ZPRÁVA O ČINNOSTI CSIRT.CZ (NÁRODNÍHO CSIRT ČR) ZA ROK 2016

CSIRT.CZ

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 podepsalo 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 uzavřelo 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 2016 v kostce

Začátkem roku 2016 jsme se soustředili na hostování TF-CSIRT/FIRST meetingu, čímž jsme chtěli umožnit již početné české komunitě týmů CSIRT zúčastnit se této, pro bezpečnostní týmy důležité akce, osobně. Druhým důležitým úkolem, se kterým vstupoval CSIRT.CZ do roku 2016, bylo získání prověrky na stupeň vyhrazené. Splněním tohoto bodu byl naplněn požadavek veřejnoprávní smlouvy uzavřené mezi sdružením CZ.NIC a Národním bezpečnostním úřadem.

V roce 2016 se zastavil trend prudkého nárůstu počtu incidentů, reportovaných týmu CSIRT.CZ a jejich počet, oproti předešlému roku, dokonce drobně poklesl. Stále však narůstá komplexnost incidentů a počet zainteresovaných IP adres. To se týká především incidentů typu DoS/DDoS či Botnet, ale v omezené míře i některých dalších. Právě u incidentů typu Botnet došlo v uplynulém roce k tak velkému nárůstu, že si to vyžádalo i vytvoření nového nástroje Convey. Tento open-source nástroj byl následně zpřístupněn celé komunitě, jak je již u projektů CSIRT.CZ zvykem. V souvislosti s řešením incidentů došlo v minulém roce také k revizi práce s incidenty.

V průběhu roku 2016 jsme také rozšířili naše služby o sledování volně dostupných informačních zdrojů, na jejichž základě jsou informováni držitelé doménových jmen v zóně .cz, pokud byl na jejich stránkách útočníky proveden defacement, tedy změna obsahu webové stránky.

I nadále jsme se zabývali také naší osvětovou a vzdělávací rolí, kdy jsme pokračovali v nastolené spolupráci se zpravodajským serverem root.cz, kde se tým CSIRT.CZ spolupodílí na tvorbě populárního seriálu Postřehy z bezpečnosti. Kromě toho jsme i nadále publikovali informace o novinkách v oblasti bezpečnosti pod názvem Aktuálně z bezpečnosti. Kromě již zavedených školení, o fungování CSIRT týmů nebo kurzu počítačová bezpečnost prakticky, byly také realizovány dva běhy školení pro neziskové organizace a novináře. Z dalších osvětových a vzdělávacích aktivit stojí za zmínku zapojení týmu CSIRT.CZ do workshopů a přednášek spojených s akcí Říjen – Evropský měsíc kybernetické bezpečnosti nebo podpora a účast na projektu středoškolské soutěže zaměřené na problematiku bezpečnosti v kyber prostoru. Více o aktivitách v oblasti osvěty a vzdělávání lze zjistit v příslušné části tohoto dokumentu.

CSIRT.CZ se i v uplynulém roce věnoval preventivní činnosti. V roli koordinátora se podílel na testování hostingových společností poté, co se ukázalo, že některé velké české hostingové

společnosti trpí starou, avšak nebezpečnou zranitelností týkající se session managementu ve sdíleném hostingu.

Již tradičně jsme rozesílali informace o ohrožení konkrétních systémů, ať se jednalo o informaci o kompromitovaných serverech distribuovanou ve spolupráci s vládním pracovištěm govCERT, nebo o upozornění na různé zranitelná, či špatně konfigurovaná zařízení. Pokračovali jsme také v zasílání dosud neznámých vzorků malware antivirovým společnostem.

Také v roce 2016 rozvíjel CSIRT.CZ spolupráci s partnery na národní i mezinárodní úrovni. Na národní úrovni jsme navázali úzkou spolupráci s odborem kybernetické kriminality Národní centrály proti organizovanému zločinu služby kriminální policie a vyšetřování a to jak ve školení jejich specialistů, tak při řešení konkrétních případů. Dvakrát jsme také zorganizovali pracovní skupinu CSIRT.CZ, pokračovali jsme v nastolené spolupráci s ČBA a podíleli se na připomínkování novely zákona o kybernetické bezpečnosti, včetně spolupráce na tvorbě vyhlášky k novele.

V rámci mezinárodní spolupráce jsme se podíleli na již zmiňovaném hostování TF-CSIRT/FIRST meetingu, připomínkování směrnice k bezpečnosti sítí a informačních systémů v Unii (NIS) direktivy, či na připomínkování návodu pro národní regulátory v oblasti elektronických komunikací (BEREC) pro implementaci síťové neutrality. Také jsme v rámci projektu CS Danube pořádali mezinárodní konferenci a hostovali školení ENISA. CSIRT.CZ se také zapojil do aktivit CSIRT Network vycházející z NIS.

I nadále jsme pokračovali v práci na projektu PROKI a kromě toho se členové týmu také zapojili do aktivit v projektu Safer Internet, na jehož běhu se sdružení CZ.NIC od roku 2016 podílí. V tomto projektu se nám podařilo uplatnit naše zkušenosti z řešení incidentů a z oblasti osvěty.

Rok 2016 hodnotíme jako úspěšný, podařilo se nám i nadále zvyšovat kvalitu nabízených služeb, rozvíjet existující projekty, zapojit se do řízení významné mezinárodní platformy a přispět bezpečnostní komunitě skrze vlastní open-source projekty i skrze spolupráci na mezinárodním projektu IntelMQ.

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 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 původce 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 a je tedy nutné, aby

se informace tohoto typu co nejrychleji dostaly k těm, kdo mohou zasáhnout a nastavit například vhodné metody obrany apod.

(4) problémy plošného rozsahu, například počítače v Botnetu, zařízení s konkrétní zranitelností, zjednodušeně řečeno informace od zahraničních partnerů týkající se více sítí v ČR.

V roce 2016 došlo poprvé v historii CSIRT.CZ k mírnému poklesu množství řešených incidentů. Zatímco v roce 2015 bylo řešeno 1160, v roce 2016 to bylo celkem 1121. Meziročně však opět přibylo incidentů, které vyžadují hlubší analýzu a komplexní řešení. Jeden incident typu Botnet, či DDos si obvykle vyžádá velké množství odeslaných zpráv. V uplynulém roce tak CSIRT.CZ odeslal celkem 6527 zpráv a to především díky nárůstu incidentů typu Botnet z 2 v roce 2015 na 71 v roce 2016.

Právě nárůst komplexnosti incidentů, co do počtu zainteresovaných sítí, vedl tým CSIRT.CZ k vytvoření a publikování open-source nástroje Convey. Tento nástroj umožňuje automatizované zpracování rozsáhlých incidentů a automatizované rozesílání adekvátních částí hlášení do příslušných sítí. V současné verzi je tento nástroj schopen pracovat s tiketovacím systémem OTRS. V průběhu roku 2017 bychom jej rádi upravili do podoby, kdy bude poskytovat výstup do univerzálního formátu CSV.

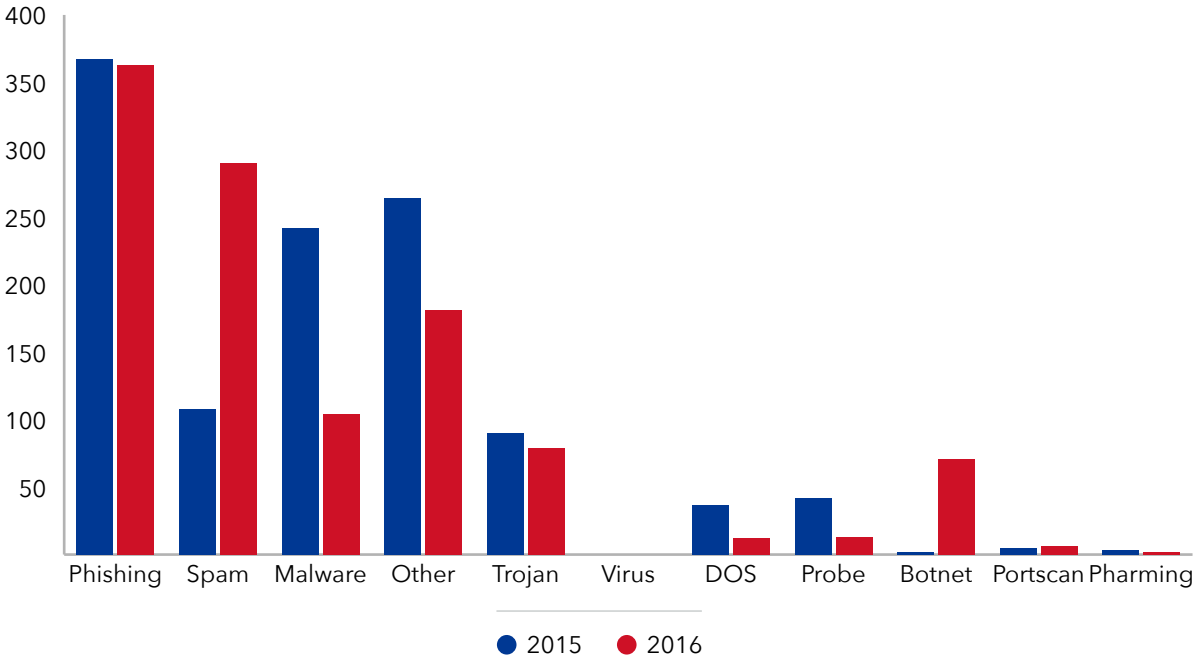
STATISTIKA PROCESU ŘEŠENÍ BEZPEČNOSTNÍCH INCIDENTŮ TÝMEM CSIRT.CZ:

	2008	2009	2010	2011	2012	2013	2014	2015	2016	**Celkem**
IDS	0	0	0	491	3 924	2 121	2 380	3 771	9 944	**22 631**
Phishing	65	220	209	144	159	175	368	367	363	**2 070**
Spam	47	28	103	26	43	73	159	108	290	**877**
Malware	53	134	121	10	20	45	117	240	104	**844**
Other	1	5	13	62	14	75	102	264	181	**717**
Trojan	66	6	26	5	5	12	56	90	79	**345**
DOS	2	4	2	2	68	72	32	37	12	**231**
Probe	0	3	14	25	12	26	86	42	13	**221**
Virus	0	84	99	0	0	0	0	0	0	**183**
Botnet	0	3	46	5	8	15	0	4	71	**152**
Portscan	10	4	1	6	1	3	2	5	6	**38**
Pharming	0	0	0	0	0	0	18	3	2	**23**
Celkem	**244**	**491**	**634**	**776**	**4 254**	**2 617**	**3 320**	**4 931**	**11 065**	**28 332**

Do celkového počtu řešených bezpečnostních incidentů se nezapočítávají incidenty typu IDS, které jsou uvedeny ve druhém řádku výše uvedené tabulky. Systém pro detekci neoprávněného přístupu do systému IDS (Intrusion Detection System) slouží k zachycování informací o strojích, ze kterých byly zaznamenány pokusy o připojení. IDS pracuje na platformě LaBrea,

která je distribuována pod licencí GPL. LaBrea využívá adresových bloků, které v Internetu dosud nebyly použity, což znamená, že na nich neexistovaly žádné uživatelské stroje. K takovým adresám nemá „zdravý" stroj důvod se připojit. Systém předstírá, že na těchto adresách běží funkční zdroje, a reaguje na pokusy o připojení přes TCP a ICMP echo (ping). Uvedený počet incidentů za rok 2016 tedy představuje počet varování zaslaných touto službou správcům koncových sítí provozovaných v ČR.

POČTY VYBRANÝCH BEZPEČNOSTNÍCH INCIDENTŮ HLÁŠENÝCH TÝMU CSIRT.CZ V LETECH 2015 A 2016:



ZAJÍMAVÉ KAUZY ROKU 2016

Jak již bylo řečeno v úvodu, i v roce 2016 pokračoval trend nárůstu incidentů, ve kterých bylo zainteresováno více subjektů. Typickými představiteli jsou incidenty typu DDoS nebo incidenty typu Botnet. Mezi incidenty tohoto typu patřil například DDoS amplification útok, k němuž byly zneužity NTP servery na 395 unikátních IP adresách nebo rozesílání informací o klientech botnetu DRIDEX, které zahrnovalo 1672 unikátních IP adres.

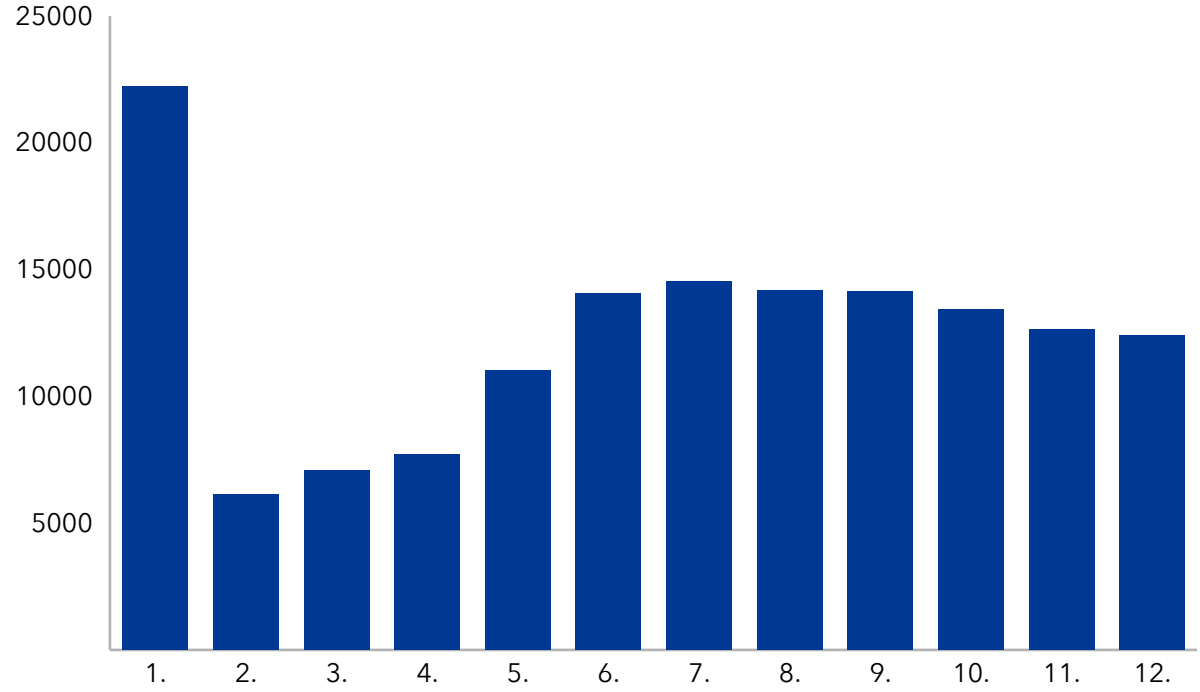
Jiným příkladem incidentu zahrnujícím velké množství uživatelů byla kompromitace více než 5000 e-mailových schránek, jejichž seznam obdržel CSIRT.CZ od vládního CERT a které byly ukradeny z jednoho českého portálu. V tomto případě jsme informaci o kompromitovaných účtech poslali držitelům jednotlivých doménových jmen, kteří tak měli možnost upozornit příslušné uživatele bezpečnou cestou.

Poněkud netradičním incidentem byl neúmyslný DoS, který byl způsobený chybnou konfigurací na straně spam listu UCEPROTECT a který se týkal společností, jejichž autonomní systém má vyšší číslo než 16 bitové délky. Z důvodu zpětné kompatibility vidí systémy podporující pouze 16bitová čísla autonomních systémů, nová 32bitová ASN jako v minulosti rezervované číslo AS 23456. To v případě výše zmiňovaného spam listu vedlo k neoprávněnému hromadnému blokování všech IP adres z autonomních systémů, které byly spam listem vyhodnoceny jako AS 23456. Po naší intervenci byl problém na straně UCEPROTECT odstraněn.

Ve spolupráci s PČR jsme se zabývali analýzou jednoho velkého DDOS útoku nebo jsme řešili zablokování podvodného e-shopu, který cílil na české uživatele. Ten byl umístěn v doméně .com a hostován v zahraničí. Podvodný e-shop byl na základě naší intervence odstaven během několika hodin.

SLUŽBA MDM (MALICIOUS DOMAIN MANAGER)

V rámci služby MDM využíváme především veřejně dostupné zdroje informující o doménách s webovými prezentacemi, které byly napadeny a jsou pak útočníky zneužívány k phishingovým útokům či šíření malware. Pomocí této služby jsou tedy vytěžována data z veřejných zdrojů a následně přeposílána osobám zodpovědným za chod napadené domény, s žádostí o prošetření a případnou nápravu situace.



V roce 2016 byla služba MDM rozšířena o novou aktivitu. Z veřejně dostupných internetových fór získáváme informace o webových stránkách, které se staly obětí takzvaného defacementu. Ten může mít různé projevy, od snahy útočníka pochlubit se svými schopnostmi, až po propagaci extrémistických postojů a teroristických organizací.

Příklady defacementu na řešených doménách:

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

AKTUÁLNĚ Z BEZPEČNOSTI

V roce 2016 bylo publikováno celkem 230 novinek. Díky pokračující spolupráci se serverem root.cz jsme se mohli v AZB i nadále soustředit na praktické informace z oblasti bezpečnosti, zatímco v seriálu Postřehy z bezpečnosti na serveru root.cz jsme publikovali rozšiřující informace, které dokreslují celkovou situaci na poli bezpečnosti a jsou zajímavé především pro odbornou komunitu.

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

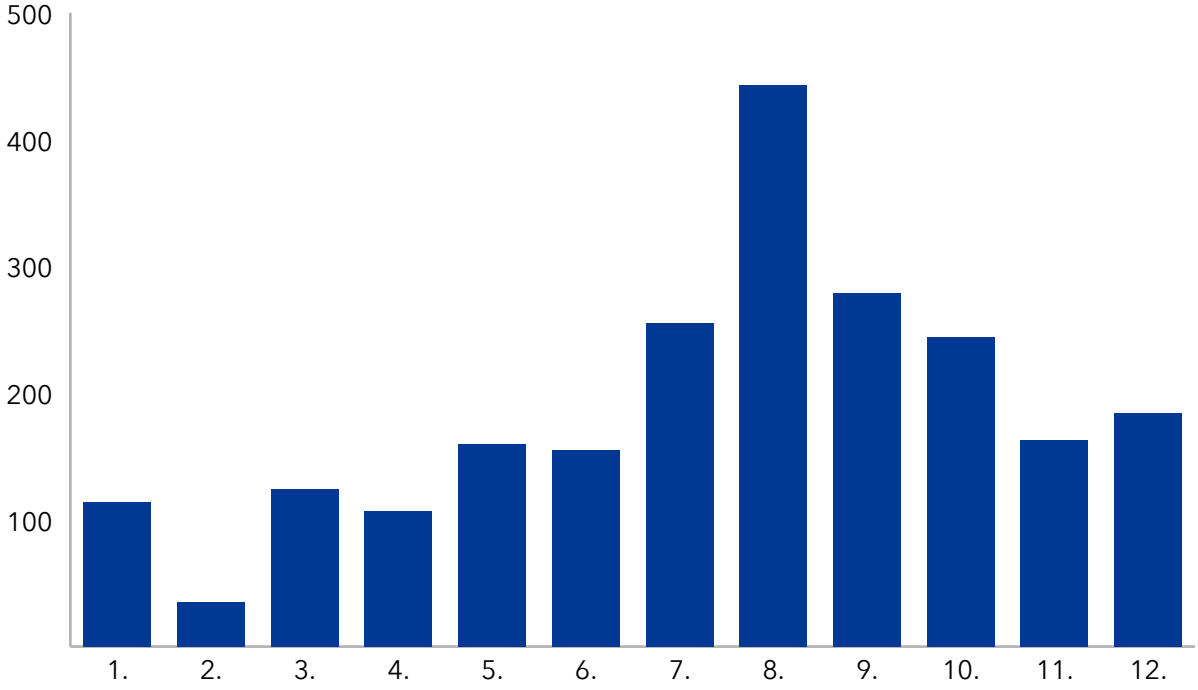
Služba Skener webu byla spuštěna v roce 2013 s cílem zvýšit povědomí o možnostech lepšího zabezpečení webových stránek. Nadále testujeme webové aplikace přes automatizované nástroje, jejichž výsledky jsou pak doplněny o ruční testy. V roce 2016 jsme k sérii automatizovaných nástrojů přidali Focu, která analyzuje metadata z dokumentů Open Office, PDF či Wordu. Daný nástroj nám umožňuje zjistit, či se na webovém serveru nenacházejí dokumenty, které by neměly být veřejně dostupné. Pro kontrolu výsledné závěrečné zprávy z testování a její případné doplnění je ruční testování vykonané ještě jednou dalším členem týmu. Celkově pracují na službě tři členové týmu, avšak každý z nich má kromě této služby taky jiné povinnosti.

Rok 2016 se, co se týče počtu objednávek a otestovaných webů, příliš nelišil od roku 2015. Způsoby zaslání objednávky byly v roce 2016 rozšířeny o možnost zaslat objednávku přes datovou schránku. Spolu s elektronicky podepsaným mailem to byl nejčastější způsob jak nám byla objednávka na službu Skener webu doručena. Způsob zaslání objednávky přes datovou schránku využívaly hlavně státní a veřejné instituce. Menší weby a soukromé osoby většinou využívali možnost zaslání objednávky přes validovaný účet mojeID. Jenom dva žadatelé využili možnost zaslání úředně ověřené objednávky písemnou formou. Celkově jsme v roce 2016 obdrželi 44 objednávek na testování. Počet webů na jednu objednávku se pohyboval mezi jedním až jedenácti. Celkově jsme otestovali 89 různých webových aplikací.

Honeypoty

I v uplynulém roce jsme využívali informace získané z námi provozovaných honeypotů. V roce 2016 jsme zaznamenali 5109 unikátních vzorků malware, z nichž 2263 nebylo do té doby testováno platformou VirusTotal a 41 vzorků jsme díky navázané spolupráci předali k dalšímu zkoumání společnosti Avast.

KIPPO, POČTY NOVÝCH VZORKŮ MALWARE (TAKOVÝCH, KTERÉ NEBYLY NA VIRUSTOTAL.COM). CELKEM 2263:



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 stroje zapojené do některého z botnetů.. 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, 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.

V roce 2016 začala implementační fáze projektu PROKI. V rámci této fáze jsme se aktivně zapojili do vývoje komponent mezinárodního projektu IntelMQ, který je v rámci PROKI

využíván. Jednalo se o komponentu Turris Greylist parser, která umožňuje získávat informace o útočnících přistižených při napadání nebo agresivním skenování sítí s routery Turris (tedy většiny sítí v ČR). Data považujeme za velmi relevantní pro projekt PROKI, protože dokumentují útočníky aktivní směrem do sítí v ČR a zároveň útočníky, kteří útočí z IP adres v ČR.

Další komponentou vyvinutou týmem CSIRT.CZ v rámci projektu PROKI je Generický CSV parser. Implementovali jsme univerzální parser CSV souborů, který se řídí pouze předanou konfigurací a poradí si se všemi nám známými zdroji v tomto formátu. Zvládá zpracovat i nestandardní data, jako jsou specifické oddělovače, komentáře, hlavičky, apod. IntelMQ komunita parser převzala z vývoje PROKI zpět do hlavního proudu vývoje IntelMQ a podle našich zpráv se jedná o velmi používaný modul. V našem týmu zkrátil definici zpracování nových dat z řádu hodin na minuty. To umožňuje testovat a vyhodnocovat více zdrojů dat.

Abusix expert je dalším modulem vyvinutým pro projekt PROKI a umožňuje pro danou IP adresu získat příslušný emailový kontakt určený pro hlášení incidentů. Abychom zbytečně nezatěžovali servery společnosti Abusix, kterých se modul dotazuje, je v modulu implementována cache, která slouží k vyřízení identických dotazů přímo na úrovni IntelMQ, aniž by docházelo k jejich zasílání ven ze systému.

IntelMQ nabízí pro filtraci zpracovávaných dat (událostí) vlastní filtrační modul. Pro definici výjimek, specifických úprav a testování jsme ale potřebovali výrazně komplexnější nástroj. Modul Custom filter jsme vytvořili za účelem definice vlastních výjimek a úprav událostí tak, aby byla upozornění odeslána pouze správným adresátům.

Komponenta mailer je zodpovědná za rozesílání emailů sestavených z výstupu systému IntelMQ. Abychom do posloupnosti zpracování nepřidávali další mezikrok ve formě databáze nebo jiného úložiště, pracuje mailer přímo s událostmi z IntelMQ a je připraven jako nezávislý modul.

Do testovací fáze projektu se zapojili významní poskytovatelé hostingových služeb i ISP působící v České republice. V rámci testování jsme také rozesílali informace držitelům IP adres s nejvíce „podezřelým" chováním. Reakce, které jsme obdrželi ukazují, že projekt PROKI dokáže, díky své analytické části, odhalit problémy v sítích včetně řídících serverů botnetu, napadených webových prezentací nebo infikovaných koncových klientů.

Dalším z cílů projektu PROKI je 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.

Osvěta a vzdělávaní

V rámci školení jsme využili možnosti školení v Akademii CZ.NIC. Celkově jsme ve spolupráci s akademií realizovali 3 různá školení. Jednalo se o kurz Počítačová bezpečnost prakticky, Základy fungování CSIRT týmu a školení pro neziskové organizace ohledně bezpečného používání internetu se zaměřením na specifické potřeby a problémy neziskových společností. V rámci vzdělávání jsme také prezentovali pro studenty Policejní akademie České republiky či ve stejné instituci pro policisty v rámci kurzů celoživotního vzdělávání. Za zmínku stojí také workshop zabývající se různými aspekty bezpečnosti uskutečněný na míru pro Agenturu pro regionální rozvoj.

Kromě školení se členové CSIRT.CZ věnovali také přednášení v rámci mnoha různých akcí

a konferencí. Jednalo se o prezentace na setkáních organizací FIRST, TF-CSIRT, ISACA či ICANN či na konferencích Internet a technologie, Security training camp, CS Danube a řadě dalších.

V roce 2016 jsme se významněji podíleli také na publikační činnosti. Snažili jsme se pokrýt jak tištěná, tak internetová média. Pravidelně jsme publikovali na portálu root.cz (celkově 22 článků), na blogu sdružení CZ.NIC (8 článků) a pak také v IT Systems, Data Security Management či Security World. Několikrát jsme také vystoupili v televizi či v rozhlase a podíleli jsme se na tvorbě scénářů pro naučný seriál Nauč tetu na netu.

V rámci podpory vzdělávaní a osvěty u školou povinné mládeže jsme se zapojili do partnerství Středoškolské soutěže v kybernetické bezpečnosti kde jsme kromě hodnotných darů pomáhali s přípravou otázek do prvního kola soutěže.

V rámci prevence jsem se podíleli také na koordinování řešení starší zranitelnosti, která doposud nebyla řešena několika velkými hostingovými společnostmi. Po nahlášení dané chyby jedním výzkumníkem jsme oslovili 94 společností poskytujících hostingové služby s nabídkou bezplatného otestování na zranitelnost nacházející se v prostředí sdíleného hostingu. 20 společností mělo zájem o testování a 5 společností bylo zranitelných. Zranitelnost se týkala služeb pod PHP se sdíleným úložištěm session cookies. Test byl prováděn třetí stranou a pro hostingové společnosti byl bezplatný.

Národní a mezinárodní spolupráce

V roce 2016 probíhala příprava novely Zákona o kybernetické bezpečnosti která měla reflektovat směrnici Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii (NIS směrnice). V rámci přípravy novely jsme se podíleli na jejím připomínkováním.

V oblasti národní spolupráce jsme vyjádřili podporu pro získání statutu „listed" dalších týmů. Celkově v roce 2016 získali status „listed" v rámci Trusted Introducer čtyři české týmy. V roce 2016 tak počet oficiálních tuzemských CSIRT týmů v rámci služby Trusted Introducer stoupl na 26. Spolu s Německem a Francií tak patří Česká republika i nadále mezi státy s nejvyšším počtem bezpečnostních týmů v Evropě.

Posilování národní spolupráce pravidelně pomáhají také školení v Akademii CZ.NIC a přednášky členů týmu CSIRT.CZ. Nadále pokračujeme také ve spolupráci s Českou bankovní asociací a bližší spolupráci jsme navázali s odborem kybernetické kriminality Národní centrály proti organizovanému zločinu služby kriminální policie a vyšetřování.

V rámci zlepšování mezinárodní a národní spolupráce jsme v lednu 2016 organizovali setkání bezpečnostních týmů sdružených v rámci TF-CSIRT a organizace FIRST. Byla to dobrá příležitost jak zviditelnit sdružení CZ.NIC a tým CSIRT.CZ mezi zahraničními týmy a umožnit početným českým týmům účastnit se tohoto největšího setkání bezpečnostních týmů v rámci Evropského regionu. Kapacita 180 míst byla naplněna na 100 %. České týmy obdržely na tuto konferenci slevové kódy a téměř každý český tým měl na setkání zástupce. Konference se uskutečnila na Fakultě informačních technologií v pražských Dejvicích a trvala tři dny. První dva dny sestávaly z přednášek a třetí den byl věnován praktickým workshopům. Ve stejný den probíhala výše zmíněná Pracovní skupina CSIRT.CZ. Spojení těchto dvou akcí umožnilo pozvání zahraničních přednášejících také na lokální pracovní skupinu.

Velmi náš těší zvolení Zuzany Duračinské, jednoho z členů týmu CSIRT.CZ, do Steering Committee platformy TF-CSIRT. Ta představuje volenou skupinu z komunity bezpečnostních týmů, která kontroluje plnění služeb Trusted Introducer a rozvoj dalšího

fungování skupiny TF-CSIRT. Komunita spojená v této platformě ocenila zvolením našeho zástupce dlouhodobou kvalitní práci týmu CSIRT.CZ v oblasti mezinárodní spolupráce i aktivní účast na setkáních této platformy.

V důsledku schválení NIS směrnice vznikla v minulém roce CSIRT Network. V roce 2016 se uskutečnila první dvě neoficiální setkání této skupiny jejichž cílem bylo především schválení podmínek dalšího fungování této skupiny a agenda, kterou by tato skupina měla řešit aby doplnila již fungující seskupení bezpečnostních týmů. Tým CSIRT.CZ, který bude fungovat jako kontaktní místo pro poskytovatelé digitálních služeb by měl mít v CSIRT Network své zastoupení a proto jsme se aktivně podíleli na tvorbě pravidel podle kterých bude seskupení od roku 2017 oficiálně fungovat.

Pracovní skupiny

V roce 2016 jsme uspořádali dvě pracovní skupiny. V lednu se uskutečnila otevřená pracovní skupina na kterou byli pozváni všichni, který se nachází v mailing listu workgroup-int@lists.nic.cz. Co se týče účasti, šlo zatím o největší pracovní skupinu. Celkem bylo zaregistrováno 86 účastníků. V dopoledních hodinách probíhala otevřená skupina pro zástupce ze všech sektorů a odpoledne byla vytvořena uzavřená skupina sestávající pouze z členů CSIRT týmů. Zástupcům CSIRT týmů byl rozdán dotazník ohledně spokojenosti s fungováním této skupiny, programem samotného setkání a motivací pro větší zapojení jeho členů. Zjistili jsme, že nejvíce účastníků pracuje ve společnosti poskytovatele internetového připojení, přičemž většina z nich má vytvořený také bezpečnostní tým typu CSIRT/CERT. Z přednášek účastníky nejvíc zaujala praktická forenzní analýza malwaru od kolegů z týmu CSIRT.SK a také do budoucnosti by účastníci v programu nejvíce uvítali případové studie a novinky z oblasti bezpečnosti. Další dotazy v dotazníku se týkaly zaměření práce týmu CSIRT.CZ a očekávaných výstupů z projektu PROKI.

Další pracovní skupinu jsme uspořádali v listopadu a šlo o pracovní skupinu pouze pro oficiální CSIRT týmy. Mezi hlavní témata patřila novela Zákona o kybernetické bezpečnosti a související směrnice NIS. Před setkáním jsme zaslali týmům dotazník ohledně spokojenosti se službami Trusted Introducer. Stejný dotazník byl zaslán také všem ostatním týmům se statusem listed v srpnu 2016 a tak jsme mohli jejich výsledky na pracovní skupině prezentovat. Jedním za závěru bylo, že týmy jsou nedostatečně informovány o akcích a fungování služby Trusted Introducer a TF-CSIRT. Tento problém by měl být zčásti vyřešen vytvořením mailing listu u Trusted Introducer, který bude určen speciálně pro CSIRT týmy se statusem listed. Na setkání se přihlásilo 60 lidí, čímž i tato původně menší skupina nabyla velikosti menší konference.

Kybernetická cvičení

Již tradičně jsme se v roce 2016 ujali úlohy národního koordinátora pro cvičení Cyber Europe 2016 pořádaného organizací ENISA. Hlavním úkolem koordinátora je zprostředkovaní cvičení v jednotlivých státech. Naším úkolem bylo pozvání hráčů k účasti na cvičení a jejich organizace. Cvičení Cyber Europe 2016 jsme se účastnili také jako hráči a to jak v části technické, do které byly úkoly zveřejňovány postupně od dubna do října, tak v části technicko-operační která trvala dva dny a v České republice se jí účastnilo 7 týmů. Zastoupený byl soukromý, veřejný a akademický sektor. Vzhledem k rozložení cvičení na několik měsíců bylo řešení úkolů a koordinace cvičení časově náročnější než v předešlých letech.

Další cvičení kterého jsme se účastnili v roli hráče bylo CyberCoalition pořádané mezinárodní organizací NATO. Tým složený z členů CSIRT.CZ, GovCERT, Avastu a kriminální policie analyzoval útoky hackerské skupiny Blueweeder. V první části cvičení byl analyzován zdrojový kód chytré televize. Ta byla nakažena malwarem a špehovala vládní i domácí uživatele po celém kontinentu. V druhé části jsme podrobili zkouškám chytré hodinky, které nahrávaly hovor v místnosti a uploadovaly jej hackerům skrz děravou mobilní aplikaci. Hardware nakažených hodinek i mobilu jsme přitom měli k dispozici.

Dále jsme se v roce 2016 účastnili cvičení NATO Locked Shields 2016 a národního cvičení Cyber Czech 2016.

Závěr

Z výše uvedených informací vyplývá, že se týmu CSIRT.CZ podařilo udržet vynikající kvalitu provozovaných služeb a jejich další rozšiřování. Většina existujících služeb a nástrojů doznala v uplynulém roce nějaké vylepšení či rozšíření. V oblasti reakce na incidenty se jedná o vývoj nástroje Convey či o rozšíření aplikace MDM o rozesílání informací o defacementech. Dále lze zmínit drobná vylepšení ve službě Skener webu, celou řadu komponent vytvořených pro potřeby projektu PROKI, jež jsou však zároveň využívané i ostatními členy bezpečnostní komunity či rozšíření dostupných školení nabízených v rámci spolupráce s akademií CZ.NIC. Kromě těchto úspěchů nás těší, že jsme se v roce 2016 s úspěchem zhostili role národního koordinátora důležitého celoevropského cvičení Cyber Europe.

Kdybychom měli vypíchnout tři nejdůležitější body z uplynulého roku, pak by to bylo zdařilé hostování významného mezinárodního setkání CSIRT týmů, zvolení zástupce týmu CSIRT.CZ do Steering Committee platformy TF-CSIRT a udržení vysoké kvality existujících služeb.