ZPRÁVA O ČINNOSTI CSIRT.CZ (NÁRODNÍHO CSIRT ČR) ZA ROK 2020

CSIRT.CZ

Obsah

O 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 automaticky přešla pod tento nový správní orgán.

Rok 2020 v kostce

Rok 2020 přinesl řadu turbulentních změn a požadavků na provedení nezbytně nutných a rychlých reakcí, ale také spolehlivých a funkčních řešení odpovídajících měnícím se podmínkám. Tým CSIRT.CZ zvládl i v tomto náročném roce plnit svou roli, jak v oblasti řešení a koordinace řešení bezpečnostních incidentů, tak také na poli prevence a výzkumu.

Za nejvýraznější počin a přínos bezpečnostní komunitě i koncovým uživatelům lze označit analýzu škodlivého doplňku prohlížeče (Video Downloader for Facebook), určeného ke stahování videí. Doplněk ohrožoval více než 200 tisíc uživatelů. Přijímal pokyny v metadatech zdánlivě bezvýznamného obrázku, na pozadí měnil výsledky vyhledávání a četl soukromá data. Díky partnerům v antivirové společnosti Avast Threat Intelligence, kterým jsme výsledky šetření dále předali, odinstalovaly společnosti Google a Microsoft v polovině prosince tento malware stovkám tisíc uživatelů. Na základě této práce byla následně identifikována rozsáhlá kampaň, pojmenovaná Cache Flow, čítající na 3 miliony instalací v prohlížečích.

V rámci aktivit v oblasti prevence jsme informovali společnosti v ČR postižené únikem přihlašovacích údajů (včetně plaintext hesel) k FortiGate VPN. K samotnému úniku hesel došlo skrze zranitelnost CVE-2018-13379. Mezi dotčenými subjekty byly také nemocnice, nebo instituce spadající pod ZKB. Z toho důvodu byl postup řádně koordinován také s Národním úřadem pro kybernetickou a informační bezpečnost.

Další významnou změnou bylo spuštění komerční služby penetračního testování, které bylo pilotně zahájeno již v předešlém roce nebo rozšíření a upevnění a rozšíření rozsahu a možností národní a mezinárodní spolupráce. Více podrobných informací k jednotlivým službám poskytovaným Národním bezpečnostním týmem ČR je možné nalézt vždy pod patřičnými názvy následujících kapitol této výroční zprávy.

Je podstatné zmínit, že rok 2020 pochopitelně nepřinášel jen samé úspěchy či bezproblémové situace – nebylo možné s ohledem na komunitní charakter například zorganizovat Pracovní skupinu CSIRT.CZ, jejíž stěžejním významem je mimo jiné osobní setkání

členů bezpečnostní komunity ČR a Slovenska – poukázal však, že tým CSIRT.CZ disponuje dostatečnou schopností a způsobilostí udržet kvalitu služeb i v náročných podmínkách.

1.1. Statistiky incidentů v roce 2020

Služba incident handling a incident response (řešení a koordinace řešení bezpečnostních incidentů) 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 2020 bylo řešeno celkem 1 267 incidentů. Jde o zásadní meziroční nárůst v porovnání nejen s předchozím rokem, kdy bylo řešeno 954 incidentů, ale zejména také s jakýmkoliv předešlým rokem. Tým dosáhl dosud nejvyššího registrovaného množství řešených incidentů v evidenci vlastních statistik.

Tento nárůst reflektuje mimo jiné také celkový počet reakcí na incidenty. Reakcí na incidenty jsme zaregistrovali 17 423, což je o 3 540 více než tomu bylo v roce 2019. S jedním incidentem je nezřídka spojovaná řada emailů – až desítky emailů. Důvodem je komplexnost útoků, botnety, zranitelná zařízení, kompromitované účty.

STATISTIKA PROCESU ŘEŠENÍ BEZPEČNOSTNÍCH INCIDENTŮ TÝMEM CSIRT.CZ

	2017	2018	2019	2020
Sensor Network*	13 858	18 435	14 911	16 217
Phishing	409	518	483	738
Spam	121	144	128	216
Malware	99	135	85	109
Other	200	58	85	86
Probe	26	171	141	68
Trojan	94	0	0	0
DOS	14	7	16	16
Botnet	29	20	4	2
Virus	0	0	0	0
Portscan	13	16	3	29
Pharming	3	10	9	3
Celkem	**1 008**	**1 079**	**954**	**1 267**

* Sensor Network není započten do celkového počtu

Jak je patrné z výše uvedené tabulky, v roce 2020 došlo zejména k zásadnímu nárůstu phishingu. Již v měsíci červnu byl dle našich dostupných statistik překonán počet incidentu v kategorii phishing za předchozí léta. Mimo to došlo ke zvýšení počtu incidentů v kategorii spam, malware- zejména ransomware, portscan. Ve zbylých kategoriích, tedy u probe (kategorie zahrnující brute force útoky), botnet, pharming došlo naopak k poklesu incidentů.

Nárůst incidentů ve výše popsaných kategoriích není náhodný, stejně jako samotný počet incidentů v kategorii phishing. Při podrobném zkoumání počtu jednotlivých incidentů je explicitně patrná souvislost s pandemií a krizí spojenou s Covid-19.

Pandemie Covid-19 přirozeně přinesla a také uměle vytvořila řadu podnětů a aktuálně plošně sledovaných témat, které začali útočníci zneužívat ve velkém, jak pro phishing, scamy, spam, ale také další druhy útoků.

Není účelem tohoto dokumentu taxativně jmenovat veškeré prvky ovlivňující nárůst incidentů. Je vhodné však uvést alespoň některé z nich, zejména ty klíčové.

V rámci snahy zachovat alespoň částečně kontinuitu fungování společnosti, byli v souladu s nařízeními, zaměstnanci firem ve velkém rozsahu přesunuti z kanceláří do prostředí domova. Došlo k rozšíření tzv. threat surface attack, tedy na co všechno je možné zaútočit. Promptní a vynucený přesun zaměstnanců do prostředí vlastního domova spolu s potřebou přístupu do firemního prostředí, pro který jsou užívané protokoly pro vzdálený přístup, vedl pochopitelně k nárůstu otevřených portů. Z pohledu uživatele se jedná o snadné řešení, z pohledu kybernetické bezpečnosti o řešení nesoucí sebou zásadní hrozby.

Reakce ze strany útočníků na takto ohromný nárůst otevřených portů je tedy předpokládaná. Zároveň lze tímto vysvětlit nárůst počtu incidentů v kategorii portscan.

Je podstatné zmínit, že do celkového počtu řešených bezpečnostních incidentů se nezapočítávají incidenty typu IDS (označeno jako 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).

Součástí řešení bezpečnostních incidentů je také spolupráce s dalšími bezpečnostními týmy nejen v rámci působnosti ČR, ale také distribuování důležitých informací o zranitelnostech, útocích a další. Podrobnější informace viz kapitola Aktuálně z bezpečnosti a Národní a mezinárodní spolupráce.

Mimo spolupráci s bezpečnostními týmy je potřeba zmínit také spolupráci se státní správou, dále s Policií České republiky na desítkách incidentů – většinou v zahraničí. Mezi nejčastější registrované podvodné aktivity řešené v roce 2020 ve spolupráci s PČR patří:

- falešné e-shopy
- podvodné weby nabízející investice do virtuálních měn
- podvodné reklamy, zejména na sociální síti Facebook
- falešné stránky (například pokus o vylákání finančních prostředků americkým vojákem na misi v Afganistánu).

Řešení bezpečnostních incidentů zahrnuje také spolupráci se specializovaným pracovištěm PČR. V roce 2020 tým CSIRT.CZ sehrál roli zprostředkovatele pro spolupráci PČR a členy projektu Fénix při řešení útoků na nemocnice, ke kterým docházelo na jaře roku 2020.

1.2. Vývoj open-source nástrojů a utilit

Samotný meziroční nárůst incidentů ovlivňuje také samotný proces vývoje open-source nástrojů a utilit napomáhající procesu řešení bezpečnostních incidentů.

Za účelem zefektivňování a usnadňování procesu incident handlingu dochází k neustálému vývoji systémů, nástrojů a doplňků, které tým CSIRT.CZ používá.

Již před několika lety byl vyvinut vlastní open-source nástroj Convey umožňující automatizovanou komunikaci, ve které participuje několik stran. V minulého roce došlo k rozšíření vlastností této utility o možnost práce s kvótami LACNICu a schopnosti převádění napříč 50 datovými typy konkrétních hodnot. Navazující vývoj přinesl také zjednodušení instalace, vytvoření doplňku do prohlížeče urychlujícího práci s interně užívanými aplikacemi – zvláště s OTRS. Doplněk byl dál vyvíjen a rozšířen o možnost automatického určení jazykové šablony odpovědi na základě domény příjemce, zobrazení náhledu problematické stránky nebo automatické dopočítávání metadat potřebných pro řešení konkrétních incidentů. Vývoj nástroje i nadále aktivně pokračuje dál.

Tým zároveň umožňuje jak používání utility, tak i sledování vývoje i dalším bezpečnostním týmům zveřejněním na Gitlabu.

Další posun, se kterým tým v roce 2020 přišel je výsledek vývoje knihovny Envelope určené na programatické zacházení s emaily. Původní motivace zahrnovala vizi poskytnout jednoduché rozhraní pro šifrování textu. Po roce vývoje nabízí Envelope kompletní podporu podepisování i kryptografického šifrování pomocí standardů jak S/MIME, tak i PGP. Umožňuje e-maily nejen vytvářet, ale také číst. To v praxi znamená, že programátor se tak spolehlivým způsobem dostane k hlavičkám, přílohám i adresám e-mailů, což umožňuje a také usnadňuje automatickou analýzu.

Knihovnu lze použít jako modul v skriptovacím jazyce Python nebo jako program z příkazové řádky.

2. 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.

3. Aktuálně z bezpečnosti

V roce 2020 bylo publikováno celkem 23 článků. Nádale pokračujeme v aktivní spolupráci se serverem root.cz s vlastním seriálem Postřehy z bezpečnosti. Jedná se o pravidelný bezpečnostní přehled uplynulých dní. Publikované informace poukazují na nejzajímavější události, aktuality, stejně jako i zranitelnosti, kterým by měla být věnována pozornost.

Sekce Aktuálně z bezpečnosti nacházející se na webových stránkách CSIRT.CZ je určená nejen k rychlému šíření nejpodstatnějších informací o aktuálně probíhajících útocích a objevených zranitelnostech. Sekce AZB se stala vyhledávaným zdrojem spolehlivých 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.

4. Skener webu

V oblasti prevence tým poskytuje od roku 2013 bezpečnostní službu nazývanou Skener webu. Projekt je určen provozovatelům a správcům webů, kterým pomáhá bezplatně odhalit potenciální zranitelnosti jejich internetových prezentací. Služba je určená především neziskovým organizacím a veřejné správě.

Samotná analýza zranitelnosti probíhá ve dvou fázích. Během první fáze je pomocí automatických nástrojů proveden test webu. Následně je vykonán manuální test webu zkušeným testerem, který mimo jiné vyhodnotí nalezené zranitelnosti v kontextu celého webu a navrhne vhodná řešení a východiska pro zlepšení. Na konci je žadateli zaslána podrobná závěrečná zpráva, která obsahuje nalezené zranitelnosti, jejich posouzení dle závažnosti, a také návrhy konstruktivního řešení.

Analýza potenciálních zranitelností vychází nejen z vlastních měření a aplikace zkušeností bezpečnostního týmu, ale také ze zkušeností bezpečnostní komunity. Přihlíží se také k žebříčku Top 10 obecně nejzávažnějších bezpečnostních rizik sestavených v rámci projektu Open Web Application Security (OWASP).

V průběhu roku 2020 došlo k testování 41 domén na základě 14 podaných objednávek. U významných subjektů bylo testováno celkem 22 domén.

Dále to pak byly 3 subjekty v rámci projektu Safer Internet Centre.

5. Penetrační testování

Tým CSIRT.CZ po řádném pilotním testování služby penetračního testování spustil možnost testování naplno. V roce 2020 bylo úspěšně testováno několik subjektů. Objednavatel po testování obdrží detailní report, který obsahuje výstup o všech nálezech a z nich vyplývajících doporučení.

Prvním ze zadavatelů se v předešlém roce stal kraj Vysočina. Pozitivní zpětná vazba podpořila rozhodnutí o zahájení poskytování této služby. Služba je poskytována na komerční bázi. Vybraným typům subjektů jsou poskytovány markantní slevy z důvodu prevenčního zaměření týmu.

6. Honeypoty

Na linuxových honeypotech cowrie jsme v roce 2020 zaznamenali 2 141 unikátních vzorků malware. Na Windows honeypotech dionaea jsme pak zachytili 138 vzorků. V případě cowrie honeypotů se jedná v porovnání s předešlým rokem, kdy bylo evidováno 1 878 vzorků o jednoznačný nárůst. Opačně je tomu v případech dionaea, kde došlo k poklesu ze 435 vzorků na 138.

HAAS STATISTIKY

Počet registrovaný uživatelů	3 159
Počet provedených příkazů	15 069 808
Počet útoků/spojení	24 113 894
Počet unikátních útočících IP adres	669 197
Počet zachyceným unikátních vzorků	2 564

7. PROKI

V roce 2015 zahájil Národní bezpečnostní tým CSIRT.CZ realizaci projektu Predikce a Ochrana před Kybernetickými Incidenty (dále jen PROKI; VI20152020026) podpořeného v rámci Bezpečnostního výzkumu České republiky 2015–2020. V technické oblasti vývoje softwarového řešení projekt sleduje tři hlavní cíle.

Prvním je agregace a obohacování dat o bezpečnostních incidentech a dalších souvisejících skutečnostech 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.

Druhým cílem je umožnit analytikům bezpečnostního týmu CSIRT.CZ provádět na základě těchto dat analýzy konkrétních případů, korelovat hlášení z různých zdrojů a identifikovat tak ohrožené nebo již kompromitovaná zařízení. V této analytické činnosti tým pokračoval i v roce 2020 a podařilo se mu odhalit několik nakažených strojů, jejichž kompromitace nebyla na první pohled zřejmá. Dle standardního postupu byli kontaktováni jejich správci.

Posledním, třetím cílem je tyto informace předávat koncovým správcům sítí a systémů, kteří na jejich základě mohou identifikovat zranitelné či kompromitované zařízení a učinit

potřebná opatření. Protože však množství takových informací zdaleka přesahuje možnosti manuálního rozesílání, bylo nutné vyvinout řešení pro automatizovanou distribuci těchto informací. V prvotním řešení bylo rozhodnuto pro rozesílání e-mailem na tzv. abuse kontakt, v dalších verzích pak bylo umožněno správcům dotazování na data skrze REST API.

Rok 2020 byl formálně posledním rokem běhu projektu, nicméně i v následujících letech tým CSIRT.CZ plánuje systém PROKI dále provozovat, využívat a hlavně dále rozvíjet. Zkvalitňování získaných informací vyžaduje provádění pravidelných revizí zdrojů dat, vyhledávání nových zdrojů, a případně vyřazení těch, které již nejsou nadále relevantní. Jelikož je systém založen na open-source technologiích vyvíjených komunitou, také tým CSIRT.CZ usiluje o zapojení, a to jak vlastním kódem, tak přispíváním do diskuzí o budoucím směřování vývoje.

8. Osvěta a vzdělání

Tým CSIRT.CZ i nadále v roce 2020 pokračoval v oblasti školení a vzdělávání ve spolupráci s Akademií CZ.NIC. Přestože nebylo umožněno zájemcům zúčastnit se vzdělávacích kurzů in persona, alespoň část školení probíhala virtuálně. Uživatelé se tak mohli zúčastnit online školení na téma Bezpečnost a soukromí na internetu zaměřeného na nejčastější hrozby v oblasti kybernetické bezpečnosti, to, jak je rozpoznat, směřuje také k pochopení prevence a seznámení uživatelů s aktivními a pasivními digitálními stopami. Tedy s riziky, zásady bezpečného chování, soukromím a anonymitou na Internetu.

Do osvětové činnosti patří také již zmíněné publikování dvaceti šesti příspěvků v rámci seriálu Postřehy z bezpečnosti, zveřejnění příspěvku v rámci sekce Aktuálně z bezpečnosti. Více informací viz stejnojmenná kapitola.

K dalším aktivitám stojícím za zmínku v této kapitole stojí například také další kolo školení pro zaměstnance Nestlé Česko s.r.o.

9. Národní a mezinárodní spolupráce

Tým CSIRT.CZ v průběhu roku 2020 aktivně spolupracoval s dalšími bezpečnostními týmy v rámci celé Evropy – zejména v otázce řešení a koordinace řešení bezpečnostních incidentů. Na úrovni České republiky to pak bylo projednávání možností zapojení jednotlivých týmů do mezinárodní komunity a kroky vedoucí k aktivnímu zapojení.

Vzhledem k probíhajícími opatřením spojeným s pandemií Covid-19 nebylo možné s ohledem na komunitní charakter zorganizovat Pracovní skupinu CSIRT.CZ.

I přes výše zmíněná opatření nedošlo k narušení fungující úzké spolupráce mezi týmem CSIRT.CZ a NÚKIB. Tato dlouhotrvající spolupráce je založená zejména na společném řešení incidentů, sdílení nezbytných informací, stejně jako nejrůznějších odborných konzultacích, zejména mezi Národním bezpečnostním týmem CSIRT.CZ a vládním týmem GovCERT.CZ. Spolu tyto týmy plní povinnosti definované NIS směrnici ve vytvořeném CSIRT Networku, v jehož rámci mimo jiné aktivně spolupracují s dalšími evropskými národními a vládními týmy.

Národní bezpečnostní tým CSIRT.CZ a vládní tým GovCERT.CZ se několikrát ročně setkávají při nejrůznějších příležitostech. Tím je zajištěn dostatečný prostor pro pravidelné informování o práci a činnosti jednotlivých týmů, pravidelná konzultace a případná koordinace spolupráce. Kromě zmíněného se týmy spoluúčastní setkání v rámci TF-CSIRT a dalších mezinárodních komunitních konferencí a meetingů.

V uplynulém roce se podařilo dostat do mezinárodní bezpečnostní komunity hned několik dalších týmů, čímž se ČR dostala na první místo v Evropě v počtu bezpečnostních týmů zapojených v mezinárodní komunitě Trusted Introducer v rámci jednotlivého státu. K závěru roku 2020 bylo zapojeno celkem 51 bezpečnostních týmů z ČR.

Tým se pravidelně účastní virtuálních meetingů a konferencí.

Aktivně pracuje na organizaci a plánování mezinárodního kybernetického cvičení CyberEurope.

Technicko-organizační cvičení CyberEurope bylo po několika týdnech projednávání, během kterých se došlo ke konsenzu mezi jednotlivými plannery kvůli pandemii odloženo.

Kromě této zmíněné spolupráce se tým v oblasti národní i mezinárodní spolupráce angažuje prostřednictvím nejrůznějších konzultací a podpory, kterou poskytuje dalším bezpečnostním týmům.

Závěr

Rok 2020 je vzhledem k probíhající pandemii a velmi ztíženým podmínkám náročné komparovat s předešlými roky. Je třeba nahlížet na změny – ať již pozitivní, tak negativní zvláštní optikou. Tým CSIRT.CZ byl i v době pandemie řízen koncepčně i organizačně tak, že se mu podařilo nejen udržet stávající kvalitu poskytovaných služeb, ale také posunout se vpřed, zejména v oblasti vývoje. Úspěšně se zdařilo také udržet úroveň a pracovat na dalším rozvíjení mezinárodní i národní spolupráce. V neposlední řadě se velmi zdárně podařilo spustit poskytování služby penetračního testování, čímž došlo k rozšíření struktury samotné agendy a úkolů Národního bezpečnostního týmu CSIRT.CZ také v oblasti prevence.

Zcela na závěr, důležitým úspěchem pro tým a sdružení CZ.NIC se stalo publikování a sdílení informací o objevení škodlivého doplňku jedním z členů týmu, Edvardem Rejtharem v několika zahraničních médiích a fórech.