Audit činnosti CSIRT.CZ (Národního CSIRT ČR)

za rok 2011

Vypracoval: CZ.NIC, z.s.p.o.

Dne: 12. ledna 2012

Úvod

Pracoviště CSIRT.CZ bylo v polovině prosince roku 2010 Ministerstvem vnitra prohlášeno za Národní CSIRT České republiky a za jeho provozovatele určilo sdružení CZ.NIC, správce české národní domény. Stalo se tak podpisem Memoranda mezi MV ČR a sdružením CZ.NIC. Pracoviště CSIRT.CZ bylo vybudováno a v letech 2008 – 2010 provozováno sdružením CESNET, z.s.p.o. v rámci plnění grantu ***Kybernetické hrozby z hlediska bezpečnostních zájmů České republiky (VD20072010B13)****, který v letech 2007-2010 financovalo Ministerstvo vnitra ČR.*

Rok 2011 obecně

V první polovině roku 2011 jsme se soustředili na zajištění tří klíčových oblastí fungování CSIRT.CZ:

1. **Udržení kontinuity provozu** pracoviště CSIRT.CZ.
2. **Převod technologického zázemí a agendy** pracoviště od sdružení CESNET.
3. **Informování národních i mezinárodních struktur o změně** mandátu týmu CSIRT.CZ a jeho převod k novému provozovateli.

1: **Udržení kontinuity provozu** se povedlo provést bezvýpadkově díky zaměstnancům sdružení CZ.NIC, kteří již měli zkušenosti se zakládáním, organizací a provozem týmu typu CSIRT (CZ.NIC-CSIRT[1]), a podpory ze strany předchozího provozovatele – sdružení CESNET[2]. Zde se jednalo především o udržení jednotného rozhraní pro komunikaci se stěžovateli (těmi, kdo byli dotčení nějakým bezpečnostním incidentem, který měl původ v sítích provozovaných v ČR) a osobami zodpovědnými za sítě, ve kterých měly reportované incidenty původ.

2: **Převod technologického zázemí** (sítě, serverů, aplikací) proběhl rovněž bezvýpadkově a byl úspěšně dokončen spolu s transferem agendy a know-how v červnu 2011. Obnášel migraci tří systémů – mailového, webového a systému pro zpracování příchozích hlášení a sledování celého životního cyklu reportovaných incidentů. Dále se přenášelo několik menších systémů, správa diskuzní skupiny CSIRT.CZ, serveru pro ukládání informací pro BIS, intranetu pro členy skupiny a také samotné zprávy doménového jména.

3: **Informování národních i mezinárodních struktur o změně** mandátu týmu CSIRT.CZ a jeho převodu k novému provozovateli jsme informovali neprodleně na nejbližším setkání světové komunity bezpečnostních týmů (meeting TF-CSIRT), které se konalo v lednu 2011 v Barceloně (Španělsko). Zároveň jsme informovali o aktuálním stavu budování bezpečnostní infrastruktury v České republice a o tom, že CSIRT.CZ se stal Národním CSIRT České republiky.

Souběžně s výše uvedenou činností jsme se v roce 2011 věnovali především následujícím oblastem:

- ✔ definování role a cílů rozvoje CSIRT.CZ pro následující roky,
- ✔ udržení a posílení pozice CSIRT.CZ v národní i mezinárodní infrastruktuře,
- ✔ rozvojem základní služby, kterou je proces řešení a koordinace řešení

1 http://www.nic.cz/csirt/

2 CESNET je provozovatelem páteřní akademické počítačové sítě České republiky, http://www.cesnet.cz/.

bezpečnostních incidentů (tzv. *incident handling* a *incident response),*
- ✔ plnění role *vládního CSIRT České republiky*, jak stanoví Memorandum.

Poslední výše uvedený bod, tj. plnění role *vládního CSIRT České republiky*, se nám úspěšněji dařilo plnit z „vnějšího" pohledu, tj. byli jsme kontaktem pro hlášení bezpečnostních incidentů. Bohužel jsme nebyli úspěšní v navázání užší spolupráce s Odborem kybernetické bezpečnosti MV ČR, protože v první polovině roku 2011 na navázání spolupráce nebyl dostatečný prostor a pod odchodu Ing. Aleše Špidly z funkce ředitele Odboru zase podmínky. První spolupráce byla navázána až v srpnu 2011 a to s panem Františkem Stejskalem. To už ale byla v běhu změna gesce za oblast kyberkriminality z MV ČR na NBU, takže jsme se omezili pouze na zajištění nejdůležitějších záležitostí.

Aktuální stav týmu CSIRT.CZ:

Tým CSIRT.CZ plní roli Národního CSIRT České republiky tak, jak tuto roli definuje např. organizace ENISA[3]. Z hlediska základní služby řešení a koordinace řešení bezpečnostních incidentů, které jsou týmy typu CERT/CSIRT povinny plnit, naplňuje tým CSIRT.CZ roli tzv. „last resort" – místa poslední záchrany, kam je možné ohlásit závažný, přetrvávající nebo opakující se bezpečnostní incident. V říjnu 2011 přiznal úřad Trusted Introducer[4] týmu CSIRT.CZ status „accredited".
Tým CSIRT.CZ má v současné době oficiálně čtyři členy, kteří zajišťují provoz týmu a jeho základní služby. Na chodu týmu se ale podílí řada dalších zaměstnanců sdružení CZ.NIC – správci sítí a služeb, specialisté na právo, odborníci na problematiku bezpečnosti sítí a služeb, výzkumníci a další. V současné době nedokážeme vyčíslit, kolik HR (FTE) je na provoz Národního CSIRT ČR alokováno.

Polem působnosti týmu CSIRT.CZ jsou všechny sítě provozované v České republice, tzn. všechny IP adresy (adresové rozsahy) přidělené organizací RIPE NCC do České republiky.

Základní kontaktní informace jsou zveřejněny na www stránkách týmu CSIRT.CZ – http://www.csirt.cz/.

Jak je možné tým CSIRT.CZ kontaktovat

Tým preferuje kontakt elektronickou poštou. K nahlášení bezpečnostního incidentu slouží adresa abuse@csirt.cz, pro obecný kontakt adresa info@csirt.cz. V urgentním případě, nebo v případě, že není možné poslat zprávu elektronicky, je možné použít telefonní číslo +420 222 745 111, jehož příjem zajišťuje dohledové centrum sdružení CZ.NIC v nepřetržitém provozu.

3 Evropská agentura pro bezpečnost sítí a informací, http://www.enisa.eu.
4 Úřad TI napomáhá vzniku CERT/CSIRT týmů a provádí jejich akreditace a certifikace, http://www.trusted-introducer.org/

Role a cíle CSIRT.CZ:

- ✔ Plnit roli PoC (Point of Contact), tzn. zajišťovat jednoduchý a důvěryhodný kontakt pro Českou republiku
- ✔ Udržování zahraničních vztahů – se světovou komunitou CERT/CSIRT týmů a organizacemi, které tuto komunitu podporují.
- ✔ Spolupráce 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

Služby poskytované CSIRT.CZ:

- ✔ Řešení a koordinace řešení bezpečnostních incidentů, které mají původ nebo cíl v sítích provozovaných v České republice, nebo se obecně dotýkají kyberprostoru České republiky.
- ✔ Osvětová a školící činnost.
- ✔ Proaktivní služby v oblasti bezpečnosti.

Řešení a koordinace řešení bezpečnostních incidentů

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

- ✔ jedna zveřejněná phishingová stránka
- ✔ zavirovaný stroj (síť), který je zdrojem spamu
- ✔ jeden stroj se zjevně narušenou bezpečností (hack)
- ✔ jeden stroj, který je zdrojem DOS útoku, scanu

Tato událost (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 provozu za rok 2011:

- ✔ Celkový počet řešených bezpečnostních incidentů = 776
- ✔ Podle ***koncových stavů incidentů*** (při zavírání kauzy/ticketu jej klasifikujeme, bude podrobněji popsáno níže):

Uzavřeno vyřešeno	131
uzavřeno-jsme informováni	19
uzavřeno-pozitivní změna	119
uzavřeno-upozornění	496
uzavřeno-nevyřešeno	10
uzavřeno-neschopni vyřešit	0

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

Phishing	144
IDS	491
Virus	1
Spam	27
Malware	9
Trojan	5
Other	62
Botnet	5
Probe	25
Portscan	6
DOS	1
Crack	0
Copyright	0

Celkově bylo na adresu pro hlášení bezpečnostních incidentů abuse@csirt.cz zasláno přibližně **1655 zpráv**. Z tohoto počtu bylo jako tzv. *spam*[5] označeno **automaticky** cca **628 zpráv**, **ručně** některým členem týmu cca **199 zpráv**. **Korektních zpráv** (tzv. *ham*) bylo přijato cca **1012**. Toto množství představuje oněch 776 bezpečnostních incidentů, které v roce 2011 tým CSIRT.CZ řešil. Rozpor mezi čísly označujícími *počet přijatých hlášení* a *počet řešených incidentů* je dán tím, že občas je incident nahlášen najednou z více zdrojů. Počet zpráv **odeslaných** v rámci procesu řešení bezpečnostních incidentů bylo cca **1200**.

Při uzavírání 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

5 Nevyžádaná pošta obtěžujícího nebo nesmyslného charakteru, často nesoucí závadný obsah ve formě virů apod.

	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.

V některých případech se stává, že koncový stav incidentu je překlasifikován, např. ze stavu **jsme informováni** na stav **vyřešeno/nevyřešeno**. Tak se stane v případě, kdy stěžovatel v pozdější fázi řešení problému požádá o pomoc CSIRT.CZ, nebo se závažnost incidentu zvýší.

Mezi bezpečnostními incidenty ohlášenými týmu CSIRT.CZ se v roce 2011 objevilo několik velice zajímavých případů:

1. **SCADA**

   V listopadu náš tým obdržel od týmu ICS-CERT seznam přibližně osmdesáti potenciálně ohrožených ICS (Industrial Control System) systémů v Česku. ICS systémy zahrnují systémy SCADA, DCS a PLC. Tyto systémy nebyly přímo napadeny, ale jejich provozovatelé je měli dostupné z internetu a mnohdy pouze s minimálním zabezpečením, či dokonce s

defaultním jménem a heslem. Informace jsme zpracovali a individuálně předali všem provozovatelům těchto systémů. Více informací lze nalézt například na této stránce.

2. **Spolupráce s FBI a MVČR**

   V říjnu náš tým ve spolupráci s MVČR pomáhal FBI s předběžným zajištěním důkazů. Jednalo se o server, který sloužil několik let jako hlava botnetu. Protože existovala reálná možnost, že by po sobě vlastník tohoto serveru mohl zamést stopy, byli jsme požádáni o vyjednání předběžných záloh dat důležitých pro další vyšetřování. Podařilo se nám s provozovatelem hostingové služby dohodnout provedení kompletní zálohy disku tohoto C&C serveru.

3. **SOOM.CZ**

   Při prověřování obsahu serveru soom.cz, kvůli nahlášenému podezření na šíření virové nákazy, jsme narazili na veřejně dostupný článek, informující o zranitelnostech webů http://cds.mfcr.cz/, http://i.statnisprava.cz/ a http://www.czechpoint.cz. Jednalo se o chyby v rozsahu od XSS, přes SQL injection, až po možnost procházet obsah adresářů. Správce uvedených serverů jsme o těchto zranitelnostech informovali a většina jich byl krátce po našem upozornění odstraněna. Tato akce měla kladnou zpětnou reakci ze strany BIS.

4. **Kasina a e-shopy**

   V srpnu bylo přijato hlášení o incidentu, jehož původce investoval do nákupu legálního hostingu. Nejprve si u O2 pronajal celou síť, v níž provozoval různá kasina, e-shopy s podezřele levným software a podobně. O2 zvolilo taktiku mrtvého brouka. Smlouvu tomuto zákazníkovi vypovědělo až v říjnu, kdy už pro něj situace byla neúnosná. Došlo totiž k zablokování všech jejich SMTP serverů společností SpamHause. Provozovatel webů se však pouze přesunul k UPC. U UPC se situace opakovala. Až ve chvíli, kdy důsledky chování tohoto zákazníka dopadly na další zákazníky, došlo na výpověď smlouvy. Poté proběhlo stěhování k menšímu provozovateli webhostingových služeb – službě fastport.cz. Tam sice také nechtěli zákazníka odpojit, ale byli ochotni o celé věci diskutovat. Když jsme jim vysvětlili, že provozovat kasina lze v České republice pouze po nahlášení u Ministerstva financí ČR a poukázali na předchozí události spojené s provozováním těchto webů, rozhodl se sám aktivně smlouvu vypovědět. Tato poslední zkušenost pravděpodobně odradila provozovatele těchto webů od jejich dalšího provozování v naší zemi, neboť CSIRT.CZ od té doby již žádnou další stížnost neobdržel.

5. **DOS RC**

   V závěru roku byl zajímavý případ masivních DDOS útoků vedených na e-shopy provozované v ČR. Tímto případem se ještě stále ve spolupráci s CSIRT týmem Ministerstva obrany ČR zabýváme.

Osvětová činnost

Snažili jsme se nezanedbávat ani osvětovou činnost. V červenci 2011 jsme

uspořádali první školení nazvané ***„Svět Internetu a domén"***. Školení je určeno zaměstnancům státní správy, zejména složkám Policie ČR. Je koncipováno jako základní exkurs do problematiky internetu jako takového, jeho základního fungování a objasnění principů. Speciální pozornost je věnována praktickým záležitostem, 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, 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
- ✔ 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.

Toto školení nabízíme jako službu v rámci našeho závazku spolupracovat s bezpečnostními složkami ČR a vzdělávat jejich členy. Úvodní cílovou skupinou, kterou jsme oslovili a toto školení jim nabídli, byli pracovníci Ministerstva vnitra České republiky a BIS (Bezpečnostní Informační Služba, http://www.bis.cz). Toto první školení bylo pojaté jako pilot, kde cílem bylo mimo jiné od účastníků získat zpětnou vazbu o obsahu. Tento účel byl naplněn, od účastníků jsme získali cenné náměty, které byly použity pro doplnění a zlepšení školicích materiálů.

Zaměstnanci týmu CSIRT.CZ se také aktivně spoluúčastnili čtyřdenního školení pro zaměstnance ČTÚ, kde měli jeden den na školení o principech fungování internetu, sítí a internetových protokolů. Další důležitou částí bylo informování o možných způsobech dohledávání informací k nahlášeným incidentům, se zaměřením na využití veřejně dostupných zdrojů dat. Součástí školení byly také názorné příklady a ukázky. Dalším bodem bylo vysvětlení funkce a důležitosti týmů typu CSIRT, vysvětlení pojmů vztahujících se k různým způsobům napadení v prostředí internetu s praktickými ukázkami.

Z veřejně pořádaných akcí jsme se s příspěvkem zúčastnili těchto konferencí a workshopů:

- ✔ **1. dubna** – přednáška o Národním CSIRT České republiky na odborném semináři k problematice elektronické bezpečnosti, který v Jihlavě pořádal Kraj Vysočina.
- ✔ **9. června** – přednáška „Přínosy zřízení a provozu CSIRT týmu v organizaci " na konferenci domácí konferenci IT11
- ✔ **4. srpna** – přednáška „Národní CSIRT České republiky" na konferenci „Internet v Telči", kterou uspořádal kraj Vysočina spolu se společností Autocont.
- ✔ **15. září** – přednáška „CERT/CSIRT - zkušenosti z provozu" na konferenci „České právo a informační technologie" v Hrotovicích. Více informací je zde:

http://cpit.law.muni.cz/content/cs/

- ✔ **15. října** – přednáška „Bezpečnostní týmy typu CSIRT/CERT" na uzavřené konferenci pořádané ČTU.
- ✔ **25. října** – přednáška „Bezpečnostní týmy typu CSIRT/CERT" na konferenci "Bezpečnost kyberprostoru"
- ✔ **14. října** – přednáška „CERT/CSIRT - zkušenosti z provozu" na konferenci „Dětská kybernetická kriminalita a sociální sítě" v Jihlavě. Více info zde: http://www.kr-vysocina.cz/pozvanka-na-konferenci-detska-kybe rneticka-kriminalita-a-socialni-site/d-4037362/p1=36499

Random porty

Další výraznou akcí CSIRT týmu bylo informování provozovatelů nedostatečně zabezpečených DNS serverů. Akce proběhla ve spolupráci s laboratořemi CZ.NIC, které dodali potřebné vstupy, které pak členové CSIRT týmu dále zpracovali a distribuovali. Jednalo se o informace o DNS serverech, jejichž odpovědi na DNS dotazy bylo možné jednoduše podvrhnout, díky špatné konfiguraci serveru. Při této akci byla zjištěna tato chyba na 2397 originálních IP adresách. Celkem 34 % oslovených správců reagovalo na oznámení opravou, či odstavením DNS serveru.

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.

Pracovní skupina E-CRIME

Pracoviště CSIRT.CZ spolupracuje s Krajem Vysočina (Jihlava) a její Pracovní skupinou E-CRIME, která se zabývá zlepšením situace v oblasti elektronické bezpečnosti kraje a jejímiž členy jsou vedle pracovníků krajského úřadu z odboru informatiky, školství a sociálních věcí, také odborní pracovníci z řad Policie ČR, Krajské hospodářské komory kraje Vysočina, Okresního státního zastupitelství v Jihlavě, příspěvkové organizace Vysočina Education, dále pak odborníci ze společností Saferinternet.cz, AutoCont Jihlava a sdružení CESNET.

CSIRT.CZ v rámci této spolupráce vystoupil s příspěvky o činnosti Národního CSIRT ČR, problematice CERT/CSIRT týmů nebo jiným odborným tématem na několika akcích pořádaných Krajem Vysočina a spolupracujícími partnery (viz odstavec Osvětová činnost).

Bezpečnostní složky

Spolupráce s BIS (Bezpečnostní informační službou) pokračovala i v roce 2011 a to v oblasti výměny informací o řešených bezpečnostních incidentech, tak v oblasti výměny know-how. Zaměstnanci BIS byli účastníky prvního pilotního školení nazvaného „Svět Internetu a domén" a v závěrečné diskusi poskytli cennou zpětnou vazbu, kterou jsme použili pro zlepšení obsahu jednotlivých přednášek z oblasti organizace Internetu, provozu sítí a služeb, práva apod.

Zaměstnanci BIS se také účastnili **6th CERT workshopu**, který ENISA pořádala v Praze a to na naši žádost – aby Česká republika měla důstojného reprezentanta z LEA složek.

Pracovní skupina CSIRT.CZ

Pracovní skupina CSIRT.CZ se v roce 2011 setkala jednou – 20. dubna 2011. Na tomto setkání byli její členové informováni o aktuálním stavu budování bezpečnostní infrastruktury v ČR, stavu převodu CSIRT.CZ od sdružení CESNET ke sdružení CZ.NIC a byly prodiskutovány plány na další činnosti Pracovní skupiny CSIRT.CZ. Dále proběhla diskuse nad materiálem *„Strategie ČR pro oblast kybernetické bezpečnosti"*, který předložil ředitel Odboru kybernetické bezpečnosti MV ČR Aleš Špidla.

Světové platformy pro spolupráci (TF-CSIRT, FIRST)

V rámci mezinárodní spolupráce jsme se pravidelně zúčastňovali hlavních setkání světových bezpečnostních týmů, které organizovala TERENA, FIRST a ENISA. V roce 2011 to byly tyto akce:

- ✔ 32nd TF-CSIRT/FIRST Technical Colloquium, leden 2011, Barcelona (Španělsko)
- ✔ 33th TF-CSIRT Meeting, květen 2011, Malahide (Irsko)
- ✔ 23th Annual FIRST Conference, červen 2011, Vídeň (Rakousko)
- ✔ 34th TF-CSIRT Meeting, září 2011, Luxembourg (Lucembursko)
- ✔ 6th CERT workshop, říjen 2011, Praha

Prohlášení CSIRT.CZ za Národní CSIRT ČR nám otevřelo cestu do dalších zajímavých mezinárodních uskupení – stali jsme se členy skupiny CERT/CSIRT týmů s národním/vládním mandátem, kterou organizuje CERT/CC[6] a zúčastnili jsme setkání této skupiny, které proběhlo dne 19. června 2011 ve Vídni (Rakousko) v rámci výroční konference FIRST. Zde jsme stručně představili Národní CSIRT ČR, jeho vznik, roli a cíle.

Získání akreditace u úřadu TI

6 CERT Coordination Centre, http://www.cert.org/. CERT/CC je první oficiálně ustanovený týmu typu CERT na světě, ten, který položil základ pro budování bezpečnostní infrastruktury.

Ministerstvo vnitra svým prohlášením pracoviště CSIRT.CZ za Národní CSIRT České republiky a podpisem Memoranda odstranilo problém se vstupem CSIRT.CZ do akreditačního procesu (accreditation proccess) u úřadu Trusted Introducer (http://www.trusted-introducer.org) – úřad v roce 2008 po přidělení statusu „listed" varoval před podáním žádosti o akreditační proces z důvodů nejasné situace v České republice na poli budování a provozování národního/vládního pracoviště CSIRT. Až v červnu 2011, poté co došlo k vyjasnění pozice CSIRT.CZ, jsme tedy úřad Trusted Introducer požádali vstup do procesu akreditace. Proces akreditace započal v červenci a úspěšně jsme jej dokončili v říjnu 2011. Tím se Národní CSIRT České republiky dostal do elitního klubu tzv. *akreditovaných* týmů, které mají přístup k celé řadě zajímavých informací a spolupráci.

Spolupráce s ENISA

Tým CSIRT.CZ, který ze své pozice „modelového pracoviště" a „posledního místa záchrany", byl mezinárodní infrastrukturou vnímán již od svého vzniku jako tzv. **de facto national CSIRT team** (volně přeloženo jako „v podstatě národní CSIRT tým"), se stal za Českou republiku už v roce 2010 spolupracovníkem organizace ENISA. V rámci této spolupráce se 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 účastníme – v roce 2011 jsme se zúčastnili cvičení Cyber Atlantic 2011, o kterém podrobně hovoří samostatná zpráva.

V roce 2011 jsme se stali členy expertní pracovní skupiny zabývající se spoluprací mezi světem orgánů činných v trestním řízení a světem CERT/CSIRT týmů v oblasti boje proti kyberkriminalitě (Cooperation between CERTs and Law Enforcement Agencies to fight against cybercrime). Výsledkem práce této expertní skupiny bude dokument mapující zkušenosti získané od existujících týmů na obou stranách (LEA a CERT/CSIRT), sada doporučení a především podklad pro další práci.

Kromě výše popsané činnosti v pracovní skupinách ENISA se tým CSIRT.CZ podílel ve spolupráci s ENISA a Europol na organizaci mezinárodního workshopu zaměřeného na internetovou bezpečnost - **6th CERT/CSIRT workshop ENISA**, který proběhl ve dnech 3. a 4. října 2011 v Praze. Workshopu se zúčastnili členové evropských národních a vládních CERT/CSIRT týmů (za Českou republiku se samozřejmě zúčastnili členové CSIRT.CZ) a zástupci orgánů činných v trestním řízení z celé Evropy.

V listopadu 2011 jsme se aktivně zúčastnili ještě jedné zajímavé akce – cvičení **SISE 2011**. Toto cvičení uspořádal tým CSIRT.SK (vládní CSIRT Slovenska) s cílem ověřit schopnost spolupráce různých subjektů na Slovensku a požádal týmy CSIRT.CZ a CERT.at o spolupráci. Úkolem CSIRT.CZ bylo reagovat podle předem daného scénáře, simulovat práci na řešení bezpečnostního incidentu a komunikovat se subjekty ze Slovenska. Byla to zajímavá a z hlediska dalšího rozvoje CSIRT.CZ cenná a motivující zkušenost.

Závěr

V současné době jsou v České republice oficiálně úřadem Trusted Introducer konstituovány čtyři týmy 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

Další funkční tým typu CSIRT, i když není oficiálně napojen na světovou infrastrukturu a konstituován v rámci úřadu Trusted Introducer nebo FIRST, je provozován také Ministerstvem obrany ČR – jedná se o vojenský CSIRT tým určený pro spolupráci s obdobnými týmy v rámci členských zemí NATO. Na podzim 2011 došlo k prvnímu oficiálnímu setkání CSIRT týmu Ministerstva obrany a CSIRT.CZ.

Výše uvedené samozřejmě neznamená, že v České republice existuje pouze 5 bezpečnostních týmů. Zkušenosti z řešení nahlášených bezpečnostních incidentů víme, že ačkoliv v rámci komerčních organizací (ISP, banky, poskytovatelé služeb) v České republice nejsou CERT/CSIRT týmy oficiálně ustaveny, existují zde oddělení a týmy, které se bezpečností sítí a služeb reálně zabývají a roli CERT/CSIRT týmu de facto plní. Tato oddělení a týmy nejsou ale napojeny na světovou bezpečnostní infrastrukturu CERT/CSIRT týmů a nezapojují se do mezinárodní spolupráce a výměny informací.

Dne 19. října 2011 přijala vláda České republiky usnesení č. 781 o ustavení NBÚ (Národní bezpečnostní úřad) gestorem problematiky kybernetické bezpečnosti a zároveň národní autoritou pro tuto oblast. V listopadu 2011 došlo k první schůzi pracovníků NBÚ a CSIRT.CZ na půdě sdružení CZ.NIC. Obě strany na tomto setkání deklarovaly ochotu ke spolupráci, výměně informací a vzájemné pomoci v oblasti budování bezpečnostní infrastruktury v ČR. Tým CSIRT.CZ ve vzniku vládního CSIRT očekává spolupracujícího partnera na té nejvyšší odborné úrovni.