ZPRÁVA O ČINNOSTI CSIRT.CZ (NÁRODNÍHO CSIRT ČR) ZA ROK 2017

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 2017 v kostce

Rok 2017 byl ve znamení turbulentních změn v oblasti právních předpisů, které se činnosti CSIRT nějakým způsobem dotýkají. Tým CSIRT.CZ se zapojil do přípravy a připomínkování novely zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), který vstoupil v platnost dne 1. srpna 2017 a přináší především novinky související s implementací evropské směrnice NIS do českého právního řádu. CSIRT.CZ se také zapojil do připomínkování související vyhlášky o kritériích pro určení provozovatelů základní služeb a byl členem expertní skupiny, která na svých pravidelných setkáních řešila obsah prováděcí vyhlášky k Zákonu o kybernetické bezpečnosti (například o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech hlášení kybernetických incidentů v oblasti kybernetické bezpečnosti či likvidaci dat (vyhláška o kybernetické bezpečnosti)).

Kromě toho se CSIRT.CZ účastnil široké diskuze bezpečnostních týmů o možných dopadech Obecného nařízení o ochraně osobních údajů, známého po zkratkou GDPR na práci bezpečnostní komunity. Abychom posílili povědomí o této problematice mezi bezpečnostními týmy fungujícími v České republice, pozvali jsme do podzimní pracovní skupiny CSIRT.CZ Bernda Fitena ze společnosti Time.Lex, který si pro české bezpečnostní týmy připravil přednášku Legal aspects of data processing by CSIRTs.

I v roce 2017 pokračoval trend představovaný větší komplexností řešených incidentů a větším množstvím IP adres, které byly v incidentu zainteresované. Tým CSIRT.CZ tak například řešil malware Mumblehard, kterým bylo infikováno 2 284 unikátních IP adres, nebo DDoS útok, na němž se podílelo 4 091 unikátních IP adres z celkem 46 zemí. V rámci incident handlingu jsme také na požádání prováděli hlubší analýzu některých incidentů.

V souvislosti s negativním vývojem spočívajícím v narůstající komplexnosti incidentů jsme již v roce 2016 vytvořili nový open-source nástroj Convey, který nám umožňuje poloautomaticky zpracovávat incidenty, ve kterých figuruje více IP adres. V tomto roce jsme pokračovali v úpravách tohoto nástroje, který tak nyní umí pracovat s libovolným SMTP serverem a není již svázaný pouze s jedním tiketovacím systémem. Díky tomu bude nyní využitelnější i v širší

komunitě bezpečnostních týmů. Nástroj je volně dostupný na portálu GitHub a je také zařazen do seznamu nástrojů, které jsou vyvíjené evropskou komunitou bezpečnostních týmů.

Vzdělávací a osvětová činnost je dlouhodobě důležitou součástí služeb poskytovaných naším bezpečnostním týmem, a proto jsme se této oblasti věnovali i v uplynulém roce. Uspořádali jsme celkem pět běhů školení pro zájemce o informace o fungování CSIRT týmů, ve spolupráci s krajem Vysočina jsme uspořádali školení pro zájemce z řad Policie ČR, v rámci Evropského měsíce kybernetické bezpečnosti se konal celodenní seminář pro veřejnost na Jihočeské universitě, zorganizovali dvě setkání Pracovní skupiny CSIRT.CZ, vystupovali jsme na řadě konferencí a v médiích, pokračovali v psaní osvětového seriálu Postřehy z bezpečnosti a také jsme se zapojili do připomínkování scénářů osvětových seriálů pro dětské diváky.

Také v roce 2017 jsme se věnovali prevenci na poli kybernetické bezpečnosti. Kromě již standardní distribuce informací získaných v rámci procesu incident handlingu, případně z vlastní proaktivní činnosti, jsme také zahájili automatickou distribuci informací o incidentech do koncových sítí, kdy jsou tyto informace získávány v rámci provozu systému PROKI.

Kromě toho tým CSIRT.CZ pokračoval v provozování honeypotů, realizoval akci, při které hledal v rámci .CZ domény zranitelné CMS systémy a také zrealizoval jedno penetrační testování pro významného zákazníka z oblasti veřejné správy a dva zátěžové testy odolnosti vůči DoS a DDoS útoků. Další vývoj probíhal i v rámci naší služby Skener webu, kde jsme provedli rozsáhlé testování existujících nástrojů a na jehož základě jsme vybrali nové nástroje pro provádění penetračních testů webových aplikací. Vytvořili jsme také vlastní aplikaci domaincheck, která automatizuje některé často se opakující testy, které museli analytici dosud provádět ručně.

Pokračovali jsme také v úspěšně nastolené spolupráci na národní i mezinárodní úrovni. Kromě již zmiňovaných dvou setkání pracovní skupiny CSIRT.CZ jsme se účastnili setkání CSIRT Network, TF-CSIRT či FIRST. V rámci činnosti ve Steering Committee TF-CSIRT jsme se také zapojili do tvorby strategie, dokumentů pro podporu nových týmů a dalších aktivit. Díky zapojení kolegyně Zuzany Duračinské do školení TRANSITS jsou její dlouholeté zkušenosti z fungování CSIRT.CZ sdíleny s novými členy bezpečnostní komunity. Kromě toho jsme se i v roce 2017 aktivně zapojovali do kybernetických cvičení na národní i mezinárodní úrovni.

V roce 2017 jsme také pokračovali v práci na projektech, do kterých je CSIRT.CZ zapojen. V projektu Safer Internet jsme využili naše praktické zkušenosti z provozování národního bezpečnostního týmu v rámci řešení hlášení přicházejících na STOPonline, ale také při školeních, která jsou v projektu realizována pro žáky základních a středních škol.

Rok 2017 byl náročný, jak kvůli probíhajícím legislativním změnám, tak díky zapojení do nových aktivit a rozšiřování stávajících. I přes některé dílčí problémy se však daří udržovat kvalitu již poskytovaných služeb našeho bezpečnostního týmu a zároveň postupně přidávat další aktivity zvyšující bezpečnost kyberprostoru. Jednotlivé činnosti CSIRT.CZ jsou pak detailněji popsány dále v této zprávě.

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,
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 2017 řešil CSIRT.CZ celkem 1 008 bezpečnostních incidentů. I v uplynulém roce mírně narostl počet e-mailů (z 6 527 v roce 2016 na 6 867 v roce 2017) odeslaných v rámci procesu řešení incidentů. Tento trend je způsobován narůstající komplexností incidentů, kdy do jednoho incidentu je často zapojeno více různých stran, které je v rámci řešení incidentu potřeba oslovit.

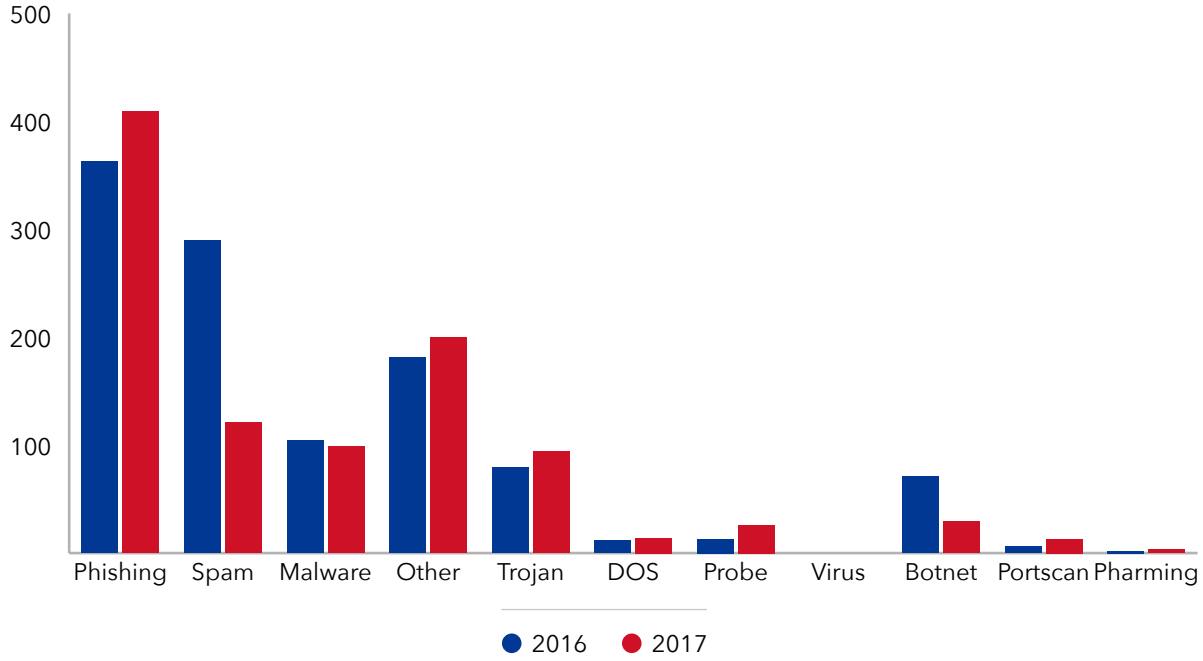
Již v roce 2016 byl v našem týmu vyvinut open-source nástroj Convey, který nám umožňuje automatizovat komunikaci ohledně bezpečnostních incidentů, do kterých je zapojeno více stran. V roce 2017 jsme pokračovali v dalších úpravách tohoto nástroje. Ten je tak nyní mnohem univerzálnější a není vázán pouze na tiketovací systém používaný naším bezpečnostním týmem, což jej otevírá širšímu využití v bezpečnostní komunitě. Mezi další nově přidané vlastnosti patří možnost universální práce se sloupci, dohledání rozšiřujících informací, jako je země, nebo hostname a DNS/WHOIS information batch fetching.

STATISTIKA PROCESU ŘEŠENÍ BEZPEČNOSTNÍCH INCIDENTŮ TÝMEM CSIRT.CZ:

	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017
IDS*	0	0	0	491	3 924	2 121	2 380	3 771	9 944	13 858
Phishing	65	220	209	144	159	175	368	367	363	409
Spam	47	28	103	26	43	73	159	108	290	121
Malware	53	134	121	10	20	45	117	240	104	99
Other	1	5	13	62	14	75	102	264	181	200
Trojan	66	6	26	5	5	12	56	90	79	94
DOS	2	4	2	2	68	72	32	37	12	14
Probe	0	3	14	25	12	26	86	42	13	26
Virus	0	84	99	0	0	0	0	0	0	0
Botnet	0	3	46	5	8	15	0	4	71	29
Portscan	10	4	1	6	1	3	2	5	6	13
Pharming	0	0	0	0	0	0	18	3	2	3
Celkem	**244**	**491**	**634**	**285**	**330**	**496**	**940**	**1 160**	**1 121**	**1 008**

*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 2017 tedy představuje počet varování zaslaných touto službou správcům koncových sítí provozovaných v ČR.

POČTY VYBRANÝCH BEZPEČNOSTNÍCH INCIDENTŮ HLÁŠENÝCH TÝMU CSIRT.CZ V LETECH 2016 A 2017:



ZAJÍMAVÉ KAUZY ROKU 2017

Stejně jako v předchozích letech jsme i v roce 2017 zaznamenali několik větších DDoS útoků, botnetů, kampaní šířících malware včetně známého ransomware WannaCry, brute force útoků a řešili jsme i seznam kompromitovaných e-mailových účtů především na velkých freemailových službách.

Velmi zajímavý incident byl iniciován naším systémem IDS (Intrusion Detection System), který reaguje na pokusy o komunikaci odesláním informačního e-mailu do sítě, ze které požadavek na zahájení komunikace dorazil. Na základě upozornění odeslaného naším systémem nás kontaktoval ISP, který prováděl testování nového CPE. Protože bylo zjevné, že zařízení bylo nějakým způsobem kompromitováno a provádí skenování jiných sítí, dohodli jsme se s dodavatelem na jeho zapůjčení. Jednalo se o zařízení Billion BiPAC 9800VNXL, které slouží jako router kombinovaný s modemem. Analytici našeho týmu pak nalezli na tomto zařízení zranitelnost, která byla již dříve popsána u modemů Eir D1000. Následně jsme kontaktovali

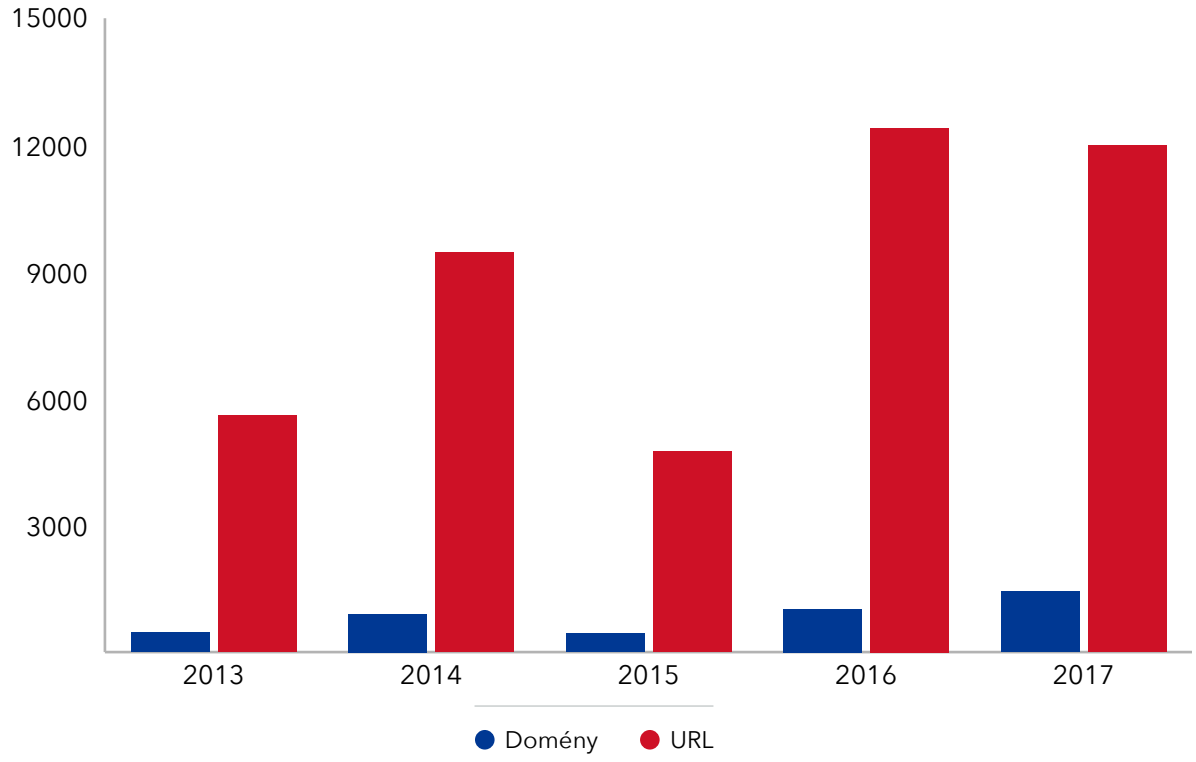
přímo výrobce, který potvrdil, že o chybě již ví a zákazníkům začal distribuovat opravenou verzi firmwaru.

Dále jsme se věnovali analýze malware Routex, který se v říjnu objevil na zařízeních Ubiquiti a kde jsme se zabývali také vytvořením honeypotu, který by nám o šíření této nákazy řekl více. Kromě těchto incidentů jsme se také věnovali analýze routeru Asus RT-AC66U, který nám byl zapůjčen ke zkoumání na základě podezření na možnou kompromitaci tohoto zařízení. Naše zkoumání však nepotvrdilo žádný zásah do firmwaru zařízení. Postupný nárůst počtu otevřených TCP spojení, na která si uživatel stěžoval tak mohl být způsoben například chybou, kvůli které router tato spojení udržoval otevřená. Protože zadáním bylo v tomto případě vyloučit kompromitaci zařízení, naši analytici se již dále důvody podezřelého chování nezabývali.

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.

MDM – POČTY ŠKODLIVÝCH URL, KTERÁ JSME V JEDNOTLIVÝCH MĚSÍCÍCH EVIDOVALI JAKO VYŘEŠENÉ NEBO ŘEŠENÉ (AKTUÁLNÍ):



V roce 2016 jsme začali v projektu MDM řešit kromě phishingu, malware a C&C také defacement webových stránek. V roce 2017 jsme pak odeslali informace o 454 defacementech webových prezentací.

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 2017 bylo publikováno celkem 130 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

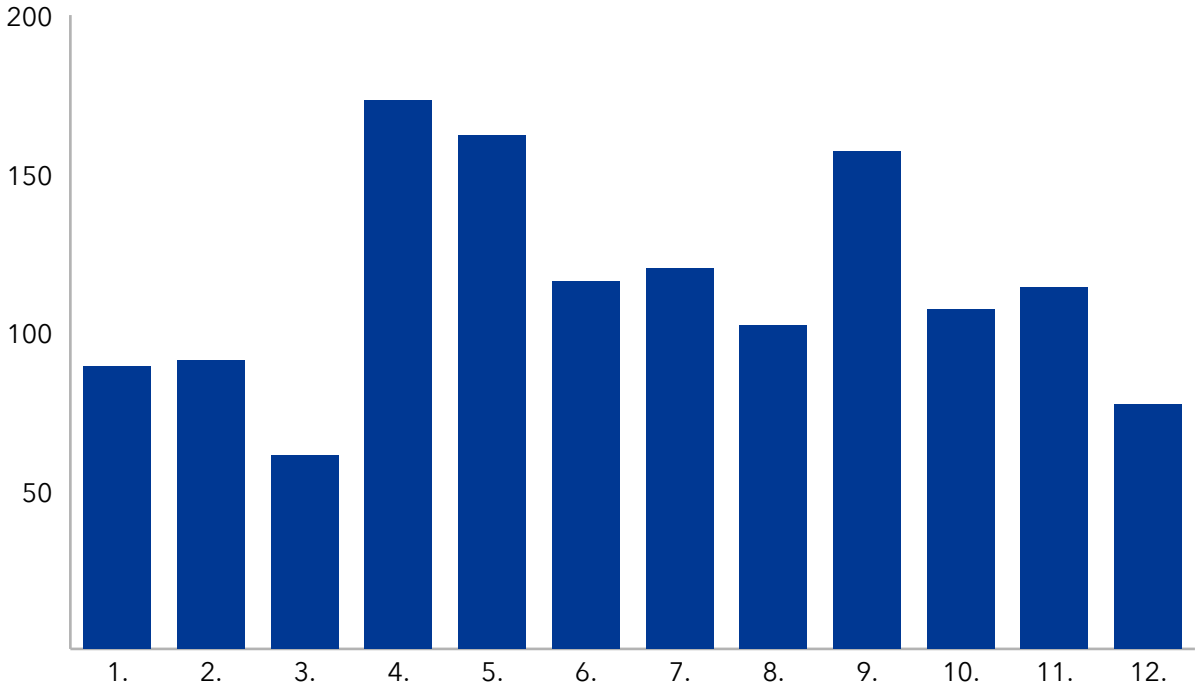
Služba Skener webu byla spuštěna v roce 2013 s cílem zvýšit povědomí o možnostech lepšího zabezpečení webových stránek. Nadále testujeme webové aplikace přes automatizované nástroje, jejichž výsledky jsou pak doplněny o ruční testy. V roce 2017 jsme se rozhodli provést velkou revizi používaných nástrojů v jejímž rámci jsme některé naše postupy přehodnotili a vylepšili. Zároveň jsme vytvořili vlastní nástroj domaincheck, který urychluje a automatizuje kontrolu hlaviček webu, kontrolu některých zranitelnosti, vyhledává možné vstupy do webové administrace a zapomenuté konfigurační soubory nebo soubory záloh.

Celkově jsme v roce 2017 otestovali 60 webových prezentací na základě 53 objednávek. Kromě toho jsme ještě realizovali testování dalších 10 webových prezentací v rámci rozsáhlejšího penetračního testování, které bylo provedeno na základě speciálních objednávek.

Honeypoty

V roce 2017 jsme z provozu našich honeypotů získali 1 987 unikátních vzorků kódu nahraného útočníky platformu Windows a 2 270 unikátních vzorků malware na platformě Linux. Z toho nebylo 1 369 do doby nahrání na naše honeypoty testováno platformou VirusTotal a 36 vzorků jsme díky navázané spolupráci předali k dalšímu zkoumání společnosti Avast.

MNOŽSTVÍ NOVÉHO MALWARE V JEDNOTLIVÝCH MĚSÍCÍCH:



PROKI

V roce 2015 zahájil Národní bezpečnostní tým CSIRT.CZ realizaci 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. V roce 2016, kdy se projekt nacházel v přípravné a implementační fázi, byly každý týden odesílány reporty vybraným správcům, kteří byly ochotni zároveň poskytnout zpětnou vazbu. V letošním roce projekt přešel do ověřovací fáze a reporty jsou od října 2017 doručovány správcům všech dotčených koncových sítí. Samotný report pak obsahuje informace 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 je možné filtrovat podle IP adresy, konkrétních adresních bloků, země „původu“, portů, počtu opakování incidentů a dalších parametrů.

Při přípravě projektu pro ověřovací fázi byla pozornost věnována především zrobustnění vlastní vývojářské a provozní infrastruktury. Proběhla migrace na nový výkonnější hardware,

čímž mohlo být realizováno oddělení testovacího a produkčního prostředí v souladu s vývojem dle zásad kontinuální integrace, ale dále probíhal také další vývoj a byly přidány některé zdroje. Pro některé z nich bylo také nutné vyvinout vlastní komponentu.

V rámci vývoje IntelMQ (jedna z komponent systému PROKI) byla pozornost věnována zjednodušení ladění chyb v rámci testovacích procesů a byly vyvinuty nové debuggovací funkce, které byly následně také zdokumentovány a dány k dispozici odborné komunitě.

Další vývoj probíhal mimo jiné na základě zpětné vazby od správců koncových sítí. Jednou z funkcí, které vznikly na podnět komunity, byla implementace podepisování PGP klíčem, který v kombinaci s nově implementovanou funkcí DKIM a SPF podstatně zvyšuje důvěryhodnost odesílaných e-mailů.

Abychom vycházeli vstříc příjemcům reportů z projektu PROKI, umožňujeme jim v jejich e-mailových reportech vynechávat některé zdroje, případně libovolné zmínky o jejich IP adresách. Protože zkušenost ukázala, že si přejí ignorovat i celé rozsahy adres, byla, v rámci námi dříve vyvinutého Custom filteru, přidána nová možnost filtrace celých síťových rozsahů.

V neposlední řadě proběhly změny a vývoj i ve formátu samotných reportů, kde jsme si především kladli za cíl zvýšit čitelnost pro správce, kteří soubor zpracovávají manuálně a zjednodušit jim tak práci.

Dalším z cílů projektu PROKI je provádění pravidelného ročního 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

Vzdělávání a osvětu na straně koncových uživatelů, ale i dalších zainteresovaných stran považujeme dlouhodobě za důležitou součást prevence proti úspěšným útokům v kyberprostoru. V uplynulém roce jsme tak opět realizovali celou řadu osvětových akcí a školení. V rámci akademie CSIRT.CZ bylo realizováno pět běhů školení Základy fungování CSIRT týmu, které se stalo oblíbeným zdrojem informací pro firmy, které zakládají, nebo se chystají založit vlastní bezpečnostní tým.

Zdařilou akcí byl celodenní seminář, který jsme u příležitosti Evropského měsíce kybernetické bezpečnosti uspořádali pro veřejnost na Jihočeské universitě. Program byl poskládán tak, abychom pokryli témata bezpečnosti, ale také témata spojená s registrem či škodlivým obsahem na Internetu. Posluchači se tak mohli dozvědět například o trendech v oblasti phishingu, malwaru či ransomwaru nebo o projektu STOPonline. Kromě toho byla pro účastníky připravena hacking challenge, při které si měli možnost vyzkoušet své znalosti a schopnosti.

V roce 2017 byla naše kolegyně Zuzana Duračinská požádána o zapojení do mezinárodního školení TRANSIT, kde v roli lektora přednášela operační část tohoto školení. V jeho rámci se účastníci seznámí s procesem incident handlingu, nejčastěji používanými tiketovacími systémy, problematikou zveřejňování informací o týmu a dalšími praktickými informacemi, potřebnými pro bezproblémové fungování bezpečnostního týmu.

V rámci spolupráce s krajem Vysočina jsme pak uspořádali školení pro příslušníky Policie ČR k problematice kybernetické bezpečnosti, kde jsme přednášeli o útocích, ale i různých podvodech na Internetu a diskutovali jsme také možnosti PČR při zajišťování potřebných důkazů.

Kromě toho jsme se účastnili celé řady konferencí a seminářů jak v České republice, tak i v zahraničí.

Členové týmu také publikovali řadu článků v tištěných, tak i v internetových médiích. Kromě populárního seriálu Postřehy z bezpečnosti na portálu root.cz jsme v roce 2017 ve spolupráci se serverem lupa.cz připravili seriál osvětových článků o ransomwaru. Také jsme se podíleli na připomínkování osvětových seriálů pro děti, vysílaných na dětském kanálu České televize.

V rámci prevence jsme mimojiné v uplynulém roce realizovali akci skenování CMS (Content Management System). Při ní jsme automatickým nástrojem provedli skenování všech webových prezentací v doméně .CZ za účelem identifikace stránek, které pro svůj běh využívají některé ze dvou populárních CMS, WordPress a Joomla. Zároveň jsme identifikovali i používanou verzi daného CMS. Pokud jsme zjistili, že jsou webové stránky provozovány na neaktuální verzi CMS, byl o tom držitel domény informován prostřednictvím e-mailu.

Pokud jde o samotné výsledky, celkem jsme nalezli 50 761 .CZ domén se zastaralou verzí některého z CMS. Konkrétně to bylo 25 606 starých verzí CMS Joomla a 25 155 zastaralých verzí WordPressu. Dva týdny po prvotním testování jsme při druhé vlně skenování, ve které jsme již skenovali pouze dříve identifikované weby, zaznamenali u 10 514 domén změnu k lepšímu, což je zlepšení o 20,71 %. Část stránek, konkrétně 2 686, také mezitím přestala být dostupná nebo již neposkytuje informace o verzi. Pokud jde o nedostupné weby, domníváme se, že stejně jako jsme to již zaznamenali při podobných akcích dříve, část držitelů doménových jmen měla někde polozapomenutý web a po našem upozornění ho raději vypnula, další mohou být expirace domén, náhodný výpadek serveru, apod.

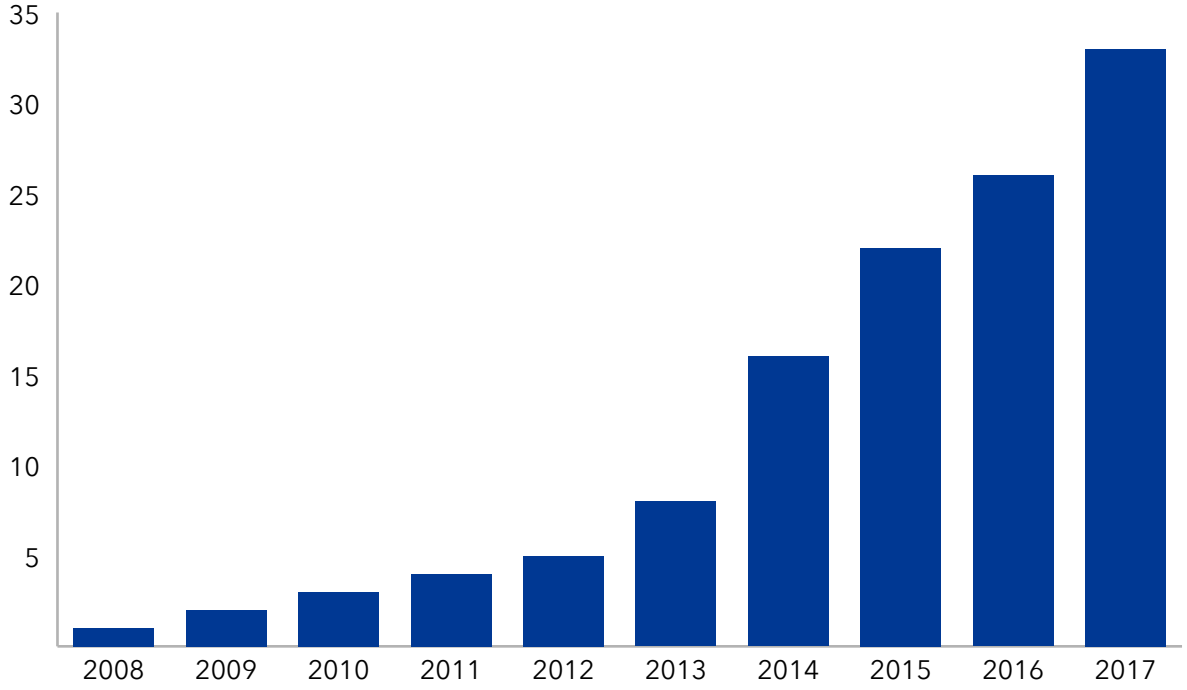
Národní a mezinárodní spolupráce

Strategickým partnerem v oblasti národní spolupráce je úřad NÚKIB a tým GovCERT. Jde například o oblast legislativy, formulování společných stanovisek v rámci CSIRT Network či spolupráci na kybernetických cvičeních. Národní a Vládní CERT se několikrát ročně potkávají při různých příležitostech, což poskytuje dostatečný prostor na pravidelné informování o práci jednotlivých týmů a jejich případnou koordinaci.

Pro úspěšné řešení incidentů je pro nás důležité udržovat kontakty s českými poskytovateli Internetu. Právě pro zlepšení komunikace a spolupráce na národní úrovni jsou pro nás důležité Pracovní skupiny CSIRT.CZ. V roce 2017 jsme uspořádali celkem dvě tato setkání, na kterých jsme řešili aktuální témata, jako GDPR, novelu zákona o kybernetické bezpečnosti nebo jsme se věnovali technickým přednáškám, například o malware cryptolockeru, analýze malware, routerů nebo užitečných nástrojů, využitelných v rámci bezpečnostní komunity. Nepsaným pravidlem se stalo, že v první polovině roku pořádáme tzv. „velkou“ Pracovní skupinu CSIRT.CZ, kde jsou pozváni všichni, kdo se o problematiku kybernetické bezpečnosti zajímají. Tohoto setkání se v červnu účastnilo 100 lidí. Na podzim se pak uskutečnila tzv. „malá“ Pracovní skupina, kde jsou pozváni jenom zástupci českých bezpečnostních týmů minimálně se statusem Listed u mezinárodní organizace TF-CSIRT. Toto setkání se konalo v listopadu.

V roce 2017 se také opět zvedl počet českých CSIRT týmů oficiálně ustanovených v rámci TF-CSIRT. Podpořili jsme vznik sedmi nových týmů. Nyní je v České republice celkem 33 CSIRT týmů. Bezpečnostní týmy ze soukromého sektoru mají největší zastoupení. Nárůst počtu bezpečnostních týmů zvyšuje také nároky na Národní tým při zapojování těchto týmů do české bezpečnostní komunity.

POČET OFICIÁLNÍCH ČESKÝCH CSIRT TÝMŮ V JEDNOTLIVÝCH LETECH:



Další rozvoj národní a mezinárodní spolupráce budeme moci z části financovat z projektu CEF, který nám byl v roce 2017 schválen. Mezi další financované aktivity z tohoto projektu patří hlavně další vzdělávání a zvyšovaní odbornosti členů týmů.

V oblasti mezinárodní spolupráce se nadále aktivně účastníme setkání TF-CSIRT, kde minimálně jednou ročně prezentujeme vlastní poznatky z různých oblastí. Pokračovali jsme také v našich aktivitách ve Steering Committee TF-CSIRT, kde jsme se podíleli na vypracování strategie fungování TF-CSIRT, dále na dokumentu jehož cílem je pomoci nově přicházejícím bezpečnostním týmům či na revizi školení TRANSIT. Vzhledem k tomu, že Česká republika patří ke státům s nejvyšším zastoupením týmů v rámci služby Trusted Introducer, snažíme se v rámci Steering Committee prosazovat také jejich zájmy a pravidelně české týmy informujeme o případných novinkách.

V rámci mezinárodní spolupráce jsme se také aktivně zapojili do CSIRT Network. Tato povinnost nám vyplynula ze směrnice NIS. Jde o seskupení převážně vládních a národních týmů na úrovni členských států EU. První rok fungování se nesl v organizačním duchu, protože dle NIS směrnice si pravidla fungování musí stanovit samotná skupina. Postupně by CSIRT Network měl řešit spíše operační úkoly, spolupráci při řešení incidentů a sdílení know-how. V nejbližších letech bude určitě na programu také implementace NIS směrnice v praxi.

Účastnili jsme se také výročního setkání organizace FIRST, která sdružuje bezpečnostní týmy z celého světa. V rámci aktivní participace jsme byli zapojeni v programové komisi konference a zároveň jsme byli v roli chaira v jedné části programu. Také jsme se účastnili setkání Národních týmů pod hlavičkou CERT CC, které se snaží již několik let jednou ročně přivést k jednomu stolu bezpečnostní týmy s národní působností z celého světa. Tato setkání navazují z logistických důvodů právě na výroční konferenci FIRST. Na setkání jsme představili rozvoj českých bezpečnostních týmů, byly jsme členem programové komise a také zde jsme byli v jedné části programu v roli chaira.

Závěr

Těší nás, že jsme dokázali i v roce 2017 udržet vysokou kvalitu poskytovaných služeb a navázali jsme tak na naše úspěšné působení z minulých let. Opět jsme se soustředili na další rozvoj již existujících nástrojů a služeb, avšak zároveň jsme hledali nové možnosti, jak prospět bezpečnostní komunitě, uživatelům, koncovým sítím i samotné bezpečnostní komunitě. V dalším roce bychom rádi připravili nové školení pro koncové uživatele, pustili se do dalších preventivních akcí, dokončili proces implementace dopadů nařízení GDPR do naší běžné praxe a stejně jako v roce 2016 se plánujeme aktivně zapojit do cvičení Cyber Europe, jak v roli hráče, tak i národního koordinátora. Kromě těchto aktivit budeme pokračovat v již existujících projektech a dále zlepšovat námi vyvíjené nástroje.

Stejně jako v roce 2016 bychom chtěli skončit vypíchnutím tří bodů, které považujeme v uplynulém roce za nejdůležitější. Jedním je akce skenování CMS, která byla i přes některé dílčí nedostatky držiteli domén hodnocena pozitivně, dalším pak přechod projektu PROKI do ověřovací fáze a třetím naše koordinační a podpůrná role v rámci komunity bezpečnostních týmů jak v rámci ČR, tak i našeho působení na mezinárodní scéně.