ZPRÁVA O ČINNOSTI CSIRT.CZ (NÁRODNÍHO CSIRT ČR) ZA ROK 2018

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. Od 1. srpna 2017 je pak na základě zákona číslo 205/2017 Sb., ústředním správním orgánem pro kybernetickou bezpečnost Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB). Uzavřená veřejnoprávní smlouva tak automaticky přešla pod tento nový správní orgán.

Rok 2018 v kostce

Za jednu z nejdůležitějších záležitostí spojenou s CSIRT.CZ v roce 2018 považujeme dokončení procesu certifikace u TF-CSIRT. Díky němu jsme se stali teprve druhým certifikovaným týmem v České republice. Dokončení obnášelo nezávislý audit a dokončení zdokumentování zažitých procesů.

Důležité změny v otázce legislativy přinesla nová vyhláška o kybernetické bezpečnosti, která byla zveřejněna ve Sbírce zákonů pod označením *„Vyhláška č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti)“*.

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 2018 řešil CSIRT.CZ 1 079 bezpečnostních incidentů. Za téže rok znovu narostl počet odpovědí v souvislosti s řešením těchto incidentů. Celkem bylo odesláno 10 264 e-mailů na incident, tj. o 3 748 více než v roce předešlém. S jedním incidentem mohou být spojeny až desítky odeslaných e-mailů z důvodu komplexnosti útoků, botnety, zranitelná zařízení, kompromitované účty.

Vytvořili jsme doplněk do prohlížeče, který zrychluje práci s interně používanými aplikacemi – zvláště s OTRS. Přináší řadu klávesových zkratek a předvyplňuje různá pole, na která jsme museli myslet ručně. Toto řešení nám umožnilo zapojit se do aktivit v projektu Safer Internet nad rámec provozu STOPonline bez nutnosti rozšiřovat tým. Utilitu Convey jsme dotáhli do verze 1.0, celý její životní cyklus od instalace po použití teď pracuje podle našich představ – distribuuje se jako snadno jedním řádkem instalovatelný balíček, umožňuje uživateli dopočítávat vlastní CSV sloupce externím skriptem, lépe pracuje s méně obvyklými WHOIS dotazy.

STATISTIKA PROCESU ŘEŠENÍ BEZPEČNOSTNÍCH INCIDENTŮ TÝMEM CSIRT.CZ:

	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018
Sensor Network	0	0	0	491	3 924	2 121	2 380	3 771	9 944	13 858	18 435
Phishing	65	220	209	144	159	175	368	367	363	409	518
Spam	47	28	103	26	43	73	159	108	290	121	144
Malware	53	134	121	10	20	45	117	240	104	99	135
Other	1	5	13	62	14	75	102	264	181	200	58
Trojan	66	6	26	5	5	12	56	90	79	94	0
Probe	0	3	14	25	12	26	86	42	13	26	171
DOS	2	4	2	2	68	72	32	37	12	14	7
Botnet	0	3	46	5	8	15	0	4	71	29	20
Virus	0	84	99	0	0	0	0	0	0	0	0
Portscan	10	4	1	6	1	3	2	5	6	13	16
Pharming	0	0	0	0	0	0	18	3	2	3	10
Celkem	**244**	**491**	**634**	**285**	**330**	**496**	**940**	**1 160**	**1 121**	**1 008**	**1 079**

Do celkového počtu řešených bezpečnostních incidentů se nezapočítávají incidenty typu IDS (nově označovány jako Sensor Network), které jsou uvedeny ve druhém řádku výše uvedené tabulky. Systém pro detekci neoprávněného přístupu do systému IDS (Intrusion Detection System) slouží k zachycovaní 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).

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.

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 2018 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 došlo velké revizi používaných nástrojů v jejímž rámci jsme některé naše postupy přehodnotili a vylepšili. Zároveň jsme vytvořili vlastní nástroj domain check, 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 2018 otestovali 64 domén na základě 38 objednávek – z toho 21 domén u významných subjektů, 3 v rámci projektu Safer Internet.

Honeypoty

Na linuxových honeypotech cowrie jsme v roce 2018 zaznamenali 3 882 vzorků. Na Windows honeypotech dionaea jsme pak zachytili 862 vzorků.

HAAS – ZAZNAMENANÉ STATISTIKY:

Počet uživatelů	2 374
Počet provedených příkazů	70 601 463
Počet unikátních útočících IP adres	116 803

POČET IP DLE MĚSÍCŮ:

duben	17 532
květen	16 899
prosinec	16 498
červen	15 443
únor	15 119

POČET IP DLE ZEMÍ:

US	16 993
CN	12 904
DE	9 714
RU	7 970
BR	6 794

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. Od roku 2017 projekt přešel do ověřovací fáze a reporty jsou od října doručovány správcům všech dotčených koncových sítí. Samotný report pak obsahuje informace o všech pozorovaných incidentech, které se v daném období vztahovaly k jejich síti.

V letošním roce jsme pracovali zejména na zlepšení vnitřních součástí systému. Byl vyvinut nový systém filtrování incidentů, který je založen na jazyku Sieve používaného pro filtrování emailů a umožňuje přehlednější zápis a hlavně širší možnosti. Ten byl zároveň začleněn do upstreamu stěžejního open source projektu IntelMQ, který je součástí systému PROKI.

Dále bylo věnováno úsilí na rozvoj webového rozhraní pro správu a debuggování IntelMQ, které přináší snazší ovládání klíčových komponent a větší uživatelskou přívětivost. I tato úprava byla začleněna do upstreamu projektu.

Došlo k upgradu databáze na jednu z aktuálních verzí a úpravě mapování datových typů jednotlivých polí incidentů, tak aby bylo usnadněna práce při provádění analýz incidentů.

Na základě požadavků komunity jsme také implementovali alternativní způsob odebírání incidentů správci koncových sítí. Jedná se o jednoduché API, ke kterému na vyžádání poskytneme klíč (o ten je možno zažádat na adrese proki@csirt.cz), kterým je možné pro daný abuse kontakt získávat incidenty za libovolné časové intervaly (v řádech dní). Zatím je nasazeno v testovacím provozu a na jeho rozvoji budeme stále pracovat. Jeho zpřístupnění s sebou neslo i nutné zvýšení bezpečnostních opatření celého systému.

Stále platnou činností je zkvalitňovaní informačních zdrojů pro PROKI. Některé zdroje se i podle reakcí uživatelů a administrátorů ukázaly být nevýznamné a tak došlo k jejich vyřazení. Jiné zdroje jsme naopak přidali a doufáme, že naše prvotní zhodnocení jejich užitečnosti se nám potvrdí.

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.

Během roku 2018 vystupoval CSIRT.CZ na nejrůznějších konferencích a odborných skupinách (*Internet a technologie, Peeringsdays, Pracovní skupina CSIRT.CZ, Internetem bezpečně, Incident Handling Automation Project meeting, TF-CSIRT, Policejní akademie a Ministerstvo průmyslu a obchodu*).

Mimo to bylo v roce 2018 připraveno nové školení Bezpečnost a soukromí na Internetu, které úspěšně proběhlo ve čtyřech bězích. Celkově pak CSIRT.CZ realizoval tři běhy školení Základy fungování CSIRT týmu, pět běhů specializovaného školení pro Policii o kyberzločinu, jedno specializované školení pro ředitele středních škol v rámci projektu Krajský akční plán rozvoje vzdělávání Moravskoslezského kraje a jedno specializované školení o různých aspektech bezpečnosti pro neziskové organizace na akci organizace Člověk v tísni.

K dalším počinům na poli osvěty a vzdělávání je třeba vyzvednout dokončení knihy CyberSecurity. Jiná publikační činnost pak zahrnovala uveřejňování osvětových i vzdělávacích článků (i STOPonline), a sice v konkrétní rovině to bylo čtyřiadvacet příspěvků do Postřehy z bezpečnosti, čtrnáct příspěvků na blog nic.cz. Dle témat a aktuálních potřeb to bylo rovněž publikování článků v tištěných médiích.

CSIRT.CZ se zapojil v roce 2018 do akce ECSM (European Cyber Security Month). K výběru akcí docházelo tak, aby bylo možné oslovit všechny potenciální cílové skupiny (děti, studenty, odbornou veřejnost, státní správu, školy, příslušníci PČR apod.).

Co se týká prevence, testovali jsme webové prezentace v doméně .CZ. Cílem bylo nalézt případné napadené domény šířící malware, o kterých komunita dosud neví. Hledali jsme weby, které si stahují komponenty z více různých (především zahraničních) IP adres a domén a takové jsme pak dále analyzovali. Výsledkem pokusu bylo, že komunita má velmi dobré povědomí a přehled o napadených doménách. Mimo jiné pak ověřil užitečnost aplikace MDM, která s veřejnými daty pracuje.

Národní a mezinárodní spolupráce

Strategickým partnerem v oblasti národní spolupráce je úřad NÚKIB a tým GovCERT. Zde dochází k širokému okruhu spolupráce, například v oblasti 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. Kromě toho se pravidelně spolu účastní setkávání na TF-CSIRT či CSIRTs Network.

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. 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 dubnu účastnilo 93 lidí.

Národní a mezinárodní spolupráce pak zahrnuje také podporu pro týmy, které chtějí vstoupit do organizací TF-CSIRT a FIRST, která vychází z požadavky onsite visit, obnášející kontrolu funkčnosti a plnění požadavků) u zájemců, kteří chtějí do těchto organizací vstoupit.

V roce 2018 se CSIRT.CZ zapojil do mezinárodních cvičení jako je Locked Shields (technické cvičení organizované NATO) či Cyber Europe (technicko-organizační cvičení, kterého se členové týmu účastnili ve dvou úrovních, jako hráči a jako organizátoři pro českou komunitu). Cvičení se celkově zúčastnilo 8 českých týmů a 44 hráčů z 15 firem a institucí.

Závěr

Stejně jako v předešlých letech se nám podařilo udržet vysokou kvalitu poskytovaných služeb. Nicméně se CSIRT.CZ stále posouvá vpřed. Opět jsme se soustředili na další rozvoj již

existujících nástrojů a služeb, zároveň jsme však hledali nové možnosti, jak být užiteční a prospět bezpečnostní komunitě, uživatelům a koncovým sítím.

Proto nás těší dosažený pokrok v projektu PROKI, vydání knihy Cybersecurity, spuštění nového školení a další výše popsané projekty a úspěchy. Vše je pak korunováno již zmiňovanou certifikací týmu CSIRT.CZ, která je pro ostatní aktéry zárukou kvality poskytovaných služeb.