ZPRÁVA O ČINNOSTI CSIRT.CZ (NÁRODNÍHO CSIRT ČR) ZA ROK 2015

CSIRT.CZ
powered by CZ.NIC

Obsah

Tým CSIRT.CZ

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 Národního bezpečnostního úřadu (dále jen NBÚ) 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 bylo – s platností od 1. ledna 2013 – uzavřeno Memorandum mezi sdružením CZ.NIC a Národním bezpečnostním úřadem o provozování Národního CSIRT ČR.

Toto Memorandum bylo platné do konce roku 2015 a v souladu se Zákonem o kybernetické bezpečnosti bylo nahrazeno veřejnoprávní smlouvou, uzavřenou dne 18. prosince 2015 s Národním bezpečnostním úřadem.

Rok 2015 v kostce

Bezpochyby nejdůležitější událostí v roce 2015 byl vstup zákona o kybernetické bezpečnosti a o změně souvisejících zákonů (dále jen ZKB), č. 181/2014 Sb. v platnost.
Tento zákon přinesl Národnímu CSIRT nové povinnosti a zároveň jasně ukotvil jeho existenci v rámci právního řádu. V průběhu roku se sdružení CZ.NIC, které dosud Národní tým CSIRT.CZ provozovalo, úspěšně účastnilo výběrového řízení vypsaného Národním bezpečnostním úřadem. Ke konci roku 2015 pak byla podepsána veřejnoprávní smlouva mezi sdružením CZ.NIC a NBÚ, na jejímž základě bude i nadále provozován Národní bezpečnostní tým CSIRT.CZ sdružením CZ.NIC.

V roce 2015 byla prováděna další integrace provozovaných služeb a systémů, tak aby tým CSIRT.CZ dokázal data z jednotlivých provozovaných systémů využít v samotném procesu Incident Handlingu i v dalších analyticky zaměřených projektech. V procesu Incident Handlingu tak náš tým nově informuje zahraniční i tuzemské partnery o IP adresách, identifikovaných jako problematické v rámci námi provozovaných honeypotů.

Velmi důležité je zpracování vzorků malware získaných od útočníků v rámci provozovaných honeypotů. Tyto vzorky jsou nově předávány antivirovým společnostem, které tak mohou rychleji reagovat na nové hrozby.

Data získávaná z vlastních zdrojů CSIRT.CZ dále využíváme v rámci nově budovaného analytického systému.

V roce 2015 průběžně probíhalo další vylepšování nástrojů, používaných v rámci řešení incidentů. V souvislosti s požadavky ZKB také došlo k dílčím úpravám systému OTRS, který je používán v rámci procesu řešení incidentů tak, aby bylo možné dostát zákonem kladeným požadavkům.

Důležitou součástí práce Národního bezpečnostního týmu je osvěta a národní a mezinárodní spolupráce. I v tomto roce jsme pokračovali v již nastolené spolupráci v rámci pracovní skupiny CSIRT.CZ, v pracovních skupinách organizací ENISA a TERENA, s Bankovní asociací, s organizací NCBI (Národní Centrum Bezpečnějšího Internetu), s lokálními bezpečnostními týmy, které

působí v sítích významných ISP, registrátorů bank, s bezpečnostními složkami, akademickou sférou a tak dále. CSIRT.CZ se dále zapojil do společného open-source projektu evropských bezpečnostních týmů IntelMQ a stal se tak jedním z jeho důležitých přispěvatelů.

Náš tým se také postavil do čela mezinárodního projektu „Cyber Security in the Danube Region" (CS Danube). Tento projekt, spolufinancovaný Evropskou komisí v rámci programu START, je zaměřen na spolupráci, posilování důvěry a kapacit CSIRT týmů v rámci podunajského regionu.

Dalším projektem, který začal v roce 2015 a bude mít přesah i do dalších let je projekt „Predikce a ochrana před kybernetickými incidenty" (PROKI), realizovaný v rámci Programu bezpečnostního výzkumu ČR na léta 2015 – 2020. V neposlední řadě sdružení CZ.NIC a bezpečnostní tým CSIRT.CZ předložili ve spolupráci s Institute for Information Industry (III) z Tchaj-wanu návrh projektu „Honeypot jako služba" (HaaS), který Technologická agentura ČR ohodnotila jako vůbec nejlepší projekt v dané výzvě. Realizace tohoto projektu bude zahájena 1. června 2016.

Tým CSIRT.CZ se také aktivně zapojil do několika národních a mezinárodních cvičení. Na národní úrovni se jednalo o strategické cvičení EDA, organizované Národním bezpečnostním úřadem. Na mezinárodní úrovni jsme se zapojili do cvičení NATO Cyber Coalition 2015 a do komunikačního cvičení platformy CECSP. V roli pozorovatele jsme se rovněž účastnili cvičení Cyber Czech.

V uplynulém roce se tým zapojil do připomínkování důležitých dokumentů, jako jsou Národní strategie kybernetické bezpečnosti, či Národní strategie vzdělávání v kybernetické bezpečnosti.

Za důležité považujeme též připomínkování klasifikace incidentů, která má být součástí jednotného označování incidentů v rámci celé Evropské unie, a bude sloužit mimo jiné i policejním složkám.

V závěru roku se náš tým připravoval na mezinárodní střetnutí CSIRT/CERT týmů sdružených u Trusted Introducer TF-CSIRT, které je plánováno na leden roku 2016 a které je sdružením CZ.NIC a týmem CSIRT.CZ hostováno. Chtěli bychom tím umožnit komunitě českých bezpečnostních týmů, lepší zapojení a spolupráci v mezinárodní oblasti.

Za zmínku stojí i rozšíření komunity českých bezpečnostních týmů o pět dalších oficiálně ustanovených týmů, které získaly status „listed" u služby Trusted Introducer.

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 jejího kyberprostoru.

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

(1) problémy, u kterých byly vyčerpány veškeré známé způsoby řešení, ale problém přesto přetrvává,

(2) problémy, u kterých není jednoduché identifikovat, kdo je původcem incidentu, nebo kdo by se jeho řešením měl zabývat a

(3) problémy, které mají závažný dopad na infrastrukturu v ČR. Tyto problémy mohou mít plošný charakter a negativně ovlivňovat další sítě, služby a uživatele, je tedy nutné, aby se informace tohoto typu co nejrychleji dostaly k těm, kdo mohou zasáhnout a nastavit například vhodné metody obrany apod.

V roce 2015 pokračoval nárůst řešených incidentů, ale nebyl již tak značný, jako v předchozím roce. V roce 2014 bylo týmu CSIRT.CZ nahlášeno 939 incidentů, **v roce 2015** pak **1160**. Nárůst řešených incidentů byl tedy oproti loňskému roku 23,5 %. Incidenty, které jsou týmu CSIRT.CZ předávány také dále nabývají na složitosti, komplexnosti a náročnosti při jejich zpracování.

Po provedení základní analýzy incidentu a zahájení procesu řešení (tzn. kontaktování osoby, která má prostředky problém vyřešit a odstranit) je často nutné provést další kroky, například získat seznam dalších potenciálních obětí a tyto osoby varovat, dohledat informace o možných infikovaných počítačích v dalších zdrojích dat a informací a dohledat informace o zneužitých uživatelských identitách či zranitelných zařízeních. Z tohoto důvodu opět vzrostl počet odeslaných e-mailů **z cca 5000 v roce 2014 na více 6400 v roce 2015**, což představuje meziroční nárůst o 28 %.

STATISTIKA PROCESU ŘEŠENÍ BEZPEČNOSTNÍCH INCIDENTŮ TÝMEM CSIRT.CZ:

	2008	2009	2010	2011	2012	2013	2014	2015	**Celkem**
IDS	0	0	0	491	3 924	2 121	2 380	3 771	**12 687**
Phishing	65	220	209	144	159	175	368	367	**1 707**
Malware	53	97	42	9	19	44	117	242	**623**
Spam	47	28	103	26	43	73	159	108	**587**
Other	1	5	8	62	13	75	101	264	**529**
Virus	0	121	178	1	1	0	0	0	**301**
Trojan	66	6	26	5	5	12	56	90	**266**
DOS	1	4	2	2	68	72	32	37	**218**
Probe	0	3	14	25	12	26	86	42	**208**
Botnet	0	3	46	5	8	15	0	2	**79**
Portscan	10	4	1	6	1	3	2	5	**32**
Pharming	0	0	0	0	0	0	18	3	**21**
Crack	1	4	0	0	0	0	0	0	**5**
Copyright	0	0	1	0	1	0	0	0	**2**
Celkem	**244**	**491**	**634**	**776**	**4 254**	**2 616**	**3 319**	**4 931**	**17 265**

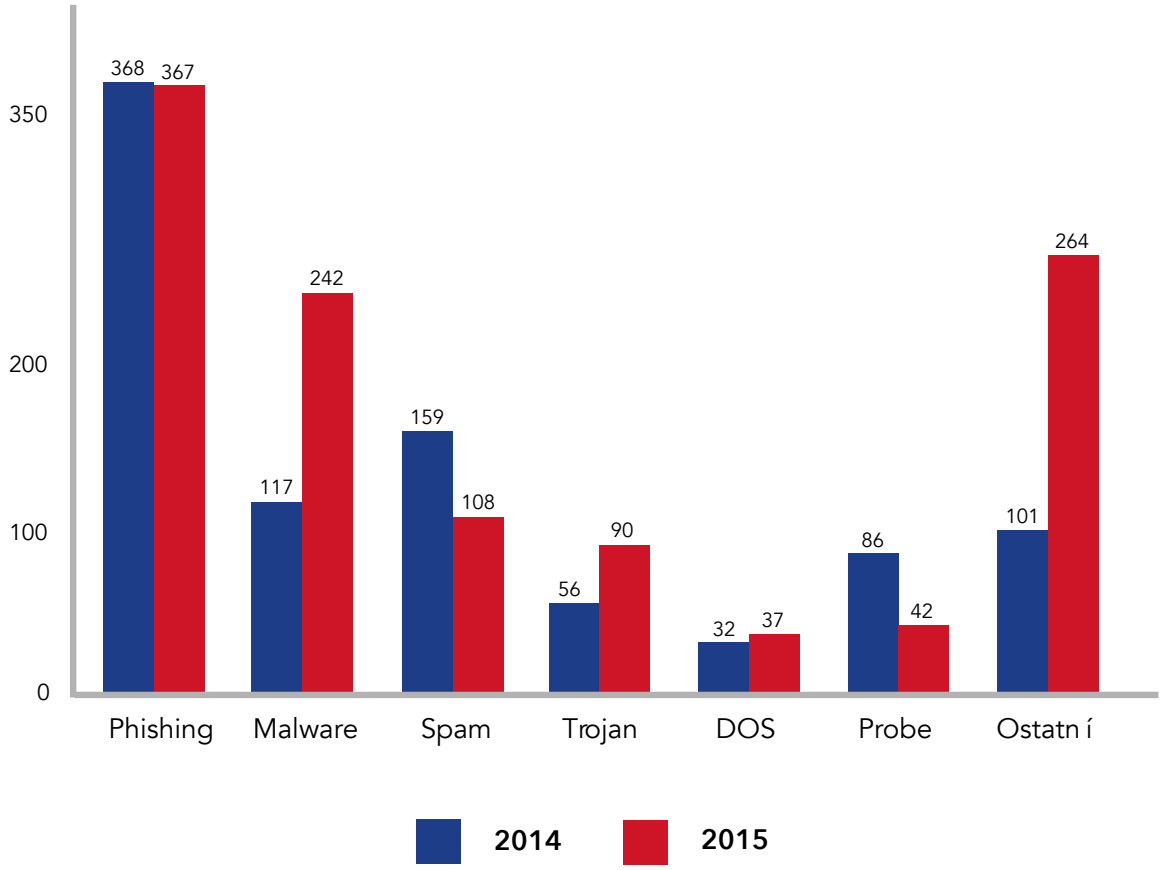
Do celkového počtu řešených bezpečnostních incidentů se nezapočítávají incidenty typu IDS, které jsou uvedeny ve druhém řádku zde uvedené tabulky. Tato automatizovaná služba typu Intrusion Detection System informuje správce koncových sítí o tom, že jejich síť je zdrojem (bezpečnostní) události, která následně může být zdrojem bezpečnostního incidentu. Uvedený počet incidentů za rok 2015 tedy představuje počet varování zaslaných touto službou správcům koncových sítí provozovaných v ČR.

S ohledem na to, že se k týmu CSIRT.CZ v roli Národního týmu ČR dostává jen nepatrná část bezpečnostních incidentů majících původ nebo cíl v sítích provozovaných pouze v ČR, je výše uvedená tabulka se statistikou bezpečnostních incidentů řešených týmem CSIRT.CZ pouze orientační. Lze však konstatovat, že loňský odhad trendu, který jsme v této zprávě za rok 2014 učinili na základě nárůstu počtu incidentů typu phishing, malware a trojan se bohužel potvrdil a i v roce 2015 bylo možné pozorovat růst těchto typů incidentů.

Zajímavý je také nárůst incidentů v kategorii „Jiné". Do této kategorie řadíme incidenty typu Fast Flax, podvodné informace na webových stránkách, incidenty z honeypotů, nebo problémy s routery ze SoHo segmentu, tedy incidenty zahrnující použití slabých hesel, configuration download, nebo Bash Remote Code Execution.

Statistiky z procesu řešení bezpečnostních incidentů jsou průběžně zveřejňovány na našich stránkách: https://www.csirt.cz/page/2635/statistiky-resenych-incidentu/.

POČTY VYBRANÝCH BEZPEČNOSTNÍCH INCIDENTŮ HLÁŠENÝCH TÝMU CSIRT.CZ V LETECH 2014 A 2015:



ZAJÍMAVÉ KAUZY ROKU 2015

V roce 2015 jsme opět řešili i několik incidentů, které svým rozsahem, provedením, nebo pozadím vybočovaly z běžného rutinního provozu.

Vzhledem k postupující integraci našich služeb začněme statistikami z našich nově zpracovávaných dat z honeypotů (více informací o našich honeypotech najdete dále v této zprávě). Data z nich jsme začali využívat v dubnu 2015 a od té doby jsme zaznamenali celkem 9 757 unikátních IP adres, které se snažily o útok na naše honeypoty.

POČTY UNIKÁTNÍCH IP ADRES (ÚTOKY NA HONEYPOTY) :

Měsíc	Počet unikátních IP adres
duben	1 474
květen	1 563
červen	2 062
červenec	1 934
srpen	823
září	565
říjen	1 336
listopad	1 131
prosinec	1 373

Na základě těchto dat bylo naším týmem v rámci prevence osloveno více než 50 zemí z celého světa.

Další aktivitou, kterou v rámci našeho týmu s pomocí honeypotů vyvíjíme je identifikace nového, nebo dosud neznámého malware. Námi identifikované, dosud neznámé vzorky, v rámci navázané spolupráce předáváme antivirovým společnostem. V roce 2015 jsme takových vzorků předali 22.

Dalším zajímavým incidentem byla **eliminace malware volgmer**, který umožňoval jeho správcům zneužívat napadené počítače k různým útokům. Tento malware, dle dosud zjištěných skutečností, stál za útoky na společnost Sony Pictures a podílel se pravděpodobně i na sběru informací o platebních kartách či krádežích přihlašovacích údajů. Na základě upozornění od Korejského národního CSIRT jsme ve spolupráci s českým vládním CSIRT distribuovali informace o napadení tímto malware do jednotlivých sítí a organizací.

Náš tým se v roce 2015 podílel také na postupné **eliminaci botnetu Ramnit**. V roce 2015 jsme obdrželi celkem 222 emailů se záznamy komunikace počítačů napadených tímto malware. Tyto informace jsou získávány díky sledování počítačů s řídícími centry tohoto botnetu (tzv. sinkholing). Celkem se jednalo o více než 335 000 záznamů z 363 unikátních IP adres v ČR.

Ramnit byl poprvé spatřen v roce 2010 jako počítačový červ, v roce 2011 jej pak autoři vylepšili. Díky zveřejnění zdrojových kódů bankovního trojského koně Zeus se jim podařilo přidat do Ramnitu funkce typické pro bankovní trojské koně. V roce 2014 se

pak tento botnet stal čtvrtým největším botnetem na světě. Díky koordinaci Europolu v roce 2015, kdy tento botnet již dosahoval síly 3,2 miliónů počítačů, se počet infikovaných počítačů začal zmenšovat.

Dále jsme v uvedeném roce řešili několik incidentů na **základě požadavků Policie ČR**. Jednalo se o odstranění několika phishingových stránek, šíření malware a také o eliminaci podvodných aplikací pro Android, které se vydávaly za aplikace společností Seznam a Facebook a následně vedly k vykrádání platebních účtů. Pomáhali jsme také se zablokováním podvodného e-shopu či serverů, které sloužily k prodeji ukradených údajů o platebních kartách a v jednom případě jsme pomáhali s analýzou logů z DDoS útoku.

Ani tento rok nás neminula **řada útoků typu DDoS**. Pomáhali jsme eliminovat útoky tohoto typu na síť velkého českého operátora i velké hostingové společnosti působící v ČR. Řešili jsme útoky vedené i v opačném směru, tedy pocházející z ČR a směřující například do Španělska nebo Gruzie, kde se tyto útoky zaměřovaly na vládní instituce nebo banky dané země.

S vládním CSIRT týmem GovCERT jsme během uplynulého roku spolupracovali na více než padesáti incidentech různého typu. Nejčastěji se jednalo o incidenty typu skenování portů, phishing, spam, malwarové infekce na koncových stanicích či přímo komunikace s řídícími servery botnetů.

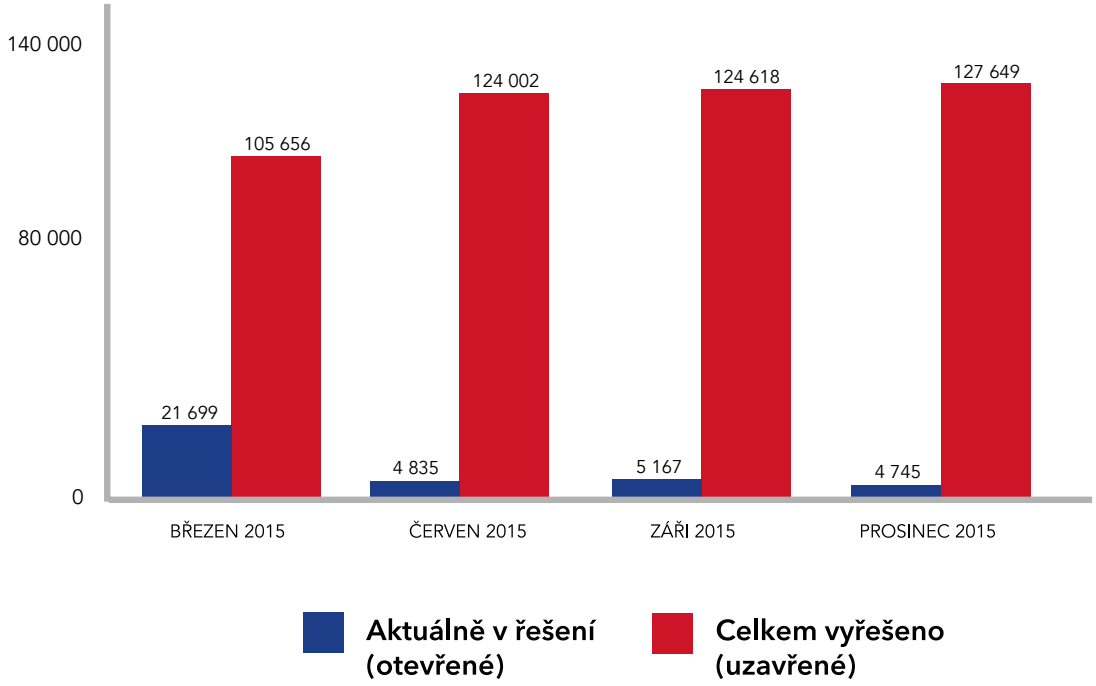
I v roce 2015 pak pokračoval trend z roku 2014 a mohli jsme se tak setkávat s útoky **zaměřenými přímo na uživatele z ČR**, přičemž jsme zaznamenali další vylepšování těchto útoků. Opět jsme tak pozorovali různá upozornění, například na údajný nedoručený balík, neuhrazené faktury, či na nařízenou exekuci. Cílem těchto útoků bylo přinutit uživatele ke spuštění přiložených souborů, obsahujících malware. Náš tým na tyto útoky vždy upozorňoval prostřednictvím naší služby AZB, z níž pak novinky čerpají i další média.

SLUŽBA MDM (MALICIOUS DOMAIN MANAGER)

V rámci služby MDM využíváme především veřejně dostupné zdroje informující o doménách, které byly napadeny nějakým druhem malware. Pomocí této služby jsou vytěžena data z veřejných zdrojů a následně přeposlána osobám zodpovědným za chod napadené domény, s žádostí o prošetření a případnou nápravu situace.

Stručnou statistiku využití této služby za rok 2015 reflektuje následující graf, který zobrazuje počet aktuálně „nakažených" domén a (kumulativní) počet domén, u kterých se po intervenci podařilo závadný obsah odstranit.

POČTY OTEVŘENÝCH A VYŘEŠENÝCH PŘÍPADŮ V SYSTÉMU MDM



V roce 2015 prošla služba MDM výrazným vývojem. Do aplikace byla přidána možnost provést automatickou analýzu incidentů na jednotlivých doménách. Díky tomuto nástroji si nyní může obsluha aplikace snadno dohledat skutečný zdroj infekce. To je dáno tím, že napadené stránky v doméně .CZ v naprosté většině případů figurují v roli prostředníka, ale nejsou samotným místem, ze kterého se spouští instalace malware. Naším cílem však není pouze čistit český doménový prostor od nebezpečných stránek, ale také identifikovat další články v řetězu. Z tohoto přístupu pak mohou profitovat i další projekty, které mohou naše zjištění využívat pro své vlastní účely.

Na požádání potom poskytujeme držitelům domén pomoc s analýzou a řešením incidentu. V případě zájmu je také možnost zadat otestování odolnosti webové prezentace na dané doméně službou Skener webu.

AKTUÁLNĚ Z BEZPEČNOSTI

V roce 2015 bylo publikováno celkem 383 novinek. Pokles počtu novinek oproti předchozímu roku je způsoben rozšířením spolupráce s odborným internetovým časopisem root.cz. Díky této spolupráci byla část novinek přesunuta do formy pravidelného seriálu Postřehy z bezpečnosti, což nám umožnilo se v rámci AZB více zaměřit na praktické informace z oblasti bezpečnosti, zatímco do seriálu Postřehy z bezpečnosti jsme přesunuli doplňkové informace, které dokreslují celkovou situaci na poli bezpečnosti a jsou zajímavé především pro bezpečnostní komunitu.

AZB se tak mohlo ještě více zaměřit na praktické informování uživatelů i odborné IT veřejnosti o nových útocích (například pokračující phishingové kampaně), o nových zranitelnostech používaných produktů, či o doporučeních ohledně bezpečného nastavení serverů i aplikací.

Za nejdůležitější aspekt AZB považujeme rychlé šíření informací o aktuálně probíhajících útocích a objevených zranitelnostech. Sekce AZB se stala 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.

SLUŽBA SKENER WEBU

V polovině roku 2013 jsme spustili novou službu, kterou jsme nazvali **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 zabezpečení, 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 a v roce **2015** již **135**. **Jedná se tedy o více než čtyřnásobný nárůst aktivit v této oblasti od spuštění služby**. Pro tyto prezentace jsme v roce 2015 vydali celkem 972 doporučení ohledně nalezených zranitelností, nebo možností vylepšení bezpečnosti pomocí různých doplňkových hlaviček protokolu HTTP a nastavení webových serverů.

Největší objednávky tvořilo v tomto roce testování 29 webů Ministerstva životního prostředí a k němu přidružených organizací a dále testování finalistů soutěže školních webů sCOOL web.

Při provádění testů pracujeme kromě jiného také s metodikou neziskové organizace OWASP, která se zaobírá problematikou webové bezpečnosti.

V rámci poskytování služby jsme také několikrát prezentovali důležitost zabezpečení webových aplikací a výskyt nejčastějších bezpečnostních nedostatků, které získáváme z provozu služby Skener webu.

Honeypoty

Jak už bylo zmíněno v části o incidentech, tento rok jsme se soustředili na rozvoj provo Jak už bylo zmíněno v části o incidentech, tento rok jsme se soustředili na rozvoj provozovaných honeypotů. Honeypot je služba, která se snaží přilákat útočníky díky záměrně chybnému bezpečnostnímu nastavení, které umožní zdánlivé ovládnutí simulovaného zařízení. Výstupy z našich honeypotů jsou k dispozici na adrese https://honeymap.cz/.

V roce 2015 jsme rozšířili portfolio provozovaných honeypotů o takzvaný vysoce interaktivní honeypot. Tyto honeypoty na rozdíl od běžných honeypotů obsahují kompletní funkce simulovaného operačního systému. Díky tomu je pro útočníka hůře rozpoznatelný a ani zkušený útočník nemusí poznat, že se místo na skutečném serveru ocitl v simulovaném prostředí. Tento druh honeypotů také umožňuje nacházet v sítích řídící servery botnetů. Nám v roce 2015 přinesl především nové vzorky malware a nové poznatky o chování útočníků.

Druhou novinkou na poli honeypotů v národním CSIRT je jejich distribuce do lokací mimo Českou republiku, konkrétně do lokací San Jose, Londýn, Frankfurt, Tokio (Heiwajima) a Sydney. Díky tomu získaly informace z honeypotů další rozměr, neboť nám například pomohou říci, zda je cílem konkrétního útoku pouze Česká republika, nebo se jedná o útok na více lokalit.

PROKI

V roce 2015 zahájil Národní bezpečnostní tým CSIRT.CZ realizaci nového projektu PRedikce a Ochrana před Kybernetickými Incidenty (PROKI; VI20152020026) podpořeného v rámci Bezpečnostního výzkumu České republiky 2015 – 2020.

V technické oblasti vývoje softwarového řešení projekt sleduje dva hlavní cíle.

Prvním je shromažďování dat o bezpečnostních incidentech z nejrůznějších zdrojů, z nichž část je zcela veřejná a pro přístup k některým dalším je potřeba splnit konkrétní požadavky. V každém případě se jedná o pestrou sbírku informací o IP adresách hostujících C&C servery, phishingové stránky, malware, či informace o IP adresách skenujících sítě v Internetu, nebo o takových IP adresách, na kterých jsou počítače, které jsou naopak do nějakého botnetu zapojeny. Zdaleka ne každá z těchto informací je reportována do sítí, ze kterých problém vzešel a proto jednou z hlavních funkcí PROKI v následujících letech bude souhrnné informování koncových sítí o incidentech, které se jich týkají. Jednou za určitou dobu, (na jejím nastavení aktuálně pracujeme a budeme ji ladit v rámci pilotního provozu v roce 2016) bude správcům příslušné sítě odeslán formátovaný report, ve kterém se dozvědí o všech pozorovaných incidentech, které se v daném období vztahovaly k jejich síti.

Druhým cílem je funkcionalita, která představuje prohledávání incidentů podle zadaných parametrů, které nám umožní podívat se na incidenty a především souvislosti mezi nimi z dalších úhlů pohledu. Incidenty bude možné filtrovat podle IP adresy, konkrétních adresních bloků, země „původu", portů, počtu opakování incidentů a dalších parametrů. V dalších fázích pak plánujeme přidat možnost detailního pohledu na IP adresu. V takovém náhledu se pak dotáhnou doplňková data z dalších zdrojů, jako jsou různé IP reputační databáze, databáze Virustotal, nebo například systém PassiveDNS.

PROKI nebude jen nástrojem pro vyhledávání nových pohledů na existující data. Slibujeme si od něj i rychlejší odhalování nových C&C serverů, phishingových stránek, stránek šířících malware a dalších problémů a to právě díky propojení s dalšími nástroji. Tyto nástroje nám mohou například říci, kam nyní směřuje doména, která ještě před pár dny směřovala na IP adresu, která již byla identifikována jako problematická a tím nám ukázat, kam byl škodlivý obsah přesunut. Kromě toho bude PROKI udržovat i historii problémů na jednotlivých IP adresách a umožní tak například vystopovat sítě, které se zaměřují na poskytování služeb kyberzločincům.

V roce 2015 probíhaly analýzy existujících řešení a na základě jejich výsledků bylo navrženo nejvhodnější možné řešení. Ke konci roku 2015 bylo na základě toho připraveno prostředí, které slouží k ověření životaschopnosti navrženého řešení.

Nedílnou součást projektu bude dále představovat efektivní systém pro hlášení kybernetických bezpečnostních incidentů dle § 8, zákona č. 181/2014 Sb., jejich vyhodnocení a předání NBÚ.

Součástí projektu bude též systém pro efektivní správu kontaktních údajů poskytovaných národnímu bezpečnostnímu týmu CSIRT.CZ nebo provádění pravidelného roční hodnocení hrozeb a rizik pro oblast kybernetické bezpečnosti na národní úrovni, a to jak na základě informací a dat zjištěných v rámci systému (poloprovozu) Cyber Threat Intelligence, tak aktuálních poznatků ze zahraničí. V této souvislosti byly výstupy projektu využity též pro zpracování této zprávy, která v souladu s cíli projektu poskytuje hodnocení kybernetických hrozeb v ČR a jejich predikci.

Osvětová činnost

V průběhu roku 2015 jsme uspořádali celkově **deset kurzů** z cyklu školení **„Počítačová bezpečnost prakticky"**, které je určeno především pro členy **bezpečnostních složek České republiky**. Těchto kurzů se pravidelně účastní zaměstnanci PČR a dalších institucí, kteří se zabývají kybernetickým zločinem a bezpečností. Uvedeným subjektům nabízíme speciální ceny daných kurzů.

Spolupráce s bezpečnostními složkami v uvedeném roce probíhala 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 a podobně.

Dále jsme připravili a realizovali **sedm běhů** školení na základě požadavku Institutu pro veřejnou správu Praha. Tématem tohoto školení určeného pro zástupce ministerstev a dalších ústředních orgánů státní správy byly především **technické aspekty implementace ZKB a Vyhlášky č. 316/2014 Sb., o kybernetické bezpečnosti**. V rámci školení jsme se v souladu s potřebami účastníků školení zaměřili především na využití open source řešení. Školení bylo velmi dobře hodnoceno.

Další zajímavou aktivitou jsou **semináře**, v nichž se členové bezpečnostních týmů mohou seznámit s důležitými pojmy z oblasti práce bezpečnostních týmů, s vhodnými nástroji, ale také s požadavky, které jsou na bezpečnostní týmy kladeny.

I v tomto roce probíhala intenzivní spolupráce s Národním centrem bezpečnějšího internetu (NCBI) a to především formou prezentací a účastí na akcích pořádaných NCBI a formou spolupráce na technickém řešení používaném NCBI pro provoz horké linky (tzv. hot-line) určené pro oznamování nelegálního on-line obsahu.

Cílem této spolupráce je zlepšení schopností, znalostí a dovedností uživatelů v oblasti bezpečného užívání výpočetní techniky a on-line služeb Internetu, dále také zvýšení povědomí uživatelů o práci týmů typu CERT/CSIRT, či vzájemný přenos informací a zkušeností. Zdrojem informací pro tyto prezentace jsou osobní zkušenosti a samotný proces řešení bezpečnostních incidentů, což přináší zajímavý přehled o tom, jaké bezpečnostní incidenty jsou právě aktuální, jakých chyb se uživatelé dopouštějí, proč by se jim měli vyvarovat a také nabízí postup jak toho dosáhnout.

Dále jsme v oblasti osvěty publikovali pět nových návodů pro administrátory i koncové uživatele. V rámci sekce Rady a návody jsme na našich webových stránkách publikovali devět článků zabývajících se bezpečností, další články jsme publikovali též na blogu sdružení CZ.NIC. Další odborné články vycházely na odborných serverech a v odborných časopisech. V rámci odborné literatury jsme přispěli do knihy Bezpečný internet kapitolou o CSIRT týmech. Nedílnou součástí práce CSIRT týmu bylo též informování veřejnosti o aktuálních

bezpečnostních trendech prostřednictvím živých výstupů v rozhlasových a televizních vysíláních. Tým CSIRT.CZ se podílel na přípravě osvětových seriálů Jak na Internet a Lovci záhad.

Ve spolupráci s Národním bezpečnostním úřadem jsme v roce 2015 uspořádali odborné workshopy pro specialisty ze Srbska a Bosny a Hercegoviny.

Národní a mezinárodní spolupráce

Národní a mezinárodní spolupráce představuje nedílnou a povinnou součást činnosti každého pracoviště typu CERT/CSIRT. 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[1], 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 Visegrádské čtyřky a Rakouska. V roce 2015 bylo předsedající zemí této platformy Maďarsko.

V roce 2015 se náš tým stal jako první CSIRT tým v České republice členem mezinárodní organizace CSIRT týmů FIRST. To přináší řadu výhod, mezi které spadá například lepší výměna informací, rozšířený přístup do celosvětové databáze CSIRT týmů nebo přednostní informace o závažných zranitelnostech.

Každý tým ucházející se o členství v organizaci FIRST musí projít externím auditem, realizovaným zástupci některého z členských CSIRT týmů. Vstup do organizace FIRST tak pro nás zároveň znamenal potvrzení správnosti a bezpečnosti našich interních procesů.

V roce 2015 se CSIRT.CZ postavil do čela projektu „Cyber Security in the Danube Region" (CS Danube), spolufinancovaného Evropskou komisí v rámci programu START. Cílem tohoto projektu, do něhož jsou zapojeny vedle České republiky týmy CSIRT/CERT z Rakouska, Slovenska, Moldavska a Srbska je především posilování vzájemné důvěry a odborných kapacit včetně sdílení informací o používaných nástrojích. V rámci projektu byla realizována dvě společná setkání zaměřená na výměnu zkušeností a další vzdělávání CSIRT týmů. Velký důraz byl kladen na analýzu malware a testování bezpečnosti webových prezentací.

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 kybernetickou bezpečností. Pro všestrannou podporu této spolupráce organizujeme pracovní skupinu CSIRT.CZ, účastníme se pracovní skupiny E-CRIME, spolupracujeme s platformami AFCEA, s Českou bankovní asociací a dalšími významnými organizacemi. V roce 2015 jsme také v rámci služeb nabízených na národní úrovni realizovali zátěžové testy[2] na DDoS útoky DDoS útoky pro společnost ČD – Telematika.

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

2 http://www.cdt.cz/cz/cd---telematika-uspesne-prosla-zatezovymi-testy-odolnosti-proti-ddos-utokum-1130/

PRACOVNÍ SKUPINA CSIRT.CZ

Pracovní skupina CSIRT.CZ se uskutečnila ve své velké formě na počátku roku 2015, v půlce roku 2015 se pak uskutečnilo ještě setkání určené pouze pro členy CSIRT týmů z České republiky.

V lednové pracovní skupině se řešil aktuální stav aktivit v oblasti bezpečnosti v České republice, aktivity v oblasti sdílení zajímavých informací typu bezpečnostní incident, bezpečnostní událost, zranitelnosti, či hrozby a také reportování bezpečnostních událostí a incidentů. Pracovní skupina především ocenila zajímavou přednášku na téma greylistů vznikajících v rámci projektu Turris a také přednášku zástupce společnosti O2, který se s bezpečnostní komunitou podělil o zkušenosti s nasazováním řešení proti spamu.

Cvičení

V roce 2015 jsme se, stejně jako v předchozím roce, zúčastnili čtyř cvičení. Každé cvičení bylo zaměřeno na trochu jinou oblast práce bezpečnostních týmů a potkávali se v nich pracovníci z různých úrovní řízení a s různými kompetencemi. Tento fakt nám přinesl mnoho zkušeností a rovnoměrné rozdělení procvičovaných oblastí mezi členy týmu.

STRATEGIC DECISION MAKING COURSE & EXERCISE ON CYBER CRISIS MANAGEMENT

Toto cvičení bylo uspořádáno Národním bezpečnostním úřadem (NBÚ) ve spolupráci s European Cyber Security Initiative (ECSI) a European Defence Agency (EDA). Cílem cvičení, které se uskutečnilo v sídle NBÚ v Praze, bylo formou table-top prověřit schopnosti státu činit rozhodnutí a účinně používat dostupné prostředky při řešení krize v kybernetickém prostoru. Během akce byly procvičeny především komunikační kanály a spolupráce při řešení kybernetických bezpečnostních incidentů mezi čtyřmi základními sektory:

(1) vládou a dalšími exekutivními složkami,
(2) armádou a zpravodajskými službami,
(3) policejními složkami a státním zastupitelstvím,
(4) soukromým sektorem.

Za tým CSIRT.CZ se cvičení účastnili dva zástupci.

CVIČENÍ CYBER CZECH 2015

Cvičení probíhalo formou praktické simulace na speciálně přizpůsobených strojích s cílem čelit kybernetickým útokům a řešit vzniklé události a incidenty. Cílem cvičení bylo procvičit technické schopnosti a sdílení informací mezi jednotlivými týmy. Cvičení bylo založeno na předem připraveném scénáři odrážejícím reálné incidenty a aplikaci ZKB. Tohoto cvičení se zúčastnil zástupce našeho týmu v roli pozorovatele.

CVIČENÍ NATO CYBER COALITION 2015

V rámci cvičení Cyber Coalition 2015 se členové CSIRT.CZ podíleli na vysoce technických úkolech – analýze USB Flash disku, paměti počítače či ransomware. Toto cvičení pro nás bylo významné a velmi přínosné díky možnosti blíže nahlédnout do procesů činností a fungování těch nejdůležitějších bezpečnostních složek státu.

KOMUNIKAČNÍ CVIČENÍ PLATFORMY CECSP

Cílem tohoto cvičení bylo především otestovat funkčnost komunikace mezi bezpečnostními týmy zapojenými do spolupráce v rámci platformy Central European Cyber Security Platform.

Závěr

Rok 2015 přinesl našemu týmu nové výzvy v podobě požadavků na fungování týmu definovaných v rámci ZKB, ale také v podobě dalšího začleňování našeho týmu do mezinárodních struktur (FIRST), nebo spuštění nových výzkumných projektů (PROKI). Z tohoto důvodu došlo v průběhu roku 2015 k vytvoření a obsazení tří nových pracovních pozic. Toto personální posílení nám umožnilo zvládnout všechny aktuální výzvy roku 2015 a zároveň se zabývat dalším rozvojem a vzájemným propojováním našich služeb.

Velice nás také těší, že se nám podařilo udržet výbornou kvalitu služeb poskytovaných v oblasti prevence a vzdělávání našimi stránkami, ať již hovoříme o AZB, nebo o sekci Rady a Návody. Dobře nastavená spolupráce s odbornými médii, především pak se serverem root.cz a rozšíření námi nabízených školení, o která odborná veřejnost projevila velký zájem, pomáhá zvyšovat celkové povědomí o bezpečnostních hrozbách a ochraně před těmito hrozbami a to jak mezi odbornou veřejností, tak také mezi běžnými uživateli.

Vystupování na konferencích, či spolupráce na osvětových seriálech České televize pak vhodně doplňují naši komplexní strategii pro oblast vzdělávání a osvěty.

Tento rok se nám také podařilo rozšířit využití již provozovaných služeb tak, aby se tyto služby mohly bez problémů stát pevným základem, na němž budeme moci i nadále stavět úspěšné projekty. V této oblasti především počítáme s využitím dat ze služeb, na jejichž dalším zlepšování jsme v roce 2015 pracovali. Honeypoty, proces řešení incidentů i Malicious Domain Manager nám nyní poskytují data, která budeme v budoucnu moci využít v rámci naší práce na projektu PROKI.

V roce 2015 také došlo k dalšímu rozšíření komunity bezpečnostních týmů v České republice. Nyní zde tedy formálně existuje 22 CSIRT týmů, oficiálně konstituovaných u úřadu Trusted Introducer a rozvoj bezpečnostní komunity v rámci České republiky i nadále zůstává jednou z priorit našeho týmu.

Z výše uvedeného je patrné, že se nám v roce 2015 podařilo navázat na úspěchy z předchozích let a hodnotíme tedy uplynulý rok jako velice zdařilý.