Zpráva o činnosti

CSIRT.CZ

(Národního CSIRT ČR)

za rok 2013

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 2013 v kostce

Začátkem roku 2013 jsme opět věnovali značné množství práce a pozornosti připomínkování a konzultacím při přípravě Zákona o kyberbezpečnosti, jehož vypracováním je vládou České republiky pověřen Národní Bezpečnostní Úřad. Připomínkování Zákona o kyberbezpečnosti bylo věnováno také jedno zasedání *Pracovní skupiny CSIRT.CZ*, které proběhlo na začátku února 2013. Za přítomnosti cca 70ti účastníků byl představen obsah zákona a následovala obsáhlá diskuse o jednotlivých aspektech a dopadech.

V první polovině roku 2013 byl Národním bezpečnostním úřadem iniciován vznik *Central European Cyber Security Platform (CECSP)*, do které se zapojil také tým CSIRT.CZ. Tato platforma sdružuje především národní a vládní CERT/CSIRT týmy ze zemí Višegrádské čtyřky a Rakouska a jejím cílem je intenzivní spolupráce týmů s národním a vládním pole působnosti, výměna zkušeností, informací a know-how. V roce 2013 proběhla pod patronátem NBÚ v Praze dvě setkání – v květnu a prosinci.

V listopadu se tým CSIRT.CZ v roli hráčů zúčastnil mezinárodního cvičení

NATO Cyber Coalition 2013 a pokračoval v přípravách na cvičení Cyber Europe 2014, které zajišťuje organizace ENISA (http://www.enisa.eu).

V oblasti služeb jsme se v roce 2013 věnovali především rozvoji informačního portálu AZB (Aktuálně Z Bezpečnosti) a přípravě nové služby *Skener webu*, zaměřené na analýzu www služeb.

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 NCBI (Národní Centrum Bezpečnějšího Internetu), s lokálními bezpečnostními týmy, které působí v sítích významných ISP, registrátorů, bank, s bezpečnostními složkami, akademickou sférou a pod.

Služby poskytované CSIRT.CZ

Incident handling a incident response

Služba *incident handling* a *incident response* (řešení a koordinace řešení bezpečnostních incidentů) je základní službou, kterou týmy 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.

Za *bezpečnostní incident* označujeme jednu konkrétní událost, která nastala v sítích provozovaných v ČR, a která byla ohlášena CSIRT.CZ, tzn. např.:

- ✔ jedna zveřejněná phishingová stránka
- ✔ jeden stroj se zjevně narušenou bezpečností
- ✔ jeden stroj, který je zdrojem DOS útoku, scanu apod.

Bezpečnostní incident se vždy vztahuje na jednu konkrétní IP adresu, v ojedinělých případech na síť menšího rozsahu, ve které se problém rozšířil na okolní počítače.

Stručná statistika za rok 2013:

- ✔ Počet řešených bezpečnostních incidentů = 495
- ✔ Podle ***koncových stavů incidentů*** (při zavírání kauzy/ticketu jej klasifikujeme, bude podrobněji popsáno níže):

Uzavřeno vyřešeno	180
uzavřeno-jsme informováni	95
uzavřeno-pozitivní změna	187
uzavřeno-upozornění	0
uzavřeno-nevyřešeno	45
uzavřeno-neschopni vyřešit	0

- ✔ Statistika incidentů ***podle jejich typů***:

Phishing	175
IDS	2121
Virus	0
Spam	73
Malware	44
Trojan	12
Other	75
Botnet	15
Probe	26
Portscan	3
DOS	72
Crack	0

Incident typu IDS (druhá řádka ve výše uvedené tabulce „statistika incidentů podle jejich typů“) se do „počtu řešených incidentů = 495“ nezapočítává, protože se jedná o zautomatizovanou službu, kdy jsou správci vyrozumíváni o tom, že jejich síť je zdrojem *události*, která může být zdrojem bezpečnostního incidentu. Číslo 2121 tedy představuje počet varování zaslaných touto službou správcům.

Celkově bylo na adresu pro hlášení bezpečnostních incidentů abuse@csirt.cz zasláno přibližně **1800 zpráv** (e-mailů). Přibližně stejné množství mailů bylo antispamovou ochranou a následně při ruční kontrole označeno za spam. Celkově jsme se tedy v roce 2012 zabývali řešení cca 495 kauz (přijatých cca 1800 mailů tvoří cca 495 kauz, rodíl je dán tím, že občas je incident nahlášen souběžně z více zdrojů). Počet zpráv **odeslaných** v rámci procesu řešení bezpečnostních incidentů bylo cca **2504**.

Při uzavírání nahlášeného bezpečnostního incidentu je tento incident oklasifikován jedním z následujících tzv. ***koncových*** stavů:

Uzavřeno-vyřešeno	Incidenty, které se prokazatelně podařilo vyřešit a odstranit jejich příčinu. *Prokazatelně* znamená např. odstranění phishingové stránky, zastavení útoku, ale především korektní komunikaci ze strany správy sítě zodpovědné za řešení daného bezpečnostního incidentu.
Uzavřeno-jsme informováni	Stížnost na incident, jehož vyřešení nelze zkontrolovat (spam apod.), kde CSIRT.CZ je pouze v kopii a incident je adresován na všechny správné a důležité adresy. Stížnost nepřeposíláme (šlo by o duplikování) a pokud se nevyskytne důvod se daným hlášením blíže zabývat, tak obvykle dále nesledujeme.
Uzavřeno-pozitivní změna	Osoba zodpovědná za IP/síť, která byla původcem incidentu nekomunikuje, ale problém „zmizí“. Od stavu **uzavřeno-vyřešeno** se liší v tom, že nemůžeme vědět, zda byl problém správně vyřešen (např. správce mohl odstranit malware nebo phishingovou stránku, ale zranitelnost serveru stále trvá).

Uzavřeno-upozornění	Stížnost na incident, jehož vyřešení nelze zkontrolovat (ojedinělá stížnost na spam apod.) přišla buď jen nám, nebo i jen některým správcům (a my známe i lepší cílové adresy). Stížnost přepošleme na správné místo, ale dále nesledujeme.
Uzavřeno-nevyřešeno	Přes maximální snahu se incident nepodařilo vyřešit. Osoba zodpovědná za IP adresu/síť, která je původcem incidentu, problém řešit nechce, odmítne, nemyslí si, že to je problém, kterým by se měla zabývat, nebo nereaguje a nepomůže ani eskalace problému na nadřazené autority (správce AS nebo LIR).
Uzavřeno-neschopni vyřešit	Incident se nepodařilo vyřešit, ačkoliv se osoba zodpovědná za danou IP adresu/síť snažila problém řešit a komunikovala. Může k tomu dojít tehdy, když správa dané sítě nemá k dispozici logy z provozu sítě a služeb za dané období, nebo data není schopna spárovat s daty ve stížnosti apod.

Statistiky z procesu incident handling jsou průběžně zveřejňovány na stránkách týmu – http://www.csirt.cz/files/csirt/statistics/stats.html.

Zajímavé kauzy roku 2013

Mezi bezpečnostními incidenty a událostmi, které tým CSIRT.CZ v roce 2013 řešil, a do kterých byl zainteresován, se objevilo několik velice zajímavých a poučných případů:

(D)DoS útoky na www služby provozované v České republice

Bezesporu jednou z nejpoučnější událostí, kterou za dobu své existence tým CSIRT.CZ zažil, byla série březnových (D)DoS útoků na www služby provozované v České republice. Série útoků začala v pondělí 4. března 2013 v dopoledních hodinách, poslední útoky byly zaznamenány ve čtvrtek

7. března odpoledne. Útoky probíhaly obvykle ve dvou vlnách – dopoledne mezi 8-11h a odpoledne mezi 14-16h. Každý den byl útok veden vůči jiné skupině cílových serverů – v **pondělí 4.3.** byly útoky vedeny proti webovým serverům Novinky.cz, iDNES.cz, IHNED.cz, Lidovky.cz, Denik.cz, Csfd.cz, E15.cz, Živě.cz, Mobilmania.cz, v **úterý 5.3.** byly útoky směrovány na služby společnosti Seznam.cz, ve středu 6.3. proti www serverům některých bank (Česká spořitelna, Komerční banka, FIO banka, ČSOB, Reiffeisen banka, Česká národní banka) a ve **čtvrtek 7. 3.** proběhl útok na servery dvou mobilních operátorů Telefónica O2 a T-mobile. V pátek 8. 3. již nebyl pozorován ani hlášen žádný (D)DOS útok takového typu, že by znepřístupnil některý z často navštěvovaných a viditelných webů. Situace se pomalu uklidňovala jak na straně provozovatelů sítí, tak ve světě médií.

Při útocích byly použity mechanismy tzv. SYN Flood v kombinaci s podvrženou adresou (IP spoofing). Další použitá verze útoku spočívala v přidání techniky „odražení“ (reflection). Celý (D)DOS útok pak vypadal tak, že útočící stroje emitovaly velké množství paketů s podvrženou zdrojovou adresou, přičemž jako zdrojová adresa byla použita IP adresa stroje, na který útok ve skutečnosti cílil. Pakety byly poslány na jiné stroje, které ale komunikaci vracely na podvrženou zdrojovou adresu (skutečný cíl útoku).

Správci v napadených sítích svou roli zvládali dobře a řešení dokázali nalézt poměrně rychle, takže nedostupnosti jednotlivých webů byly v řádech jednotek hodin. Jako profesionální hodnotíme přístup ISP, přes které byly napadené weby připojeny. Poskytovali podporu napadeným sítím a byli schopni nasadit efektivní metody ochrany. Jako velmi dobrou považujeme především schopnost a ochotu všech zainteresovaných subjektů komunikovat, sdílet zkušenosti, informace a doporučení. Roli CSIRT.CZ je v této události možno hodnotit jako „místo, kde je možné získat informace“. Od pondělí 4. 3. se na tým CSIRT.CZ obraceli provozovatelé sítí a služeb, na které bylo útočeno, nebo které měly obavu, že budou také cílem útoku, se žádostmi o radu, spolupráci a informace.

Další zajímavé kauzy

Již v červnu roku 2012 jsme řešili incident, při němž byl vybraným uživatelům jednoho českého ministerstva a jedné bankovní instituce odeslán e-mail, v jehož příloze byl Word dokument, jehož spuštění vedlo k instalaci v té době neznámého malware. Tuto informaci jsme obdrželi od CERT-EU a distribuovali jsme ji okamžitě k uvedeným institucím tak, aby mohli podniknout potřebné kroky a své uživatele varovat. V roce 2013 nás tým CERT-EU

ohledně tohoto incidentu opět kontaktoval. Dostalo se nám tak informace, že tento virus, jehož instalaci jsme včasným varováním zabránili, byl nechvalně známý špionážní malware Red October. O jeho existenci byla veřejnost informována až v lednu 2013.

V roce 2013 jsme také navázali na úspěšnou loňskou spolupráci s NCCIC/USCERT Security Operations Center (USCERT SOC) Department of Homeland Security, které nám v průběhu celého roku 2013 zasílal informace o napadených webových stránkách provozovaných v ČR, které jsou zotročeny v Botnetu známém jako Brobot. Brobot je využíván například hacktivistickou skupinou Izz ad-Din al-Qassam Cyber Fighters, a to k útokům především na cíle v USA. Jen v loňském roce se jednalo o více než 2000 URL, na kterých byl umístěn kód tohoto botnetu.

V roce 2013 jsme se také podíleli na šíření informací od CERT.BE, který získal záznamy přístupů na webovou stránku umístěnou na serveru v Belgii. Tato stránka šířila nebezpečný malware, který některé antivirové programy vůbec nedokázaly rozpoznat. Mezi počítači, které tento web navštívily, bylo také několik IP adres z České republiky. Podle informací, které jsme od námi kontaktovaných správců obdrželi, se skutečně tyto počítače při návštěvě tohoto webu nakazily, přičemž jejich uživatelé neměli vůbec tušení, že jejich počítač je infikován.

Začátkem března 2013 jsme se také podíleli na distribuci informací o novém rootkitu[1] pro Linux, který se v systému usadí v podobě knihovny spojené s SSHD, a u kterého nebylo v době jeho objevení jasné, jakým způsobem se do systému dostává. Mezi potenciálně infikovanými servery bylo i několik serverů z ČR.

V dubnu 2013 požádal uživatel z ČR o pomoc při řešení případu nového malware. Ten se šířil prostřednictvím odkazu v programu skype a většina antivirových řešení jej v té době nedokázala identifikovat. Byli jsme požádání o analýzu tohoto malware, aby bylo možné jej odstranit z infikovaných počítačů. Při analýze jsme zjistili, že soubor s malware po spuštění provedl instalaci dalšího malware a došlo také k jeho „uhnízdění“ v systému. Podařilo se nám identifikovat jak server, který byl k šíření tohoto malware použit, tak také jednotlivé soubory, které po jeho instalaci v systému vznikly a také klíče v registru, které se postaraly o jeho spuštění. Návod na odstranění malware jsme pak publikovali na našem blogu a vzorky tohoto nového malware odeslali na další analýzu několika dodavatelům antivirových řešení.

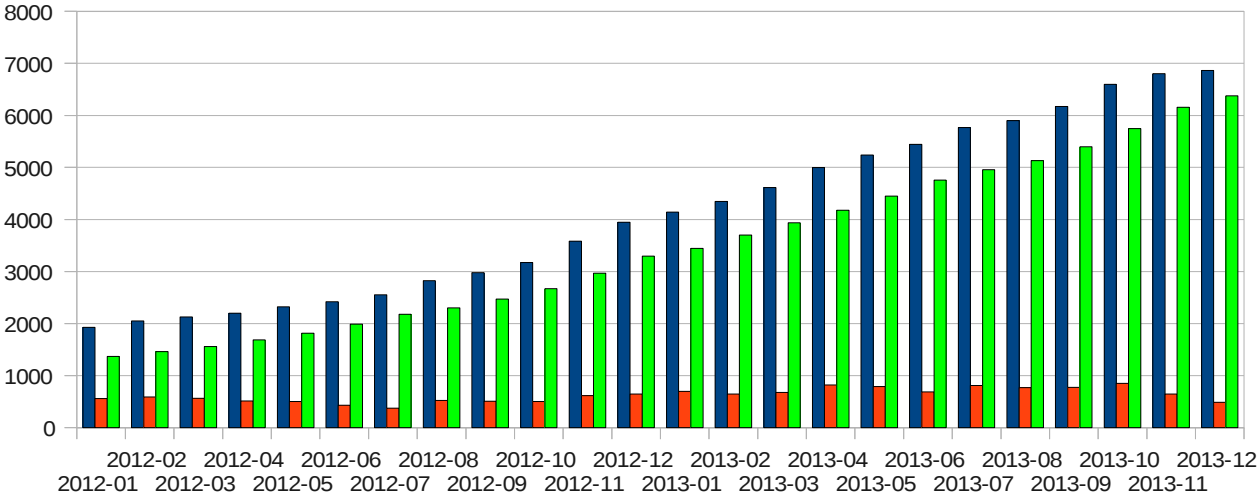
1 Více info je zde: https://isc.sans.edu/forums/diary/SSHD+rootkit+in+the+wild/15229/1

Velice zajímavý incident jsme řešili také v září, kdy se na nás obrátil CERT.SD (Súdánský CERT). Kdosi vstoupil v jejich zemi do e-mailové komunikace mezi Aujan Industry a jejími zákazníky (tzv. útok typu *man-in-the-middle*). Útočník způsobil uživatelům v Súdánu škodu ve výši 174000$. Při tomto útoku byla zneužita česká služba pro posílání anonymních e-mailových zpráv provozovaná serverem soom.cz. Díky našim dřívějším kontaktům a spolupráci s provozovatelem této služby se nám podařilo velmi rychle získat pro Súdánský CSIRT tým požadované informace. Podle zpětné vazby od Súdánského CSIRTu by námi poskytnuté informace mohly pomoci při dopadení pachatelů tohoto trestného činu.

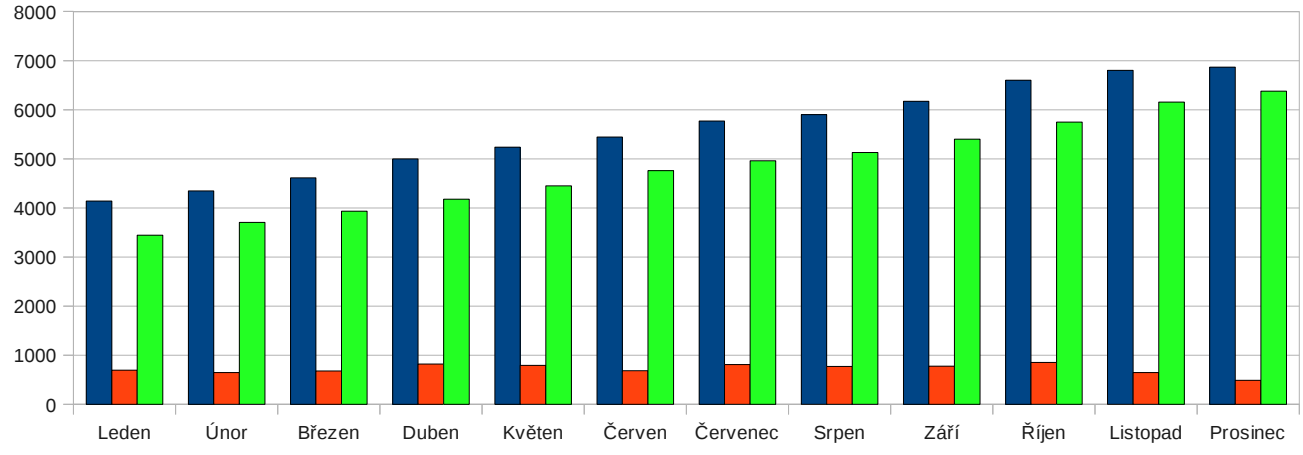
V roce 2013 jsme se také bohužel setkali s prvním případem vydírání, kdy bylo po jednom herním serveru v České republice požadováno „výpalné“ ve výši 500 EUR měsíčně s tím, že dokud nezačne platit, bude na něj pravidelně podnikán DDoS útok.

Služba MDM

Služba MDM využívá veřejně dostupné zdroje informující o doménách, které byly napadeny nějakým druhem malware a pod. 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 od jejího zprovoznění v lednu 2012 do prosince 2013 reflektuje následující graf a tabulka obsahující počty „nakažených“ domén a domén, u kterých se po intervenci podařilo závadný obsah odstranit, a u kterých bohužel přetrvává.



Statistika MDM pouze za rok 2013:



	# evidovaných domén	# škodlivých domén	# čistých domén (z evidovan
Leden	4140	697	3443
Únor	4348	646	3702
Březen	4612	678	3934
Duben	4998	818	4180
Květen	5238	790	4448
Červen	5443	684	4759
Červenec	5767	810	4957
Srpen	5899	769	5130
Září	6173	775	5398
Říjen	6599	852	5747
Listopad	6801	646	6155
Prosinec	6864	486	6378

AZB

V roce 2013 jsme pokračovali v rozvíjení našeho informačního systému **Aktuálně z bezpečnosti**. Během roku v něm bylo publikováno celkem 322 novinek. AZB se postupně vyprofiloval a v současnosti se zaměřuje na tři základní okruhy informací:

1. Informace o nových útocích zaměřených na české uživatele, nebo

s přesahem do ČR (například v případě úniku hesel ze zahraniční služby o tomto informujeme, pokud je tato služba využívána také českými uživateli).
2. Informace o nových zranitelnostech aplikací a to jak uživatelských tak serverových.
3. Informace pro administrátory vztahující se k tzv. hardeningu, tedy návodům na lepší zabezpečení spravovaných serverů a aplikací.

Za nejdůležitější považujeme rychlé šíření informací o aktuálně prováděných útocích. V minulém roce se nám takto podařilo s předstihem informovat například o spamu, jehož cílem bylo sbírat informace o používaných e- mailových adresách. Byl využíván jednoduchý trik, kdy uživatelé obdrželi e- mailovou zprávu, podle které někdo umístil na webové stránky nevhodné fotografie daného uživatele. Odkaz v e-mailu vedl na typo doménu seznann.eu. Každý uživatel obdržel své vlastní konkrétní URL. Domníváme se tedy, že kliknutím na odkaz útočníkovi potvrdil, že se jedná o funkční a používanou e-mail adresu. Naše analýza jiný možný účel nenalezla, server neobsahoval malware, ani žádný jiný nebezpečný materiál. Uživatelům se pouze zobrazila chyba 404.

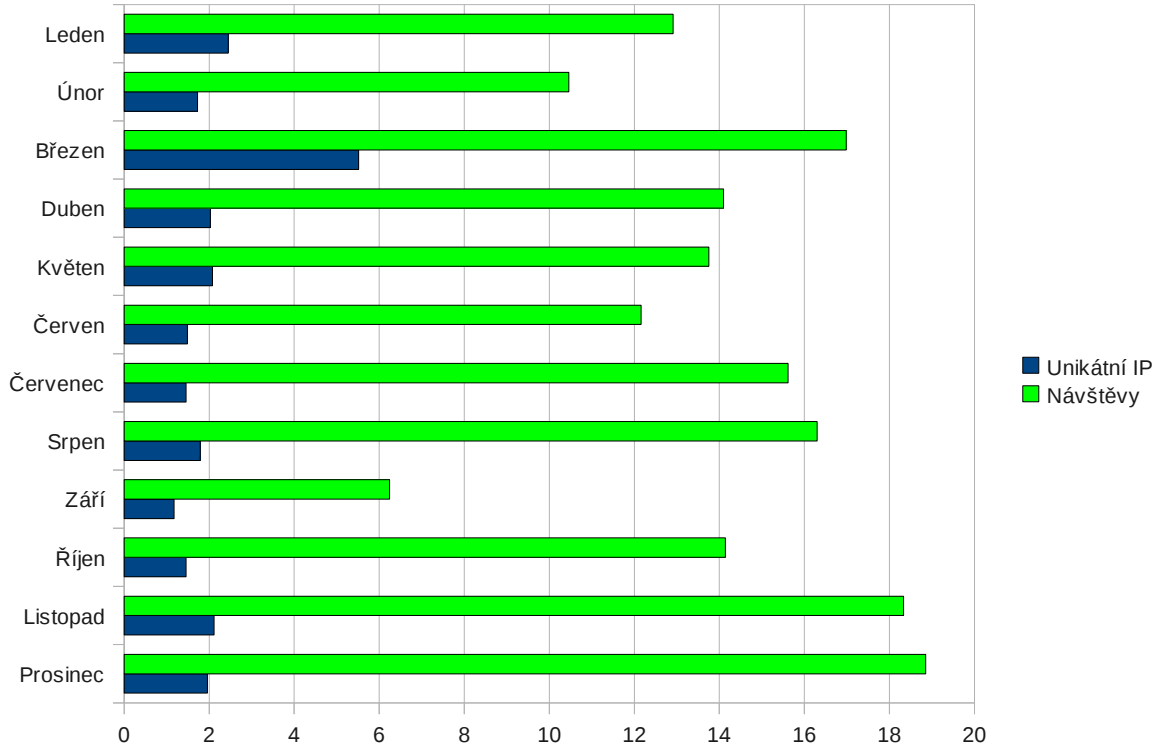
Další informace, kterou jsme přinesli mezi prvními se týkala útoku na uživatele, při kterém byl rozesílán spam, který se tvářil jako MMS zpráva přeposlaná některým z českých mobilních operátorů. Přiložený soubor však místo obrázku obsahoval malware. Velmi rychle jsme také informovali o červnovém phishingovém útoku na klienty některých českých bank.

Z dalších útoků, před kterými jsme v AZB varovali, stojí za zmínku spam předstírající erotickou seznamku, který opět sloužil k ověření, zda jsou konkrétní mailové adresy používány.

V srpnu jsme také jako jedni z prvních zaznamenali výskyt nebezpečného spamu, který se snažil uživatele přesvědčit, že se jedná o zprávu z České pošty. Odkaz ve zprávě vedl k instalaci zcela nového a velmi nebezpečného viru, později nazvaného Win32/Spy.Hesperbot.

Důležité je, že se stránky AZB 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 z našeho AZB rychle rozšířit mezi další potenciální oběti a předejít tak větším škodám. Zájem o informace uveřejněné na webových stránkách ilustruje následující graf a tabulka, které reflektují využití RSS kanálu – uvedená čísla

vyjadřují počet unikátních přístupů do dané sekce webu (čísla jsou v tisících).



	Unikátní IP	Návštěvy
Leden	2,45	12,91
Únor	1,73	10,46
Březen	5,51	16,98
Duben	2,02	14,1
Květen	2,08	13,75
Červen	1,49	12,16
Červenec	1,45	15,62
Srpen	1,79	16,3
Září	1,18	6,25
Říjen	1,46	14,14
Listopad	2,11	18,34
Prosinec	1,96	18,85

Počty uvedené ve sloupcích „Unikátní IP“ a „Návštěvy“ jsou uvedeny v tisících.

Skener webu

V polovině roku 2013 jsme spustili novou službu **Skener webu**, určenou

primárně pro veřejný a neziskový sektor. Cílem této služby je pomoci provozovatelům webových stránek ověřit bezpečnost provozovaných stránek, najít jejich slabá místa (zranitelnosti) a poradit s jejich nápravou. Ke zprovoznění této služby nás vedla zkušenost se službou MDM, která ukazuje na špatný stav některých webových stránek (domén). V mnoha případech se totiž po odstranění malware po určité době nákaza na stránky vrací. Je to dáno tím, že provozovatelé stránek nedokáží najít cestu, kterou k nim útočník pronikl, a která mu umožnila nahrát škodlivý kód, a tak odstraňují pouze projev problému, ale ne příčinu. Aby se nám podařilo zvýšit bezpečnost webových stránek určených pro české uživatele, poskytujeme službu Skener webu zdarma. Po otestování od nás instituce obdrží zprávu, ve které jsou popsány nalezené zranitelnosti, jejich závažnost a tipy na jejich odstranění.

Od spuštění této služby jsme v roce 2013 provedli analýzu celkem 29 webových prezentací, u kterých jsme nalezli mnoho problémů. Nalezené problémy lze podle závažnosti rozdělit do následujících kategorií:

- Informační charakter: 111
- Nízká závažnost: 34
- Střední závažnost: 117
- Vysoká závažnost: 139
- Kritická závažnost: 36

Osvětová činnost

V průběhu roku 2013 jsme uspořádali další dva kurzy z cyklu školení ***„Svět Internetu a domén“***, které je určené především pro členy bezpečnostních složek. Začali jsme také s přípravou dalšího kurzu, který bude zaměřen na podstatu páchání bezpečnostních incidentů, tzn. jakým způsobem dochází k průnikům do systémů apod. Toto školení by mělo pomoci policistům seznámit se s podstatou nejčastějších počítačových útoků a kriminálních činů.

V souvislosti s březnovými (D)DoS útoky vedenými proti www službám provozovaným v České republice, jsme zaznamenali velkou poptávku po prezentacích na toto téma. Celkově jsme prezentací o DDoS útocích zaznamenaných v březnu 2013, obecně o principech útoků typu DDoS, metodách obrany apod. v různých variantách (technická verze zaměřená na principy útoků a možnosti obrany, organizační verze zaměřená na spolupráci a výměnu informací při problému tohoto typu, souhrnná) poskytli okolo

desítky, a to na následujících domácích i zahraničních akcích:

- Setkání AFCEA
- Meeting TF-CSIRT, Bukurešť, Rumunsko
- Konference ITTE 2013, Brno
- Konference Network & Security 2013, Brno
- Konference Network & Security 2013, Bratislava, Slovensko
- 2nd ENISA International Conference on Cyber Crisis Cooperation and Exercises, Athény, Řecko
- Konference v Senátu Parlamentu České republiky, pořádaná Národním Centrem Bezpečnějšího Internetu, Praha
- Školení členů PČR v Holešově
- Octobertfest, Tallin, Estonsko
- Cyber Security Seminar, Bratislava, Slovensko

Spolupráce s NCBI

V roce 2013 jsme rozvíjeli spolupráci s NCBI (Národním Centrem Bezpečného Internetu, http://www.ncbi.cz/) v rámci některých jeho projektů, např. projektem *SaferInternet* nebo projektem *Praha bezpečně online*. Při této spolupráci jsme se aktivně, tzn,. přednáškou, zúčastnili následujících akcí:

- **Měsíc kybernetické bezpečnosti (říjen 2013)**
- **Kulatý stůl Evropského měsíce kybernetické bezpečnosti ČR**
- **Konference „Kraje pro bezpečný Internet“ pořádané v Plzni**
- V rámci projektu **„Praha bezpečně online“** jsme vystoupili na konferenci věnované problematice bezpečnosti a také na školeních zaměřených na členy Policie ČR v rámci policejní prevence rizikových jevů spojených s online komunikací.
- Cyklu seminářů programu **Místní prevence kybernetické kriminality a dalších rizikových jevů** na Praze 6, 7 a 14, kde jsme se podíleli na proškolení několika desítek pedagogů, preventistů a členů bezpečnostních složek.

Cílem této spolupráce a participace na výše uvedených akcích je zlepšení gramotnosti uživatelů v oblasti bezpečného užívání výpočetní techniky a Internetu, zvýšení povědomí uživatelů o práci týmů typu CERT/CSIRT, ale také přenos zkušeností z oblasti bezpečnosti směrem k uživatelům a především k pedagogickým pracovníkům – učitelům, preventistům apod.

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.

Osvěta mezi dospívajícími

Tým CSIRT.CZ si je vědom důležitosti edukačních aktivit a především pak edukace mezi mladými lidmi, kteří jsou často ohroženi těmi nejhoršími formami kybernetické kriminality. Proto jsme se v rámci spolupráce s knižní edicí CZ.NIC podíleli na překladu knihy ***Own Your Space***, která je určena dospívající mládeži, a která pojednává o mnoha rizicích spojených s používáním počítačů a internetu. Kniha se věnuje tématům virů a malware obecně, spamu, hackingu, rizikům on-line nakupování, ochraně soukromí na sociálních sítích avšak nevyhýbá se ani závažnějším tématům, jakými je kyberšikana, phishing, či rizika sexuálního zneužívání dětí na internetu.

Kniha *Own Your Space* vyšla pod českým názvem ***Buď pánem svého prostoru*** a je možné zakoupit buď tištěnou verzi této knihy, nebo si ji na stránkách edice CZ.NIC zdarma stáhnout v elektronické formě.

Národní a mezinárodní spolupráce

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

Výkladový slovník kybernetické bezpečnosti

V roce 2012 jsme se podíleli na tvorbě první verze **Výkladového slovníku kybernetické bezpečnosti** a to ve spolupráci s NBÚ, AFCEA, Policejní akademií ČR, Pracovní skupinou PS05, sdružením CESNET, AOBP, ISACA a ICT Unií. V roce 2013 se v této činnosti pokračovalo a světlo světa spatřilo druhé vydání. Toto druhé vydání, které v omezeném nákladu vyšlo také knižně, obsahuje výklad téměř 700 pojmů z oblasti kyberbezpečnosti. Výklad je pro větší přesnost proveden jak v češtině, tak v angličtině, slovník je tedy

dvojjazyčný. Anglický název je **Cyber Security Glosarry**. Cílem vytvoření výkladového slovníku je sjednotit terminologii v oblasti (kyber) bezpečnosti počítačů a Internetu a dát příslušným pracovníkům (zákonodárcům, zástupcům státní správy, členům bezpečnostních složek, právníkům, členům bezpečnostních týmů) nástroj pro rychlé zorientování se v problematice počítačové terminologie.

Bankovní asociace

Na podzim 2013 jsme se zapojili do nově vniklé platformy pro spolupráci v oblasti bankovního a finančního sektoru. Na jednom ze setkání jsme představili roli, fungování a služby CSIRT.CZ a dohodli možnosti a formu spolupráce a výměny zajímavých informací užitečných pro bankovní sektor (především informace relevantní k provozování www služeb).

Pracovní skupina CSIRT.CZ

Pracovní skupina CSIRT.CZ se v roce 2013 setkala dvakrát – v únoru a v prosinci. Únorové setkání bylo opět věnováno především zákonu o kybernetické bezpečnosti, který vypracoval Národní Bezpečnostní Úřad. Prosincové setkání bylo zaměřeno technicky a věnovalo se bezpečnosti na úrovni ISP a diskutovaly se následující oblasti:

- ochrana vlastní infrastruktury z pohledu ISP;
- možnosti ochrany připojených subjektů (sítí) a provozovaných služeb;
- připravenost a aplikaci mechanismů obrany v případě vzniklého problému (útoku);
- ochrana proti DDoS útokům;
- bezpečnost ve vztahu k uživatelům apod.

Spolupráce s ENISA

V rámci spolupráce s organizací ENISA se dlouhodobě účastníme pracovní skupiny zabývající se organizací cvičení (exercises), které mají za cíl ověřit připravenost bezpečnostní infrastruktury na vážné ohrožení (útok) sítí a služeb a schopnost spolupráce napříč organizacemi – CERT/CSIRT týmy, bezpečnostními složkami, krizovými štáby, vládou jednotlivých zemí a pod.

V roce 2013 ENISA cvičení nepořádala a soustředila se na přípravu cvičení **Cyber Europe 2014**, které proběhne v roce 2014 a bude mít tři fáze. Této přípravy se aktivně účastníme, v roce 2013 tato příprava obnášela 4 setkání, na kterých se probíraly cíle cvičení, průběh, technické aspekty a především scénář. Vzhledem k různorodosti členských státu je snahou vytvořit takový scénář, který by byl aplikovatelný na všechny členské státy EU a který by dokázal adekvátně připravit CSIRT týmy na reálnou situaci. Proto bylo rozhodnuto pokrýt všechny fáze potencionální krize v návaznosti na její možnou eskalaci, což vyústilo ve 3-fázové cvičení – **technické**, **operační** a **politické (strategické)**. Vzhledem k tomu, že příprava a průběh cvičení budou závislé na nově vytvořené platformě, podíleli jsme se na jejím testování. V prosinci už začala ostrá příprava na cvičení – rozhodnutí o zapojení do jednotlivých fází cvičení a úrovně dle náročnosti, výběr a oslovení vhodných hráčů, plán setkání a edukace apod.

Cvičení Cyber Coalition 2013

Ve spolupráci s NBÚ jsme se v listopadu 2013 opět v roli „hráče“ zúčastnili cvičení NATO Cyber Coalition 2013. V rámci naší role jsme plnili řadu úkolů technického charakteru, spolupracovali jsme s dalšími hráči, vyměňovali si informace a zajišťovali komunikaci s médii.

Závěr

V roce 2013 byly v České republice konstituovány čtyři nové bezpečnostní týmy typu CERT/CSIRT. Tři z nich mají pole působnosti v komerčním sektoru – Seznam.CZ, Dial Telecom, Telefónica Česká republika (O2), čtvrtým týmem je GovCERT.CZ, Vládní CERT ČR provozovaný NBÚ. Tým CSIRT.CZ pomáhal společnostem, které jej o to požádali s ustanovením CSIRT týmu a s jeho uvedením do seznamu řádných členů úřadu Trusted Introducer (http://www.trusted-introduce.org).

V současné době je tak v České republice oficiálně úřadem Trusted Introducer konstituováno celkem devět týmů typu CERT/CSIRT:

- ✔ **CESNET-CERTS**, bezpečnostní tým provozovaný sdružením CESNET pro dohled nad sítí národního výzkumu a vzdělávání CESNET2
- ✔ **CSIRT-MU**, bezpečnostní tým provozovaný Masarykovou univerzitou v Brně

- ✔ **CZ.NIC-CSIRT**, bezpečnostní tým provozovaný sdružení CZ.NIC pro dohled nad sítí sdružení CZ.NIC a českou národní doménou (.cz)
- ✔ **CSIRT.CZ**, Národní CSIRT ČR, provozovaný na základě Memoranda mezi Národním bezpečnostním úřadem a sdružením CZ.NIC
- ✔ **Active24-CSIRT**, bezpečnostní tým provozovaný společností Active24
- ✔ **GovCERT.cz**, Vládní CERT České republiky, provozovaný Národním bezpečnostním úřadem
- ✔ **Seznam.cz-CSIRT**, CSIRT provozovaný společností Seznam.cz
- ✔ **DIAL-CERT**, CSIRT tým provozovaný společností Dial Telecomem
- ✔ **O2.cz CERT**, CSIRT tým provozovaný společností Telefónica ČR

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.

Opět je nutné zdůraznit, že výše uvedený přehled oficiálně konstituovaných CERT/CSIRT v ČR neznamená, že zde existují pouze výše uvedené bezpečnostní týmy. Ze zkušeností z řešení bezpečnostních incidentů v prostředí týmu CSIRT.CZ víme, že ačkoliv v rámci komerčních organizací (ISP, banky, poskytovatelé služeb) v České republice nejsou ustaveny 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. Dalším důkazem toho, že v prostředí významných sítí a poskytovatelů služeb v ČR působí řada odborně zdatných specialistů na počítačovou a síťovou bezpečnost, je vidět také na diskusích při setkáních *Pracovní skupiny CSIRT.CZ* a také při setkáních odborné veřejnosti při připomínkování věcného záměru zákona o kyberbezpečnosti a Návrhu zákona o kybernetické bezpečnosti.

Celkově hodnotíme rok 2013 jako zajímavý a úspěšný – v rámci procesu IH jsme zaznamenali řadu úspěchů v oblasti prevence a varování uživatelů, kvalitní a plodnou spolupráci s bezpečnostními složkami ČR, zahraničními týmy i dalšími platformami, které se zabývají bezpečností. Zprovoznili jsme novou zajímavou službu Skener webu pro uživatele Internetu v ČR a v nově konstituovaných CSIRT týmech jsme získali řadu nových partnerů pro spolupráci.