ZPRÁVA O ČINNOSTI CSIRT.CZ (NÁRODNÍHO CSIRT ČR) ZA ROK 2019

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, kteréuzavřelo 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 2019 v kostce

V roce 2019 to bylo poprvé od roku 2014, kdy počty incidentů reportovaných CSIRT.CZ klesly pod celkový počet jeden tisíc incidentů za rok. Největší podíl incidentů jsou, jako každý rok, útoky typu Phishing. Z pohledu procesu řešení incidentů považujeme za důležité další vývoj nástrojů Convey a doplňku do prohlížeče. Jedná se o nástroje, které usnadňují a urychlují řešení bezpečnostních incidentů. Jedním z mnoha benefitů je například možnost hromadně zpracovávat tisíce řádků logů při distribuci informací ohledně DoS nebo DDoS útoků.

Jako každý rok se CSIRT.CZ v roce 2019 věnoval osvětové a vzdělávací činnosti v podobě populárních a odborných článků, publikováním novinek z bezpečnosti, školením kurzů z oblasti informační bezpečnosti či organizováním takových školení od externích lektorů. Stejně tak i členové týmu se snaží aktivně rozšiřovat své znalosti účastí na různých školeních, kurzech či konferencích.

Novinkou, na které CSIRT.CZ pracoval, je služba penetračního testování. Tu jsme v roce 2019 připravovali jak po stránce administrativní, tak po stránce technické. Na podzim jsme pak službu spustili v pilotním provozu a otestovali prvního zákazníka. Tuto službu plánujeme do budoucna dále rozšiřovat a od roku 2020 aktivně nabízet zákazníkům.

V neposlední řadě je třeba zmínit projekt PROKI a jeho rozvoj, kde došlo k vývoji dalších softwarových komponent a zároveň k přidání nového důležitého zdroje dat, který umožnil rozšířit prováděné analýzy.

Služby poskytované týmem CSIRT.CZ

INCIDENT HANDLING A INCIDENT REPONSE

Služba incident handling a incident response (řešení a koordinace řešení bezpečnostníchincidentů) je základní službou, kterou týmy 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
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.
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 2019 řešil CSIRT.CZ 954 bezpečnostních incidentů. Zároveň znovu narostl počet odpovědí v souvislosti s řešením těchto incidentů. Celkem bylo odesláno 13 883 e-mailů, tj. o 3 821 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, apod.).

STATISTIKA PROCESU ŘEŠENÍ BEZPEČNOSTNÍCH INCIDENTŮ TÝMEM CSIRT.CZ

	2017	2018	2019
Sensor Network	13 858	18 435	14 911
Phishing	409	518	483
Spam	121	144	128
Malware	99	135	85
Other	200	58	85
Probe	26	171	141
Trojan	94	0	0
DOS	14	7	16
Botnet	29	20	4
Virus	0	0	0
Portscan	13	16	3
Pharming	3	10	9
Celkem	**1 008**	**1 079**	**954**

* Sensor Network není započten do celkového počtu

Již v roce 2016 byl vyvinut open-source nástroj Convey, který umožňuje automatizovat komunikaci ohledně bezpečnostních incidentů, do nichž je zapojeno více stran.

V roce 2019 byla utilita Convey obohacena o další vlastnosti, které umožňují členům týmu pracovat daleko efektivněji. Jedná se například o naučení práce s kvótami LACNICu nebo schopnost převádění napříč 50 datovými typy konkrétních hodnot. Zároveň byla

zjednodušena instalace tohoto nástroje. Díky zveřejnění na gitlabu ho nyní mohou využívat všechny bezpečnostní týmy v komunitě i mimo ni.

V roce 2018 byl také vytvořen doplněk do prohlížeče, který zrychluje práci s interně používanými aplikacemi – zvláště s OTRS. V roce 2019 došlo k vylepšení tohoto doplňku o automatické určení jazykové šablony odpovědi na základě domény příjemce, zobrazení malého náhledu problémové stránky nebo automatické dopočítávání metadat potřebných pro řešení konkrétních incidentů.

Do celkového počtu řešených bezpečnostních incidentů se nezapočítávají incidenty typu IDS (nově označovány jako Sensor Network). 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).

Statistikám jednotlivých typů incidentů stále vévodí phishing, na druhé místě je pak incident označovaný jako Probe. Pod tento typ incidentu řadíme mimojiné brute force útoky na uživatelské účty, respektive pokusy o prolomení hesla na cílených strojích. Jedná se o typ útoku, kde útočník po zjištění přihlašovacích údajů může zneužít napadaný stroj ve svůj prospěch a pro páchání dalších útoků v kyberprostoru. Tyto praktiky jsou momentálně mezi útočníky velmi oblíbené. Na třetím místě se pak nachází nevyžádaná pošta.

Součástí procesu řešení incidentů je také rozesílání informací v případě zranitelných systémů. V roce 2019 jsme realizovali distribuci informací vztahujících se ke zranitelnosti CVE-2019-11510 v Pulse Secure VPN, která umožňovala potenciálnímu útočníkovi k privátním klíčům a heslům uživatelů. Z tohoto důvodu jsme požádali společnost Bad Packets LLC, která zranitelnost nalezla, aby nám dala k dispozici seznam zranitelných serverů, které diagnostikovala v České republice. Těmto subjektům pak bylo rozesláno upozornění.

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 požádat o otestování odolnosti webové prezentace na dané doméně službou Skener webu.

AKTUÁLNĚ Z BEZPEČNOSTI

V roce 2019 bylo publikováno celkem 60 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.

SKENER WEBU

Skener webu je jedna z preventivních bezpečnostních služeb, která byla spuštěna v roce 2013. Tento projekt je určen provozovatelům a správcům webů, kterým pomáhá bezplatně odhalit potenciální zranitelnosti jejich internetových prezentací. Služba je určena především neziskovým organizacím a veřejné správě. Analýza zranitelnosti probíhá ve dvou fázích.

Nejdříve pomocí automatických nástrojů a následně je proveden manuální test webu zkušeným testerem, který mimo jiné vyhodnotí nalezené zranitelnosti v kontextu celého webu a navrhne vhodná řešení. Na konci je žadateli poslána závěrečná zpráva, která obsahuje nalezené zranitelnosti, jejich ohodnocení dle závažnosti a také návrhy na jejich možná řešení. Při analýze potenciálních zranitelností služba staví jak na vlastních měřeních a zkušenostech bezpečnostního týmu, tak na seznamu Top 10 obecně nejzávažnějších bezpečnostních rizik podle projektu Open Web Application Security (OWASP).

Celkově bylo v roce 2019 otestováno 38 domén na základě 19 objednávek – z toho 6 domén u významných subjektů a 2 v rámci projektu Safer Internet Centre. V rámci projektu penetrační testování bylo otestováno více jak 20 domén.

PENETRAČNÍ TESTOVÁNÍ

CSIRT.CZ v roce 2019 spustil pilotní provoz nové služby penetračního testování. Prvním zájemcem, který tuto službu využil, byl kraj Vysočina. Na základě jejich kladné zpětné reakce byla vyhodnocena pracnost a analýza vhodnosti nasazení služby a bylo rozhodnuto o nasazení služby v průběhu roku 2020.

HONEYPOTY

Na linuxových honeypotech cowrie jsme v roce 2019 zaznamenali 1 878 unikátních vzorků malware. Na Windows honeypotech dionaea jsme pak zachytili 435 vzorků.

HAAS STATISTIKY

Počet registrovaný uživatelů	2 820
Počet provedených příkazů	51 707 878
Počet útoků/spojení	41 902 489
Počet unikátních útočících IP adres	207 161
Počet zachyceným unikátních vzorků	5 150

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

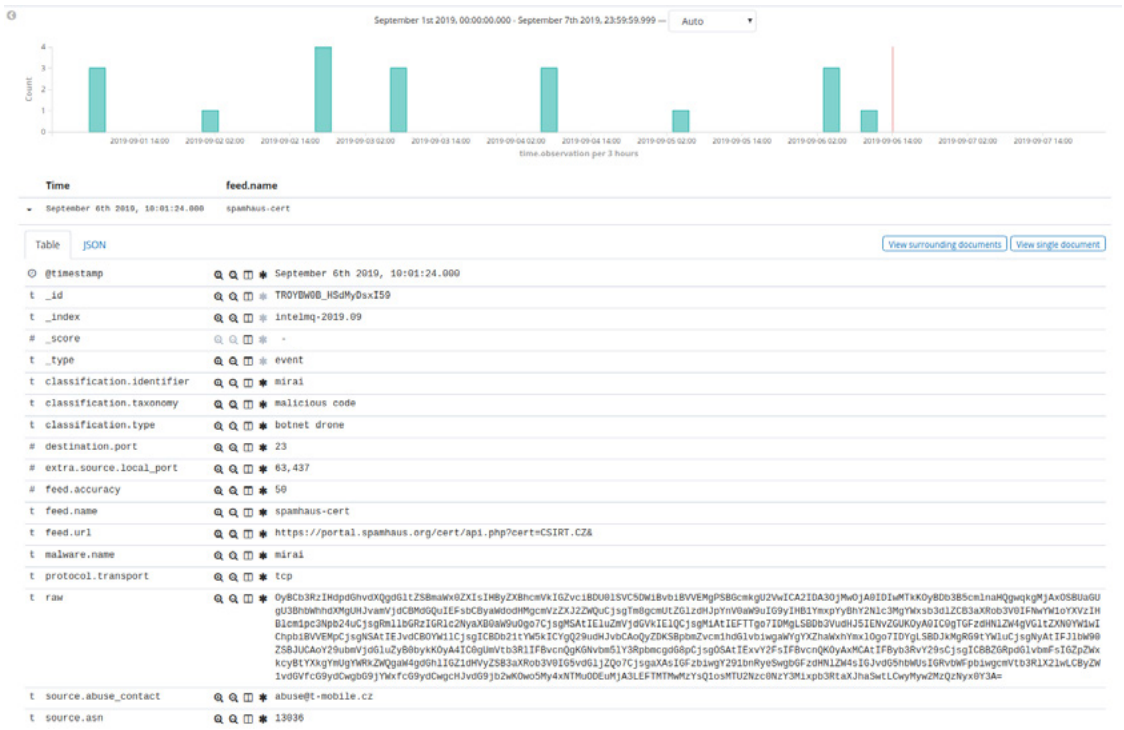
hostujících C&C servery, phishingové stránky, malware či informace o IP adresách skenujících sítě v Internetu nebo o takových IP adresách, na kterých jsou stroje zapojené do některého z botnetů.

Nástroje Elasticsearch, Logstash a Kibana (Souhrně nazývané ELK Stack) patří k základním kamenům SW projektu PROKI. Všechny zmíněné nástroje byly v roce 2019 aktualizované na novější verzi. To přináší například bezplatný modul Security, který umožňuje zvýšit zabezpečení přístupu k datům jak skrze Kibanu, tak přímo do databáze Elasticsearch, oddělení uživatelských rolí a vymezení jejich práv.

Letošním přírůstkem je také přístup k výstupům každodenních rozsáhlých skenů prováděných službou Shodan, zprostředkované rakouským CERT týmem pro celou Českou republiku. Byť je povaha těchto dat jiná, než která jsou zpracovávána systémem PROKI, mohou nám data z Shodanu poskytnout zajímavý kontext pro interpretaci dat z PROKI. Neobsahují totiž pouze zranitelné a závadné služby, nicméně celkový stav sítě - např. jaká služba běží na konkrétním zařízení. To samo o sobě nemusí být závadné, nicméně v některých případech se může jednat o dlouho neaktualizovaný systém, který obsahuje známé zranitelnosti.

Zapojení dat ze služby Shodan nám umožnilo otestovat nový způsob analýzy dat, kdy jsme porovnáním informací služby Shodan a informací v PROKI dokázali identifikovat IP kamery, které byly kompromitovány a jsou útočníky zneužívány k dalším útokům.

Stejný princip byl pak využit i ve spolupráci s komunitou, konkrétně s týmem ALEF CSIRT, který nám poskytl seznam jimi identifikovaných Industrial Control Systems zařízení, alokovaných na IP adresách v České republice. Tato zařízení zahrnují například SCADA, ale i další zařízení. Tento seznam byl následně porovnán s informacemi v systému PROKI, což umožnilo identifikovat mezi těmito zařízeními takové stroje, které již byly s velkou pravděpodobností kompromitovány a mohou tak představovat značné bezpečnostní riziko. Provozovatelé těchto zařízení byly na možná rizika upozorněni. Na obrázku níže je možné vidět jednu z kompromitovaných IP kamer, které byly objeveny v rámci testování nového analytického postupu. Jak je vidět, v tomto případě se jednalo o IP kameru, která byla zapojena do tzv. Mirai botnetu.



Další novinkou, na které však stále ještě pracujeme, je REST API pro správu nástroje IntelMQ. To by mělo umožnit konzistentní způsob, jak vzdáleně (skrze HTTP požadavky) měnit konfiguraci IntelMQ, zapínat či vypínat jednotlivé součásti či získávat výpisy z logů. Cílem je oddělit grafické webové rozhraní IntelMQ Manager od závislosti na spouštění lokálně uložených skriptů a vytvořit univerzální způsob vzdálené komunikace s nástrojem IntelMQ ať už skrze webové či textové rozhraní. Tato nová součást je však stále v experimentálním stadiu a v roce 2020 ji budeme dále testovat a vyvíjet.

OSVĚTA A VZDĚLÁVANÍ

Během roku 2019 vystupovali členové týmu CSIRT.CZ opět na nejrůznějších konferencích a odborných skupinách (Internet a technologie, Pracovní skupina CSIRT.CZ, Internetem bezpečně, TF-CSIRT, Policejní akademie České republiky, Festival bezpečného Internetu (FBI19), Řešení elektronického násilí a kyberkriminality, Ministerstvo průmyslu a obchodu ČR). Členové týmu také v případě potřeby komentovali aktuální dění v plošných médiích.

Mimo to bylo v roce 2019 připraveno nové školení Úvod do forenzní analýzy paměti, které mělo úspěšnou premiéru v prosinci. Celkově pak CSIRT.CZ realizoval čtyři běhy školení Bezpečnost a soukromí na Internetu, a dvě specializovaná školení pro Policii České republiky. Dále pak jedno školení pro zaměstnance Nestlé Česko s.r.o., jedno specializované školení pro Státní úřad pro jadernou bezpečnost a jedno pro Českou národní banku.

Další publikační činnost pak zahrnovala uveřejňování osvětových i vzdělávacích článků. Konkrétně se jedná o čtyřiadvacet dílů seriálu Postřehy z bezpečnosti a další příspěvky na blog.nic.cz. Dle aktuálních témat a situace na poli kybernetické bezpečnosti šlo rovněž o publikování článků v tištěných médiích. Za zmínku stojí uvést příspěvky v časopise IT Systems o bezpečnosti protokolu MQTT, nebo o modelování rizik v CVSS. CSIRT.CZ také pokračoval v publikování návodů pro správce a uživatele na vlastních webových stránkách.

CSIRT.CZ se v roce 2019 zapojil také do organizace školení bezpečnostních týmů v ČR zahraničními lektory z agentury ENISA (Mobile forensics, Memory forensics). Dále také členové týmu absolvovali mezinárodní cvičení CyberSOPex 2019, Cybersecurity Summer BootCamp a vybraná školení SANS.

NÁRODNÍ A MEZINÁRODNÍ SPOLUPRÁCE

Strategickým partnerem v oblasti národní spolupráce je NÚKIB a tým GovCERT. S těmito subjekty spolupracujeme například v oblasti legislativy, kybernetických cvičení, formulování společných stanovisek v rámci CSIRT Network i na dalších projektech. Národní a Vládní CERT se několikrát ročně setkávají při různých příležitostech, což poskytuje dostatečný prostor pro pravidelné informování o práci jednotlivých týmů a jejich případnou koordinaci. Kromě toho se obě organizace pravidelně spoluúčastní setkání v rámci TF-CSIRT či CSIRT Network.

Pro úspěšné řešení incidentů je důležité udržovat kontakty s českými poskytovateli Internetu. Právě pro zlepšení komunikace a spolupráce na národní úrovni jsou důležitá setkání Pracovní skupiny CSIRT.CZ. Nepsaným pravidlem se stalo, že v první polovině roku byla sdružením pořádána tzv. „velká" Pracovní skupina CSIRT.CZ, kam jsou pozváni všichni, kdo se o problematiku kybernetické bezpečnosti zajímají. O toto setkání je vždy velký zájem. V roce 2019 se pracovní skupina věnovala tématům jako jsou citlivá data a zranitelnosti na českém webu, systémy NERD či PROKI, protokol DANE pro bezpečný transport pošty, DNS firewall a další. Velmi oceňujeme také účast zástupců Vojenského zpravodajství, kteří přišli s členy pracovní skupiny diskutovat návrh novely zákona o VZ.

Národní a mezinárodní spolupráce pak zahrnuje také podporu pro týmy, které chtějí vstoupit do organizací TF-CSIRT a FIRST. Ty vyžaduje tzv. on-site visit, což obnáší kontrolu funkčnosti a plnění požadavků u zájemců, kteří chtějí do těchto organizací vstoupit.

V roce 2019 se CSIRT.CZ zapojil do mezinárodních cvičení jako je Locked Shields (technické cvičení organizované NATO), Cybersecurity Summer BootCamp a CyberSOPex.

Závěr

Stejně jako v předešlých letech se nám podařilo udržet vysokou kvalitu poskytovaných služeb. CSIRT.CZ se snaží každý rok zvyšovat kvalitu poskytovaných služeb a rozšiřovat služby nabízené komunitě. 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 nejen dosažený pokrok v projektu PROKI, spuštění nové služby penetračního testování, ale i další výše popsané projekty a výstupy naší činnosti.