidentů**. Nárůst jsme ovšem nezaznamenali pouze v počtu řešených incidentů, ale také v jejich náročnosti. Incidenty, které jsou předávány k řešení týmu CSIRT.CZ nabývají na složitosti, komplexnosti a náročnosti na zpracování. Po provedení základní analýzy incidentu a nastartování rutinního procesu řešení (tzn. kontaktování osoby, která má prostředky problém vyřešit a odstranit) je často nutné provést ještě další akce, např. získat seznam dalších potenciálních obětí a jejich varování, dohledání v dalších zdrojích dat a informací informace o možných infikovaných počítačích, zneužitých uživatelských identitách, zranitelných zařízeních apod. Z tohoto důvodu je nutné zmínit nárůst počtu odeslaných e- mailů z **2281** v roce **2013** na cca **5000** v roce **2014**.

Statistika procesu řešení bezpečnostních incidentů týmem CSIRT.CZ:

	2008	2009	2010	2011	2012	2013	2014	2015	SUM
IDS				491	3924	2121	2380	241	**9157**
Phishing	65	220	209	144	159	175	368	28	**1406**
Spam	47	28	103	26	43	73	160	14	**498**
Malware	53	97	42	9	19	44	117	18	**414**
Other	1	5	8	62	13	75	100	27	**302**
Virus		121	178	1	1				**301**
DOS	1	4	2	2	68	72	32	4	**191**
Trojan	66	6	26	5	5	12	56	5	**185**
Probe		3	14	25	12	26	86	2	**172**
Botnet		3	46	5	8	15			**77**
Portscan	10	4	1	6	1	3	2		**27**
Pharming							18		**18**
Crack	1		4						**5**
Copyright			1		1				**2**
SUM	**244**	**491**	**634**	**285**	**330**	**495**	**939**	**98**	**12755**

Do celkového počtu řešených bezpečnostních incidentů (**v roce 2014 je to 939**) se nezapočítávají incident typu IDS (druhá řádka ve výše uvedené tabulce). Jedná se o automatizovanou službu typu Intrusion Detection System, která informuje správce koncových sítí o tom, že jejich síť je zdrojem (bezpečnostní) *události*, která následně může být zdrojem bezpečnostního

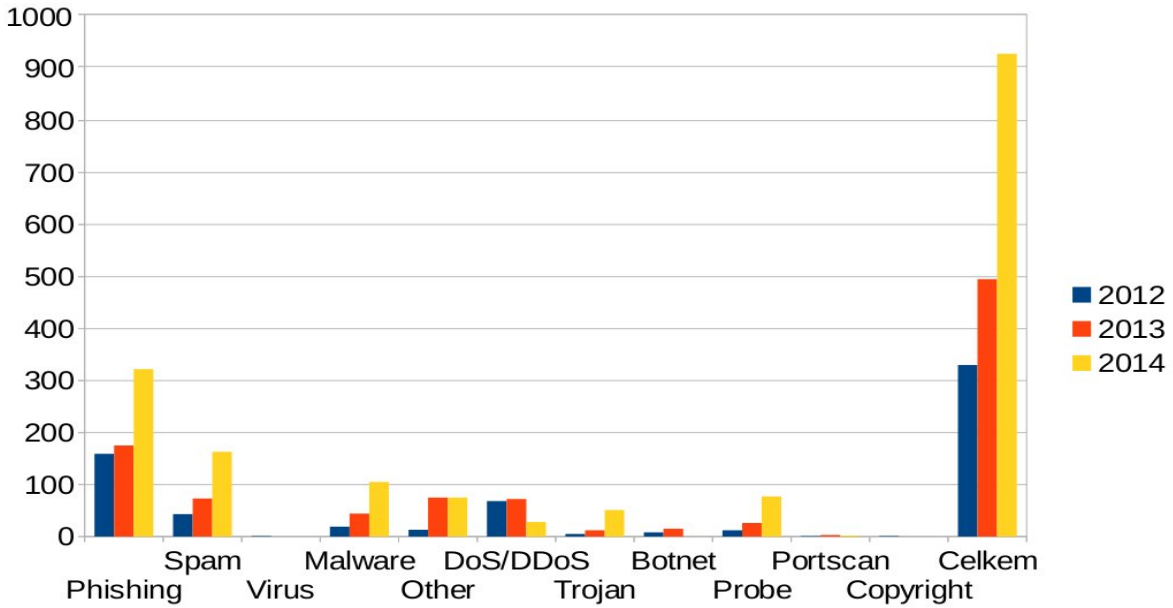
incidentu. Číslo 2380 v roce 2014 tedy představuje počet varování zaslaných touto službou správcům koncových sítí provozovaných v ČR.

Výše uvedená tabulka se statistikou bezpečnostních incidentů řešených týmem CSIRT.CZ není z hlediska výskytu a četnosti bezpečnostních incidentů reprezentativní a nelze z ní odvozovat globální trend. Je potřeba brát v úvahu, že k týmu CSIRT.CZ se v jeho roli Národního týmu ČR dostává pouze nepatrná část bezpečnostních incidentů, které mají původ nebo cíl v sítích provozovaných v ČR. Jediný trend, který ze statistiky můžeme odhadovat, je trend zvyšování počtu útoků na koncové uživatele (typy *phishing* a *malware*), které jsou týmu CSIRT.CZ hlášeny, a které tým řeší.

Statistiky z procesu řešení bezpečnostních incidentů jsou průběžně zveřejňovány na stránkách týmu:

https://www.csirt.cz/page/2635/statistiky-resenych-incidentu/.

Graf znázorňující nárůst počtu bezpečnostních incidentů hlášených týmu CSIRT.CZ za roky 2012, 2013 a 2014:



Zajímavé kauzy roku 2014

Rok 2014 přinesl v oblasti řešení bezpečnostních incidentů několik velice zajímavých kauz a to jak z procesu incident handling, tzn. z nareportovaných bezpečnostních incidentů, tak z objevených zranitelností. Zde přinášíme výběr toho nejzajímavějšího a nejilustrativnějšího z hlediska činnosti týmu v oblasti rutinního řešení incidentů a z oblasti preventivních akcí.

HeartBleed. Rok 2013 měl jako svou „stěžejní“ kauzu sérii DDoS útoků na www služby provozované v České republice, rok 2014 kauzu HeartBleed, zranitelnost nalezenou v OpenSSL knihovně, která umožňuje odchycení citlivých informací při komunikaci mezi klientem (např. pracovním počítačem, notebookem) a serverem. To činí tuto zranitelnost velice nebezpečnou. Tým CSIRT.CZ se snažil o nalezení a eliminování strojů provozovaných v ČR, které tuto zranitelnost obsahovaly. Celkově tak bylo nalezeno cca 5500 zranitelných IP adres, jejichž správci byli varováni.

ROM-0. Asi nejznámější incident v minulém roce byl ten, který se týkal zranitelnosti ROM-0 v některých routerech TP-LINK. Tato zranitelnost začala být aktivně využívána útočníky k útokům na klienty bank v České republice. Zranitelnost umožňuje napadení routeru útočníkem, který následně změní nastavení DNS serverů v routeru a oběť tak přesměruje na vlastní verze některých populárních vyhledávačů, kde pak nabídne obětem soubor s údajným update pro Flash Player, který však ve skutečnosti obsahuje malware.

Asus routery. Další, spíše preventivní akce, se týkala opět routerů. V tomto případě routerů Asus, kdy jsme na serveru Pastebin našli seznam routerů, které měly špatně nakonfigurovaný FTP přístup a umožňovaly tak přístup k připojenému disku jen s pomocí výchozího hesla. Informaci o zranitelných routerech jsme na základě IP adresy distribuovali příslušným správcům.

Se serverem **Pastebin** souvisí i další nález, tentokráte seznamu 1800 e- mailových adres českých uživatelů doplněných o heslo k dané schránce. I v tomto případě se tým CSIRT.CZ postaral o distribuci informace k příslušným správcům daných e-mailových služeb.

Podvodné phishingové kampaně. V uplynulém roce zaznamenala Česká republika několik vln podvodných phishingových kampaní zacílených na koncové uživatele. Jedna z těchto kampaní zneužívala značku České pošty; ta nejvýraznější a dle našeho názoru nejúspěšnější pak adresáta informovala o údajném dluhu. U těchto podvodných kampaní bylo zajímavé sledovat postupné zvyšování nátlaku na psychiku uživatele, kdy první kampaně pouze informovaly o údajně nezaplaceném dluhu, následné vlny pak již vyzývaly k úhradě dluhu s tím, že již probíhá exekuční řízení. Podle našich odhadů měla nejhorší dopad první vlna, kdy ještě uživatelé netušili, že by se mohlo jednat o podvod. Na druhou stranu malware v ní obsažený nebyl tak sofistikovaný a tak se nám podařilo velmi rychle zjistit, kde se v systému ukrývá, a včas nabídnout uživatelům návod na jeho odstranění. V této souvislosti musíme ocenit postoj a spolupráci společnosti Microsoft, která týmu CSIRT.CZ zdarma poskytuje přístup do své databáze MSDN, což nám umožňuje realizovat analýzy malware.

Bílí koně. V uplynulém roce se nám také podařilo medializovat problematiku najímání takzvaných bílých koní, ke kterému docházelo v České republice. Podle zpětné vazby od kolegů z bankovního sektoru se tato akce setkala s dobrou odezvou a uživatelé sami začali hlásit bankám pokud po nich někdo požadoval realizaci podezřelých finančních transakcí.

Naší zemi se bohužel nevyhýbají ani špionážní kampaně a tak zatímco před dvěma lety jsme řešili špionážní malware Red October, letos jsme ve spolupráci s vládním CERTem (GovCERT.CZ) řešili incident, který se vztahoval k útokům špionážní skupiny známé pod názvem **DragonFly**.

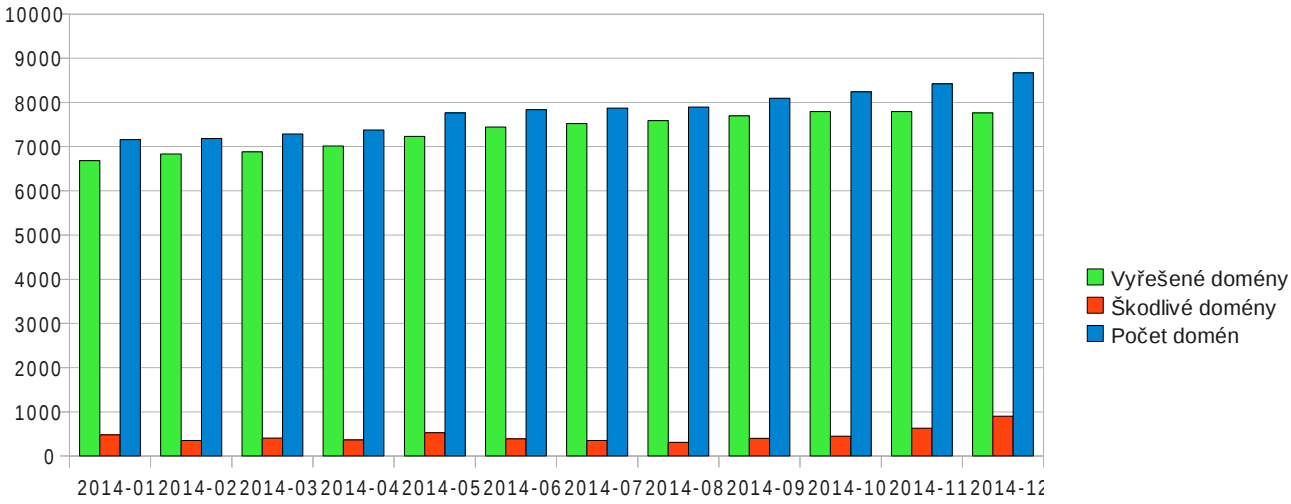
Všechny výše uvedené kauz jsme zúročili také v dalších službách a informovali jsme o nich také v seriálu AZB, jehož díly jsou pravidelně (denně) uveřejňovány na stránkách www.csirt.cz.

Služba MDM (Malicious Domain Manager)

Služba MDM využívá veřejně dostupné zdroje informující o doménách, které byly napadeny nějakým druhem malware a podobně. Pomocí služby MDM jsou data z těchto veřejných zdrojů vytěžena a týmem CSIRT.CZ přeposlána osobám zodpovědným za chod dané domény se žádostí o prošetření a

případnou nápravu situace.

Stručnou statistiku využití této služby za rok 2014 reflektuje následující graf znázorňující poměr „nakažených“ domén a domén, u kterých se po intervenci podařilo závadný obsah odstranit, a u kterých bohužel přetrvává.



V roce 2014 prošla služba MDM interním vývojem, kdy došlo k urychlení a zautomatizování procesu řešení incidentu. Každá doména s nahlášeným závadným obsahem prochází analýzou, jejímž cílem je nalézt skutečný zdroj infekce. Na požádání také poskytujeme pomoc s analýzou a řešením incidentu. V případě zájmu je také možnost zadat ověření webové prezentace dané domény službou Skener webu.

Služba AZB

Rok 2014 znamenal pro informační seriál **Aktuálně z bezpečnosti**, který je uveřejňován na stránkách CSIRT.CZ (www.csirt.cz) velký rozvoj a to jak po stránce kvalitativní tak kvantitativní. Celkově jsme uveřejnili cca **670 novinek**, tzn. cca **56 novinek za měsíc**. Proti předchozím letům 2012 a 2013 se jedná o značný nárůst, v roce 2012 jsme publikovali cca 18 novinek za měsíc, v roce 2013 cca 25 novinek za měsíc.

Zdrojem a inspirací pro AZB se staly nejen komunitou diskutované a mediálně

probírané kauzy, ale také samotný proces řešení bezpečnostních incidentů, kdy jsme řadu kauz z tohoto procesu zpracovali také do krátké zprávy v AZB s cílem co nejrychleji varovat uživatele. V roce 2014 jsme tak v AZB přinesli řadu informací o nových zranitelnostech, pishingových kampaních, podvodných útocích na uživatele, rady v oblasti zabezpečení sítí a služeb atd. Za nejdůležitější aspekt AZB považujeme rychlé šíření informací o aktuálně probíhajících útocích a objevených zranitelnostech. Stránky AZB se staly kvalitním a vyhledávaným zdrojem informací z oblasti bezpečnosti, a to nejen pro administrátory a uživatele, ale také pro média, díky nimž se pak informace o nových útocích mohou rychle rozšířit mezi další potenciální oběti, především uživatele, a předejít tak větším škodám.

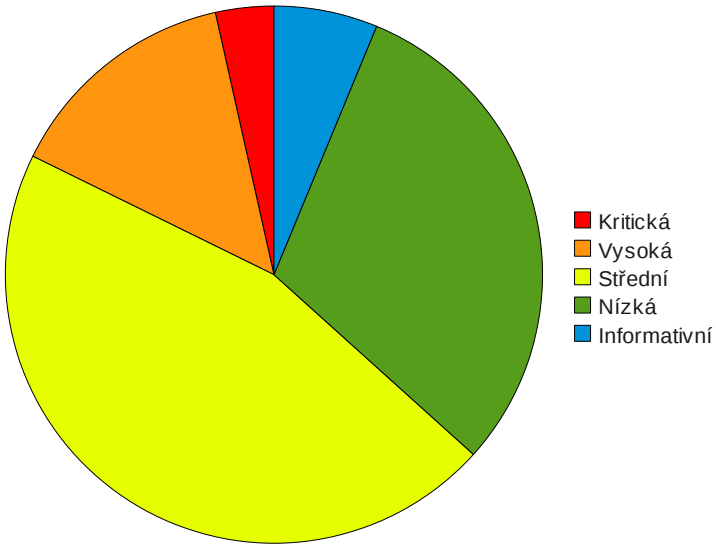
Služba

V polovině roku 2013 jsme spustili novou službu nazvanou **Skener webu,** (https://www.skenerwebu.cz/). Tato služba je určena primárně pro veřejný a neziskový sektor a jejím hlavním úkolem je pomoci provozovatelům webových stránek ověřit jejich bezpečnost, tzn. najít slabá místa (zranitelnosti), chybná nastavení a další nedokonalosti a poradit s jejich nápravou.

Testování webu probíhá v několika fázích – jako první přichází na řadu sada automatizovaných testů a na základě nalezených skutečností řada testů manuálních, kde ke slovu přichází zkušený penetrační tester a jeho zkušenosti a intuice. Po otestování od nás instituce obdrží zprávu, ve které jsou popsány nalezené zranitelnosti, jejich závažnost a tipy na jejich odstranění. Aby se nám podařilo zvýšit bezpečnost webových stránek určených pro české uživatele, poskytujeme službu Skener webu zdarma.

V roce 2013 jsme provedli testování 29 webových prezentací, v roce 2014 jsme jich otestovali 82. Celkově jsme v testovaných webových prezentacích identifikovali cca 1314 problémů různé závažnosti a formulovali cca 1230 doporučení, které se týkaly vylepšení zabezpečení webové aplikace. Až **46** doporučení bylo vydaných na základě **kritického** bezpečnostního nálezu v rámci aplikace a **187** doporučení bylo vydaných na základě nálezu s **vysokých rizikem** zneužitelnosti aplikace. Nejvíc, až **599** nálezů jsme označili **středním rizikem**, pak následují nálezy **informační** v počtu **400** a

nálezy s nízkou mírou zneužití v počtu 82.



Při provádění testů pracujeme kromě jiného také s metodikou neziskové organizace OWASP, která se zaobírá problematikou webové bezpečnosti. V roce 2014 jsme vypracovali české znění oficiálního 22 stránkového dokumentu OWASP Top 10 popisujícího 10 nekritičtějších zranitelností webových aplikací[1].

V rámci poskytování služby jsme několikrát také prezentovali, především pro organizace veřejné správy, důležitost zabezpečení webových aplikaci a výskyt nejčastějších bezpečnostních nedostatků, které získáváme z provozu služby Skener webu. Na stránkách www.csirt.cz jsme dále zveřejnili článek pro administrátory a tvůrce webových prezentací s cílem přiblížit základní pravidla pro zabezpečení webové stránky.

Osvětová činnost

V průběhu roku 2014 jsme uspořádali celkově **pět kurzů** z cyklu školení

1 Dokument je dostupný zde: https://www.owasp.org/images/f/f3/OWASP_Top_10_-_2013_Final_-_Czech_V1.1.pdf

„Počítačová bezpečnost prakticky“, které je určeno především pro **členy bezpečnostních složek České republiky**. Těchto kurzů se zúčastnilo několik desítek zaměstnanců PČR. Spolupráce s bezpečnostními složkami probíhala ale ve více rovinách, např. formou ad-hoc konzultací k probíhajícím útokům a zjištěným hrozbám, zajišťování dat v procesu incident handling, přednáškami na školeních pořádaných v rámci kurzů vzdělávání kriminalistů na Policejní akademii v Praze atd.

V rámci rozvíjení spolupráce s NCBI (Národní centrum bezpečnějšího internetu, http://www.ncbi.cz/) proběhlo bilaterální školení. Tým CSIRT.CZ školil zaměstnance NCBI o základních principech fungování Internetu, e- governance, správě domén, bezpečnostních incidentech, pracovníci NCBI popsali činnost centra, spolupráci s uživateli (převážně mládeží) a nejčastěji řešené problémy. Školení bylo završeno oboustranně užitečnou a obsáhlou diskusí o problematice trendů v oblasti páchání bezpečnostních incidentů, vzdělanosti uživatelů a prevenci.

Spolupráce s NCBI probíhala ještě v dalších oblastech, především formou prezentací a účastí na akcích pořádaných NCBI, např. na Měsíci **kybernetické bezpečnosti (říjen 2014),** na akci **Kulatý stůl Evropského měsíce kybernetické bezpečnosti ČR** a v rámci konferencí pro specialisty a preventisty pracující především s dětmi a mládeží jako např. **„Praha bezpečně online“**.

Cílem této spolupráce a participace na výše uvedených akcích je zlepšení gramotnosti uživatelů v oblasti bezpečného užívání výpočetní techniky a on-line služeb Internetu, zvýšení povědomí uživatelů o práci týmů typu CERT/CSIRT, ale také přenos informací a zkušeností především směrem k pedagogickým pracovníkům. Zdrojem informací pro tyto prezentace jsou jednak osobní zkušenosti, ale také samotný proces IH (řešení bezpečnostních incidentů), který přináší obraz o tom, jaké bezpečnostní incidenty jsou právě aktuální, jakých chyb se uživatelé dopouštějí a proč a jak se jim mohou vyvarovat.

Celkově jsme v oblasti osvěty (školení, prezentování) absolvovali přes 30 akcí - workshopů, konferencí, pracovních skupin atd.

Národní a mezinárodní spolupráce

Národní a mezinárodní spolupráce je nedílnou a povinnou součástí činnosti každého pracoviště typu CERT/CSIRT a důraz na tuto oblast je kladen obzvláště v případě týmů *národních* a *vládních*, které reprezentují danou zemi na příslušných mezinárodních fórech a jsou také prvním logickým kontaktním místem pro získání informací o stavu bezpečnosti ICT dané země.

CSIRT.CZ je od svého vzniku členem platformy TF-CSIRT[2], ve které se sdružují především evropské CERT/CSIRT týmy, ale spolupracuje také s organizacemi FIRST, ENISA a na bilaterální bázi také s dalšími českými i evropskými bezpečnostními týmy. Od roku 2013 jsme členy platformy CECSP (Central European Cyber Security Platform), což je platforma pro úzkou spolupráci národních a vládních týmů v rámci zemí Višegrádské čtyřky a Rakouska. V roce 2014 byla zemí organizující setkání Rakousko.

Na národní úrovni rozvíjíme spolupráci s GovCERT.CZ (Vládním CERT ČR), bezpečnostními CERT/CSIRT týmy konstituovanými v České republice, s bezpečnostními složkami, ale obecně s každým, kdo se zabývá oblastí kyberbezpečnosti. Pro všestrannou podporu této spolupráce organizujeme Pracovní skupinu CSIRT.CZ, účastníme se Pracovní skupiny E-CRIME, spolupracuje s platformami AFCEA, s Bankovní asociací atd.

Pracovní skupina CSIRT.CZ

Pracovní skupina CSIRT.CZ se v roce 2014 setkala pouze jednou a to v červnu. Tématem tohoto setkání byla problematika bezpečnostních incidentů, bezpečnostních událostí, reportování bezpečnostních incidentů a bezpečnostních událostí, sdílení informací tohoto typu, formátu pro jejich výměnu apod. S přednáškou na tato témata vystoupili zástupci dvou akreditovaných bezpečnostním týmů (CESNET-CERTS a CSIRT-MU), dále zástupce, zástupce ČSOB a zástupce GovCERT.CZ (Vládní CERT). Přednášející popsali aktuální stav této oblasti ve svém poli působnosti , proces *incident handling* (IH), s jakými daty týmy v procesu IH pracují, jak probíhá výměna dat mezi bezpečnostními týmy, s jakými zdroji dat (bezpečnostní incident a bezpečnostní událost) týmy pracují, jak tato data hodnotí z hlediska závažnosti, typu, urgence apod., ale také o jakých množstvích dat tohoto typu hovoříme. Jelikož se jedná o téma velmi aktuální jak v mezinárodním kontextu, tak na domácí půdě (z hlediska zákona o

2 https://www.terena.org/activities/tf-csirt/

kybernetické bezpečnosti), byla ustavena menší pracovní skupina sestávající z několika odborníků na toto téma ochotných tuto oblast hlouběji rozpracovat. Tato menší pracovní skupinka se setkala ve druhé polovině roku a diskutovala problematiku sdílení a výměny dat.

Jsme rádi, že zájem o činnost v rámci Pracovní skupiny CSIRT.CZ neutuchá, a že na každém zasedání se vždy sejde cca 60 členů. Zájem o oblast bezpečnosti a činnost CERT/CSIRT infrastruktury a také vznik několika nových CERT/CSIRT týmů v ČR nás vedl k myšlence zorganizovat setkání oficiálně konstituovaných CERT/CSIRT týmů v ČR. Toto první setkání proběhlo formou celodenního workshopu na konci listopadu 2014. Každý CERT/CSIRT tým měl na tomto setkání jednoho až dva zástupce. Setkání bylo velice živé a nastartovalo doufáme úspěšnou spolupráci této bezpečnostní infrastruktury v ČR.

Cvičení (execises)

Rok 2014 byl rokem cvičení (execises). Zúčastnili jsme se čtyř cvičení, přičemž jedno z nich (Cyber Europe 2014) je cvičení 3-fázové, takže celkově jsme absolvovali pět cvičení a u třech z nich jsme se podíleli také na jeho přípravě. V každém cvičení jsme měli trochu jinou roli a personálně jsme jej pojali různě, což nám přineslo mnoho zkušeností a rovnoměrné rozdělení cvičených oblastí mezi členy týmu.

Cyber Europe 2014
Za Českou republiku jsme se zhostili role národního koordinátora při přípravě zatím největšího evropského kybernetického cvičení, které zastřešovala Evropská agentura pro síťovou a informační bezpečnosti (ENISA) – Cyber Europe 2014. Vzhledem ke komplexnosti navržených technických a operačních úloh se cvičení odehrálo ve třech fázích, přičemž první technická fáze, která trvala dva dny, jsme kromě týmu CSIRT.CZ zapojili dalších 7 subjektů z České republiky (CESNET, GovCERT.CZ, NIX.CZ, společnost Unicorn, CSIRT-MU, Active24). Do operační fáze (OLEx) cvičení jsme zapojili ještě v té době čerstvě konstituovaný CSIRT tým společnosti Casablanca.

Cvičení CECSP
V rámci vytvořené platformy CECSP pro spolupráci států Višegrádské čtyřky

a Rakouska jsme se podíleli na přípravě společného cvičení, které odstartovalo další spolupráci vrcholových CSIRT/CERT týmů střední Evropy v oblasti řešení incidentů a budování spolupráce. Cvičení se kromě týmu CSIRT.CZ zúčastnili další zástupci přibližně 11 vrcholových bezpečnostních týmů ze zemí V4 a Rakouska. Vedle operačních úkolů jsme v průběhu cvičení řešili také právní otázky v rámci legislativy jednotlivých zapojených států.

Cvičení NATO CC2014

Jediné cvičení, které jsme absolvovali pouze v pozici hráče (tzn. nepodíleli jsme se na organizaci) bylo cvičení NATO Cyber Coalition 2014, které připravila Severoatlantická aliance (NATO). V rámci cvičení se členové CSIRT.CZ podíleli na vysoce technických úkolech – analýze základní desky a jejího programového vybavení (BIOS apod.). Při tomto cvičení jsme úzce spolupracovali s bezpečnostními experty z Národního centra kybernetické bezpečnosti.

Národní cvičení

Posledním cvičením, kterého jsme se v roce 2014 zúčastnili bylo národní cvičení, které uspořádal Národní bezpečnostní úřad. Cvičení bylo určeno pro správce sítí ze státní správy, přičemž cvičení se v roli odborné poroty zúčastnili také odborníci na legislativu, členové etablovaných bezpečnostních týmů (včetně zástupce CSIRT.CZ), bezpečnostních složek, úřadů státní správy atd. Hráči, správci sítí ze státní správy, řešili v průběhu dne dva zajímavé bezpečnostní problémy, kde jeden měl charakter záplavového útoku na infrastrukturu a druhý ohrožoval koncového uživatele. Hráči si s oběma úkoly poradili velice dobře a celé cvičení ne neslo v duchu živé diskuse a výměny názorů a informací.

Závěr

Rok 2014 zaznamenal velký boom v budování bezpečnostní infrastruktury CERT/CSIRT týmů. Celkově bylo konstituováno sedm nových týmů a další týmy jsou od loňského roku v přípravě. Tento nárůst počtu oficiálně konstituovaných týmů, které získaly status *listed* od úřadu Trusted Introducer (http://www.trusted-introduce.org), ukazuje na velmi dobrou úroveň zajištění bezpečnosti sítí, služeb a uživatelů zde v České republice, zájem o tuto oblast ze strany provozovatelů sítí a služeb a také ochotu zapojit se do infrastruktury a sdílet informace, data a znalosti.

Motivaci pro konstituování oficiálních bezpečnostních týmů CERT/CSIRT v České republice představuje také projekt českého peeringového centra NIX.CZ projekt Fenix (http://fe.nix.cz)[3]. Členství v projektu Fenix je podmíněno řadou technických a organizačních podmínek, které kandidát na členství musí splnit, jednou z podmínek je také CERT/CSIRT tým s přiznaným statusem *listed* od úřadu Trusted Introducer.

V současné době je v České republice oficiálně konstituováno a úřadem Trusted Introducer statusem ***listed*** nebo ***accredited*** označeno celkem 16 týmů typu CERT/CSIRT:

- ✔ 2CCSIRT, status *listed* získán u úřadu TI 15. dne září 2014
- ✔ ACTIVE24-CSIRT, status *listed* získán u úřadu TI dne 9. února 2012
- ✔ CASABLANCA.CZ-CSIRT, status *listed* získán u úřadu TI dne 8. března 2014
- ✔ CDT-CERT, status *listed* získán u úřadu TI dne 16. července 2014
- ✔ **CESNET-CERTS**, status ***accredited*** získán u úřadu TI dne 27. ledna 2008
- ✔ Coolhousing CSIRT, status *listed* získán u úřadu TI dne 17. září 2014
- ✔ **CSIRT-MU**, status ***accredited*** získán u úřadu TI dne 1. února 2011
- ✔ CSIRT-VUT, status *listed* získán u úřadu TI dne 20. května 2014
- ✔ **CSIRT.CZ**, status ***accredited*** získán u úřadu TI dne 13. října 2011
- ✔ CSOB-Group-CSIRT, status *listed* získán u úřadu TI dne 29. října 2014
- ✔ **CZ.NIC-CSIRT**, status ***accredited*** získán u úřadu TI dne 26. srpna 2010
- ✔ DIAL-CERT, status *listed* získán u úřadu TI dne 16. prosince 2013
- ✔ **GOVCERT.CZ**, status ***accredited*** získán u úřadu TI dne 21. srpna 2014
- ✔ O2.cz CERT, status *listed* získán u úřadu TI dne 1. ledna 2014
- ✔ SEBET (ITSELF.CZ-CSIRT), status *listed* získán u úřadu TI dne 25. října 2014
- ✔ SEZNAM.CZ-CSIRT, status *listed* získán u úřadu TI dne 18. října 2013

Další funkční tým typu CSIRT, i když není oficiálně konstituován (tzn. napojen na světovou infrastrukturu v rámci úřadu Trusted Introducer nebo organizace FIRST), je provozován Ministerstvem obrany ČR. Jedná se o vojenský CSIRT tým určený pro spolupráci s obdobnými týmy v rámci členských zemí NATO.

3 Projekt FENIX vznikl na půdě českého peeringového uzlu, sdružení NIX.CZ, v roce 2013 jako reakce na intenzivní DoS útoky, kterým v březnu tohoto roku čelila významná česká média, banky nebo operátoři. Smyslem projektu je umožnit v případě DoS útoku dostupnost internetových služeb v rámci subjektů zapojených do této aktivity.

Opět je nutné zdůraznit, že výše uvedený přehled oficiálně konstituovaných CERT/CSIRT v České republice neznamená, že zde existuje pouze šestnáct výše uvedených bezpečnostních týmů. Ze zkušeností z řešení bezpečnostních incidentů v prostředí týmu CSIRT.CZ a z akcí, které sami pořádáme nebo se jich účastníme, víme, že ačkoliv v rámci komerčních organizací (ISP, banky, poskytovatelé služeb) nejsou konstituovány oficiální CERT/CSIRT týmy, existují zde oddělení a týmy, které se bezpečností sítí a služeb reálně zabývají a roli CERT/CSIRT týmu de facto plní, a to na vysoké odborné úrovni.

Rok 2014 byl velmi náročný, ale také velmi zajímavý a úspěšný. Jsme rádi, že se nám daří kontinuální rozvoj provozovaných služeb a jejich vzájemné provázání a vytěžení ve prospěch uživatelů formou informací na webu týmu (seriál AZB) a v prezentační a osvětové činnosti. Velmi dobře hodnotíme také spolupráci s provozovateli služeb, na které se obracíme se žádostí o spolupráci při řešení bezpečnostních incidentů. Tímto jim za úspěšnou a vstřícnou spolupráci děkujeme. Máme radost také z dalšího rozvoje bezpečnostní infrastruktury v ČR, která v současné době čítá 16 oficiálně konstituovaných týmů a několik dalších týmů ve fázi výstavby. Umístění, pole působnosti, specializace a služby jednotlivých CERT/CSIRT týmů v sítích provozovaných v ČR má velký rozsah a skrývá tak velký potenciál především v oblasti spolupráce a schopnosti ČR čelit bezpečnostním incidentům a hrozbám.