Zpráva o činnosti

CSIRT.CZ

(Národního CSIRT ČR)

za rok 2012

Vypracoval:

Dne: 27. února 2013

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 o provozování Národního CSIRT ČR 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 2012 obecně

V roce 2012 jsme se soustředili na stabilizaci a rozvoj klíčových služeb provozovaných týmem CSIRT.CZ – *incident handling* a *incident response* (tzn. příjem, řešení a koordinaci řešení bezpečnostních incidentů majících původ nebo ohrožující počítačové sítě a služby provozované v ČR), pokračování ve spolupráci na národní a mezinárodní úrovni a na osvětovou činnost tak, aby byla nadále naplňována a rozvíjena role a plněny následující cíle týmu CSIRT.CZ:

- ✔ Plnit roli PoC (Point of Contact), tzn. zajišťovat jednoduchý a důvěryhodný kontakt pro Českou republiku
- ✔ Udržovat a rozvíjet zahraniční vztahy – se světovou komunitou CERT/CSIRT týmů a organizacemi, které tuto komunitu podporují (ENISA, TERENA, FIRST).
- ✔ Spolupracovat se subjekty v rámci České republiky – ISP, poskytovateli služeb a obsahu, bankami, bezpečnostními složkami, akademickým sektorem, úřady státní správy, samosprávy a dalšími institucemi, spolupráce mimo jiné v rámci *Pracovní skupiny CSIRT.CZ.*

Na poli národní spolupráce se v roce 2012 pro CSIRT.CZ (CZ.NIC) stal důležitým partnerem Národní bezpečnostní úřad (dále jen NBÚ). Začátek roku 2012 jsme v rámci této spolupráce věnovali značné množství práce a pozornosti připomínkování a konzultacím věcného záměru zákona o kyberbezpečnosti, který Národní Bezpečnostní Úřad začal připravovat bezprostředně po svém jmenování gestorem za oblast kyberbezpečnosti v listopadu 2011. Věcnému záměru zákona o kyberbezpečnosti a jeho návrhu byl věnován prostor také na obou setkáních *Pracovní skupiny CSIRT.CZ* uskutečněných v roce 2012.

V oblasti služeb jsme se v roce 2012 věnovali především rozvoji tzv. proaktivních služeb, které v aktuální podobě čerpají informace o bezpečnostních incidentech týkajících se sítí provozovaných v České republice od spolupracujícího partnera, kterým je sdružení CESNET a z veřejně dostupných zdrojů. Jedná se o služby IDS.CZ a MDM, o kterých bude řeč dále.

V oblasti osvěty, národní a mezinárodní spolupráce jsme pokračovali v udržování již navázané spolupráce (Pracovní skupina CSIRT.CZ, Pracovní skupina E-CRIME, organizace ENISA a TERENA) a v navazování nových vazeb – např. s NCBI (Národní Centrum Bezpečnějšího Internetu), CERT-RO (Národní CERT Rumunska) a s lokálními bezpečnostními týmy, které působí v sítích významných ISP, registrátorů, bank a pod (např. v roce 2012 nově konstituovaný bezpečnostní tým Active24-CSIRT).

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
- ✔ zavirovaný stroj (síť), který je zdrojem spamu
- ✔ 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 2012:

- ✔ Počet řešených bezpečnostních incidentů = 330
- ✔ Podle ***koncových stavů incidentů*** (při zavírání kauzy/ticketu jej klasifikujeme, bude podrobněji popsáno níže):

Uzavřeno vyřešeno	161
uzavřeno-jsme informováni	32
uzavřeno-pozitivní změna	130
uzavřeno-upozornění	0
uzavřeno-nevyřešeno	7
uzavřeno-neschopni vyřešit	0

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

Phishing	159
IDS	3924
Virus	1
Spam	43

Malware	19
Trojan	5
Other	13
Botnet	8
Probe	12
Portscan	1
DOS	68
Crack	0
Copyright	1

Celkově bylo na adresu pro hlášení bezpečnostních incidentů abuse@csirt.cz zasláno přibližně **7260 zpráv** (e-mailů). Z toho bylo automaticky antispamovou ochranou vyřazeno cca 6344 zpráv, dalších 54 zpráv bylo coby spam vyřazeno ručně členem týmu při procesu *incident handling*. Celkově jsme se tedy v roce 2012 zabývali obsahem cca **859 zpráv** – hlášení bezpečnostních incidentů. Tyto zprávy nakonec dávají oněch výše zmiňovaných 330 hlášených a řešených bezpečnostních incidentů, které tým CSIRT.CZ v roce 2012 řešil. Rozdíl mezi čísly označujícími *počet přijatých hlášení* (859) a *počet řešených incidentů* (330) je dán tím, že občas je incident nahlášen souběžně z více zdrojů (více cílů, eskalační procedura). Počet zpráv **odeslaných** v rámci procesu řešení bezpečnostních incidentů bylo cca 1200.

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, s CSIRT.CZ 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 Autonomního systému nebo LIR) apod.
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. Tento stav byl zaveden teprve na přelomu let 2009 a 2010.

Statistiky z procesu incident handling týmu CSIRT.CZ jsou průběžně zveřejňovány na stránkách týmu:

http://www.csirt.cz/files/csirt/statistics/stats.html.

V roce 2012 jsme část procesu řešení bezpečnostních incidentů (polo)automatizovali. Jsou to incidenty, které jsou ve zveřejněných statistikách uvedeny v kategorii IDS. Hlášení o podezření z výskytu bezpečnostního incidentu chodí ze systému IDS.CZ rovnou do rukou správce dané koncové sítě, s možností obrátit se na CSIRT.CZ pro získání dalších doplňujících informací, nebo pro konzultaci.

Zajímavé kauzy z procesu incident handling

Mezi bezpečnostními incidenty ohlášenými týmu CSIRT.CZ se v roce 2012 objevilo několik velice zajímavých případů.

Na začátku ledna 2012 byl tým CSIRT.CZ požádán týmem CERT-EU o spolupráci při řešení incidentu, při kterém došlo k úspěšnému útoku na webové stránky kanceláře velkých průmyslových rizik společného výzkumného centra EU. Při tomto útoku došlo k úniku citlivých informací (uživatelských jmen a hesel) a k jejich zveřejnění na serveru Pastebin. Tým CSIRT.CZ dohledal příslušné kontakty na uživatele v ČR, jejichž e-mailové účty byly tímto způsobem kompromitovány a všem těmto uživatelům rozeslal jak informaci o kompromitaci jejich e-mailových účtů, tak také informace ohledně dalšího vhodného postupu při nápravě této situace tak, aby bylo předejito dalším škodám.

Další větší incident byl dubnový útok na Eurobank EFG Bulgaria, na kterém se podílelo přibližně 40 IP adres z České republiky. Všem držitelům daných IP adres byla zaslána informace o zneužití jejich IP adres (zařízení na nich provozovaných).

V červnu 2012 bylo zneužito více jak 170 DNS serverů v ČR k útoku na cíle v Lotyšsku. Při tomto útoku bylo využito již delší dobu známého útoku *DNS Amplification attack*. Během řešení incidentu tým CSIRT.CZ zjistil, že část ze zneužitých zařízení byla ze segmentu SOHO, konkrétně se jednalo o výrobky společnosti Mikrotik. CSIRT.CZ provedl vlastní testování software RouterOS

pro zařízení Mikrotik. Z výsledků těchto testů vyplynulo, že DNS server v těchto zařízeních je dostupný na všech jeho portech a přístup k němu je potřeba řídit pomocí integrovaného firewallu. Toto je podstatný rozdíl od běžných routerů určených pro domácnosti a malé firmy. CSIRT.CZ okamžitě po tomto zjištění celou věc konzultoval se společností Mikrotik a následně pak vydal pro uživatele těchto zařízení varování před rizikovou konfigurací operačního systému RouterOS.

V říjnu 2012 proběhl Phishingový útok na zákazníky ČSOB. Tým CSIRT.CZ byl požádán o pomoc přímo zákaznickým centrem ČSOB a získal od nich potřebná data k analýze. Po analýze zaslaných phishingových zpráv bylo osloveno cca 40 držitelů IP adres zneužitých k hostování phishingové stránky, nebo k rozesílání phishingových e-mailů. Všechny phishingové stránky byly postupně zablokovány a odstraněny.

V říjnu 2012 NCCIC/US-CERT Security Operations Center (US-CERT SOC) Department of Homeland Security požádal tým CSIRT.CZ o pomoc při eliminaci části DDOS útoku na cíle v USA. Část provozu pocházela z ČR. Jednalo se o zneužití hacknutých webových stránek, respektive CMS systémů joomla a wordpress.

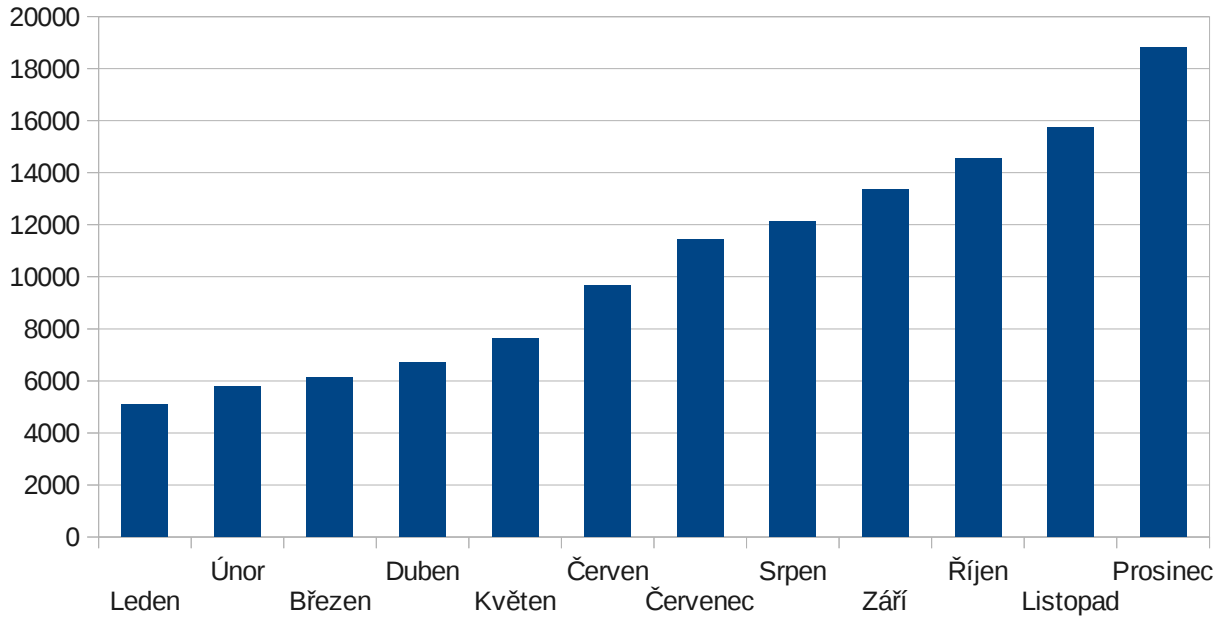
V roce 2012 se CSIRT.CZ opět účastnil některých preventivních akcí. Například v květnu 2012 proběhla preventivní akce ve spolupráci s týmem Siemens ProductCERT. Jednalo se o distribuci informací a doporučení držitelům IP adres, na nichž se nacházely z internetu volně dostupná zařízení spadající do kategorie průmyslové řídící systémy (ICS). Podmnožinou systémů ICS jsou také v poslední době často zmiňované systémy SCADA.

Další akce, zaměřená na ICS, proběhla v prosinci, kdy byli ve spoluprácí s ICS-CERT osloveni držitelé (uživatelé) 1193 unikátních IP adres.

Proaktivní služby v oblasti bezpečnosti

V roce 2012 jsme nasadili do rutinního provozu službu **MDM** (**M**alicious **D**omain **M**anager). Tato služba 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 této služby

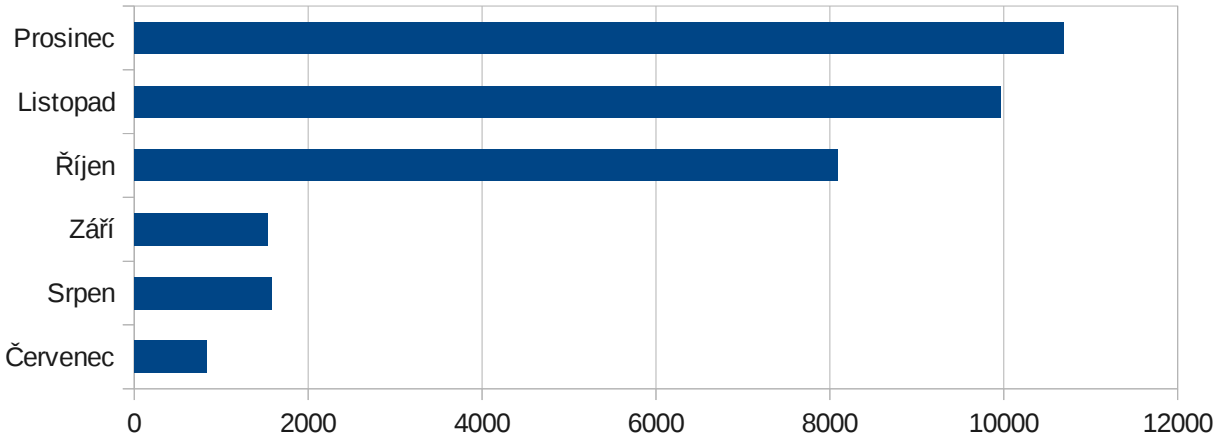
reflektuje následující obrázek:



Leden	Únor	Březen	Duben	Květen	Červen	Červenec	Srpen	Září	Říjen	Listopad	Prosinec
5086	5776	6130	6728	7612	9652	11451	12135	13354	14552	15751	18801

Aktuality z bezpečnosti

V roce 2012 jsme věnovali péči také rozvoji týmového webu. Webové stránky www.csirt.cz jsme obohatili o sekci „Aktuálně z bezpečnosti“, kde cílem je informovat uživatele o nejnovějších objevených bezpečnostních hrozbách, zranitelnostech a trendech v oblasti počítačové bezpečnosti se zaměřením na praktické informace (např. jaký typ ochrany nebo aktualizace aplikovat). V rámci snadnějšího a rychlejšího šíření nových informací jsme pro sekci „obecné novinky“ a „aktuálně z bezpečnosti“ zavedli RSS kanál, který uživatele informuje o změnách na těchto stránkách provedených. Zájem o informace uveřejněné na webových stránkách ilustruje následující graf využití RSS kanálu.



Červenec	Srpen	Září	Říjen	Listopad	Prosinec
830	1585	1539	8092	9964	10694

Osvětová činnost

V průběhu roku 2012 jsme uspořádali celkově osm kurzů z cyklu školení ***„Svět Internetu a domén“***, které je primárně určeno zaměstnancům státní správy a členům bezpečnostních složek ČR. Školení je koncipováno jako základní exkurs do problematiky internetu jako takového a jeho fungování. Speciální pozornost je věnována praktickým záležitostem z oblasti počítačové bezpečnosti, které by měly pomoci (zejména) vyšetřovatelům Policie ČR orientovat se v problematice základních typů počítačové kriminality a naučit je obracet se přímo na konkrétní subjekty, které mohou pomoci při jejich práci. Součástí kurzu je i právní hledisko, vysvětleno je postavení sdružení CZ.NIC a Národního CSIRT ČR, možnosti poškozených jak řešit jednotlivé případy i jinak než trestním oznámením atd.

V rámci školení jsou nejprve poskytnuty základní informace o tématech uvedených výše. Jednotlivá dílčí témata jsou dále rozvíjena v diskusi a na konkrétních případech. Základní osnova kurzu je:

- ✔ Základní principy fungování internetu a jeho správa
- ✔ K čemu jsou domény a jak fungují (DNS, IP adresy, hierarchie), principy registrace, zainteresované subjekty
- ✔ Kde lze co najít, jak údaje dohledat, koho o údaje požádat

- ✔ Kdo je za co odpovědný (doména, IP adresa)
- ✔ Počítačová kriminalita: typy a formy, civilní, správní a trestněprávní úprava, odpovědnost
- ✔ Doménová jména: spory a možnosti jejich řešení
- ✔ Počítačová bezpečnost: CSIRT týmy a jejich struktura
- ✔ Popis útoků – jak jednotlivé typy útoků probíhají, co je obvykle dotčeno, co je potřeba ošetřit apod.

V průběhu roku 2012 doznalo toto školení řadu změn po stránce obsahové i programové. Účastníkům kurzu je umožněno, aby předem definovali oblast zájmu z nabízených témat, takže je možné kurz zaměřit konkrétněji a jít v dané oblasti do větších detailů, nechat větší prostor na diskusi, příklady a pod.

V roce 2012 jsme navázali úspěšnou spolupráci s NCBI (Národním Centrem Bezpečného Internetu, http://www.ncbi.cz/) v rámci některých jeho projektů, např. projektem *SaferInternet* nebo *Praha bezpečně online*. V rámci této spolupráce jsme se zúčastnili následujících akcí:

- **Kulatý stůl Evropského měsíce kybernetické bezpečnosti ČR**. Tato akce se konala 26. října 2012 a měla za cíl setkání českých horkých linek a bezpečnostních týmů pro koordinaci řešení bezpečnostních incidentů v počítačových sítích (CSIRT) provozovaných v České republice. Hlavním cílem kulatého stolu je zvýšit vzájemnou informovanost organizací a společností, které se věnují vzdělávání v oblasti internetové gramotnosti a bezpečnějšího užívání internetu, prevenci online kriminality a sociálně patologických jevů na internetu nebo provozují horké linky zaměřené na řešení problémů souvisejících s řešením internetových hrozeb.
- 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.

Národní a mezinárodní spolupráce

Národní a mezinárodní spolupráce je nedílnou součástí činnosti každého

pracoviště typu CERTS/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.

CSIRT-RO

Na žádost organizace ENISA se na začátku června 2012 uskutečnilo v prostorách sdružení CZ.NIC v Praze setkání týmů CSIRT.CZ a CERT-RO (Národní CERT tým Rumunska). Cílem tohoto setkání bylo předat týmu CERT-RO maximum zkušeností z procesu budování týmu CSIRT.CZ a jeho ukotvení v roli Národního CSIRT týmu České republiky a pomoci tak CERT- RO na jeho cestě k plné operabilitě v roli Národního týmu Rumunska. Základním cíle setkání bylo osobní poznání členů obou týmů, výměna zkušeností a informací o jejich fungování, a to jak z oblasti technologické a organizační, tak co se týče spolupráce, komunikace a budování důvěry v rámci definovaného pole působnosti týmů v obou domovských zemích.

TERENA a TRANSITS II

Na jaře 2012 se sdružení CZ.NIC organizačně podílelo na uspořádání školení TRANSITS II, což je školení organizované sdružením TERENA (www.terena.org). Školení proběhlo v prostorách sdružení CZ.NIC za finanční účasti CZ.NIC a TERENA. Školení je určeno členům bezpečnostních týmů CERT/CSIRT týmů a klade si za cíl seznámit účastníky důkladněji s oblastí sledování provozu sítě, základy forenzní analýzy a jejich technik, a také na oblast komunikace a spolupráce při řešení bezpečnostních incidentů.

Výkladový slovník kybernetické bezpečnosti

V roce 2012 jsme se podíleli na tvorbě Výkladového slovníku kybernetické bezpečnosti a to spolu s NBÚ, AFCEA, Policejní akademií ČR, Pracovní skupinou PS05, CESNET, AOBP, ISACA a ICT Unií. 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.

Bezpečnostní složky

Spolupráce s BIS (Bezpečnostní informační službou) pokračovala úspěšně i v roce 2012 a to především v oblasti výměny informací o aktuálních a řešených bezpečnostních incidentech, ale také v oblasti výměny know-how. Ve spolupráci se sdružením CESNET byl uspořádán celodenní workshop, kde všechny tři zúčastněné subjekty souhrnně a stručně poreferovaly o své aktuální činnosti, rolích a cílech a navzájem se informovaly o novinkách v oblasti bezpečnosti – probíranými tématy byly především sledování provozu sítí a služeb, možnosti forenzní analýzy, spolupráce CERT a bezpečnostních složek v praxi a pod.

Pracovní skupina CSIRT.CZ

Pracovní skupina CSIRT.CZ se v roce 2012 setkala dvakrát – v dubnu a v prosinci. Obě tato setkání byla věnována především připravovanému zákonu o kybernetické bezpečnosti. Jak NBÚ (Vládní CERT), tak CSIRT.CZ ale také poreferovali o své činnosti v uplynulém období, plánech na rok 2013 a vzájemné spolupráci při rozvoji dvou vrcholových týmů – národního a vládního CERT/CSIRT.

Spolupráce s ENISA

V rámci této spolupráce 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. A samozřejmě se také cvičení aktivně a každoročně účastníme – v roce 2012 jsme se zúčastnili cvičení Cyber Europe 2012, o kterém jsme podrobně referovali jak na našich webových stránkách, tak prostřednictvím odborných on-line periodik (root.cz).

V roce 2012 jsme dále pokračovali v účasti v expertní pracovní skupině zabývající se spoluprací mezi světem orgánů činných v trestním řízení a světem CERT/CSIRT týmů v oblasti boje proti kyberkriminalitě (expertní skupina ***„Cooperation between CERTs and Law Enforcement Agencies to fight against cybercrime“***). Výsledkem práce této expertní skupiny jsou průběžně vydávané dokumenty mapující zkušenosti získané od existujících

týmů na obou stranách (LEA a CERT/CSIRT), sada doporučení a především podklad pro další práci. Dokumenty jsou průběžně zveřejňovány na stránkách ENISA (http://www.enisa.eu).

Cvičení CE2012 a CC2012

Cvičení ***Cyber Europe 2012*** uspořádaly členské státy Evropské unie a země Evropského sdružení volného obchodu (EVSO). Koordinátorem cvičení Cyber Europe 2012 byla organizace ENISA (Evropská agentura pro bezpečnost sítí a informací) za podpory Společného výzkumného centra Evropské komise. Cvičení sledovalo tři základní cíle:

1. vyzkoušet účinnost a pružnost stávajících mechanismů, postupů a výměnu informací nezbytných pro spolupráci veřejných úřadů v Evropě;
2. přezkoumat možnosti spolupráci mezi veřejnými a soukromými subjekty v Evropě;
3. odhalit trhliny a možnosti v oblasti zvyšování účinnosti zvládání rozsáhlých kybernetických incidentů v Evropě.

Cvičení Cyber Europe 2012 předcházela dlouhá a intenzivní rok trvající příprava za úzké spolupráce všech zúčastněných zemí. Každá zúčastněná země musela na počátku obsadit roli tzv. *Národního Moderátora*, který se podílel na přípravě cvičení na národní i mezinárodní úrovni, tzn. získal hráče v dané zemi, specifikoval jejich roli, seznámil je s pravidly, přibližným scénářem cvičení, podílel se na přípravě scénáře a datového zázemí pro cvičení, ale především definoval, čeho chce daná země svou účastní dosáhnout, co chce testovat. Za Českou republiku plnil roli Národního Moderátora tým CSIRT.CZ, který se rozhodl soustředit na cíl „otestovat spolupráci veřejného a privátního sektoru při plošném útoku na IT infrastrukturu“. Proto se kromě pracoviště CSIRT.CZ do cvičení na žádost CSIRT.CZ zapojilo sdružení **CESNET**, registrátor **Active24** a **Policejní akademie**. Česká republika tak měla do hry zapojeny celkově čtyři hráče – dva reprezentující privátní sektor (CESNET a Active24) a dva reprezentující veřejný sektor (CSIRT.CZ a Policejní akademie).

Na žádost NBÚ jsme se v listopadu 2012 zúčastnili také cvičení NATO Cyber Coalition 2012, kde jsme dostali roli „hráče“, což obnášelo plnění dílčích úkolů v rámci daného národního scénáře.

Závěr

V roce 2012 byl v České republice konstituován první oficiální CSIRT v komerčním sektoru – tým Active24-CSIRT provozovaný jedním z nejvýznamnějších doménových registrátorů, společností Active24 (http://www.active24.cz).

V současné době je tak v České republice oficiálně úřadem Trusted Introducer (http://www.trusted-introducer.org) konstituováno celkem pět 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 České republiky, provozovaný na základě Memoranda podepsaného mezi Ministerstvem vnitra ČR a sdružením CZ.NIC
- ✔ **Active24-CSIRT**, bezpečnostní tým provozovaný společností Active24

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 také 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 existuje pouze 5 (6) bezpečnostních týmů. Zkušenosti 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 vysoce 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, které organizuje Národní Bezpečnostní Úřad při plnění své role gestora za oblast kyberbezpečnosti.

Celkově hodnotíme rok 2012 jako úspěšný – zprovoznili jsme nové zajímavé služby pro uživatele Internetu v ČR, získali jsme řadu nových partnerů pro spolupráci a doufáme, že po letech váhání se blíží doba, kdy v budovaném Vládním CERTu budeme mít kvalitního partnera pro další rozvoj bezpečnostní infrastruktury v České republice.