ZPRÁVA O ČINNOSTI CSIRT.CZ (NÁRODNÍHO CSIRT ČR) ZA ROK 2023

CSIRT.CZ

Obsah

O CSIRT.CZ

Tým CSIRT.CZ (Computer Security Incident Response Team České republiky) plní od 1. ledna 2011 roli Národního bezpečnostního týmu ČR (dále jen CSIRT.CZ). Stalo se tak na základě rozhodnutí Ministerstva vnitra České republiky (dále jen MVČR) a uzavření Memoranda o provozu Národního CSIRT.CZ, které MVČR 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 ke zrušení Memoranda o provozování CSIRT.CZ, uzavřeného mezi sdružením CZ.NIC a MVČR v prosinci 2010, a bylo podepsáno nové Memorandum mezi sdružením CZ.NIC a NBÚ. Jelikož mělo toto Memorandum platnost pouze do konce roku 2012, bylo dne 19. prosince 2012 s platností od 1. ledna 2013 uzavřeno mezi sdružením CZ.NIC a NBÚ Memorandum o provozování CSIRT.CZ. 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 NBÚ. Od 1. srpna 2017 je pak na základě zákona č. 205/2017 Sb. ústředním správním orgánem pro kybernetickou bezpečnost Národní úřad pro kybernetickou a informační bezpečnost (dále jen NÚKIB). Uzavřená veřejnoprávní smlouva automaticky přešla pod tento nový správní orgán.

Cílem týmu CSIRT.CZ je především řešení incidentů, které se týkají kybernetické bezpečnosti v sítích provozovaných v České republice. Vedle toho se zaměřuje také na prevenci, výzkum a vzdělávání. CSIRT.CZ shromažďuje a vyhodnocuje data o oznámených incidentech a ta dále předává osobám zodpovědným za chod sítě nebo služby, která je zdrojem daného incidentu, nebo poskytuje koordinační pomoc. Při své činnosti tým spolupracuje se řadou subjektů, se kterými si na základě vzájemné důvěry vyměňuje informace o jednotlivých incidentech a jejich řešeních.

Rok 2023 v kostce

Stále se vyvíjející situace v oblasti bezpečnosti a čím dál profesionalizovanější hrozby a sofistikovanější útoky nás nutí neustále reagovat na nové výzvy. I proto pokračujeme ve vylepšování svých nástrojů, optimalizaci a automatizaci procesů i národní a mezinárodní spolupráci a osvětě. Významnou událostí letošního roku je změna taxonomie, která reaguje na dění v oblasti kybernetické bezpečnosti u nás i ve světě. Počet incidentů i v letošním roce významně vzrostl. Na mezinárodní scéně působí i kvůli válce na evropském území rozličné množství skupin útočníků (APT), jejichž útoky jsou motivované i politicky. Díky naší mateřské organizaci CZ.NIC se nám dařilo velice efektivně bojovat s phishingem v doméně .CZ, a to až do té míry, že se útočníkům v některých případech přestalo vyplácet si registrace na české doméně dělat. V rámci prevence bezpečnostních hrozeb a rizik jsme průběžně prováděli penetrační testování. Ve spolupráci s projektem bezpecnyinternet.cz se nám podařilo odhalit nebezpečnou webovou aplikaci, která by mohla mít za následek zneužití osobních informací dětí. Stále rostoucí aktivita útočníků a velmi časté zneužívání zranitelností nás utvrzuje

v nutnosti úzké spolupráce s Národním úřadem pro kybernetickou a informační bezpečnost a policií.

Spolupracovali jsme dále i s Agenturou Evropské unie pro kybernetickou bezpečnost (ENISA), a to především v rámci skupiny CSIRT Network, při přípravě školení a největšího evropského kybernetického bezpečnostního cvičení Cyber Europe, které proběhne v červnu letošního roku. Spolupráce bezpečnostních týmů probíhala na několika dalších úrovních formou setkávání členů komunity, například v rámci pracovní skupiny CSIRT.CZ, z nichž jedna byla dedikována chystané změně Zákona o kybernetické bezpečnosti. Realizovali jsme několik kurzů a školení a pokračovali jsme také v podpoře bezpečnostních týmů v rámci zapojení do mezinárodních komunit, jako je TF-CSIRT nebo Fénix.

Osvětovou činnost tým realizuje také prostřednictvím pravidelného publikování článků na serveru root.cz pod názvem Postřehy z bezpečnosti, a to ve spolupráci se sdružením CESNET, ke kterému se přidal ALEF-CSIRT, ČD Telematika a Nettles Consulting. Kromě výše uvedeného se tým zaměřuje na osvětu publikováním krátkých aktuálních zpráv na svých webových stránkách, a to pod názvem Aktuálně z bezpečnosti. Samozřejmostí je také publikace článků na blogu zaměstnanců sdružení CZ.NIC, na kterém se v letošním roce dostaly čtyři články našeho týmu do výběru TOP10 nejčtenějších článků.

Více podrobných informací k jednotlivým informacím a službám je možné nalézt vždy pod patřičnými názvy kapitol, které v této výroční zprávě následují.

1. Incident handling

Z pohledu metodologie řešení incidentů zahrnuje fáze naplánování a přípravy, detekce, eskalace, analýzy, samotné reakce a lessons learned.

Pro řádný proces incident handlingu a pro sestavení best practices a prevenci není možné žádnou z těchto fází zcela vynechat. Každý incident tak projde tímto konkrétním cyklem. Na základě reportovaných incidentů tým vede systematicky statistiku řešených incidentů.

1.1. Změna taxonomie

V roce 2023 jsme se pustili do revize taxonomie incidentů, která již dostatečně nereagovala na vývoj kybernetické bezpečnosti v ČR a ve světě. V rámci našeho úsilí o optimalizaci klasifikace bezpečnostních incidentů jsme provedli důkladnou analýzu a revizi existujících kategorií, které jsou s ohledem na povahu naší činnosti poměrně specifické, a použití standardních klasifikací tak není přímo aplikovatelné.

S cílem dosáhnout lepšího porozumění a přehlednějšího rozřazení incidentů jsme se inspirovali existujícími taxonomiemi používanými jinými zeměmi a bezpečnostními týmy zejména v materiálech agentury ENISA, služby Trusted-Introducer a EUROPOLu. Výsledkem této

revize je nová taxonomie, která sjednocuje některé kategorie a vytváří pro lepší pokrytí různých typů incidentů nové.

Konkrétně jsme sjednotili kategorii Malware, do té jsme přidali původní kategorie Virus a Trojan. Vytvořili jsme novou kategorii Information Gathering, do které jsme přidali původní kategorie Probe a Portscan, a kategorie Intrusions nově zahrnuje původní kategorie Botnet a Pharming. Také jsme provedli přetypování některých incidentů, které byly původně zařazeny do kategorie Other, a přeřadili jsme je do kategorií odpovídajících jejich charakteristice. Pro podrobnější informace o jednotlivých typech incidentů, které řešíme, odkazujeme na naše veřejně dostupné materiály dostupné na našem webu.

1.2. Statistiky incidentů v roce 2023

Služba incident handling a incident response (řešení a koordinace řešení bezpečnostních incidentů) je základní službou, kterou týmy CERT/CSIRT plní a musejí plnit v rámci svého definovaného pole působnosti. V případě CSIRT.CZ se jedná o řešení a koordinaci při 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, 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.

Dohromady bylo řešeno 2 752 incidentů, jejich počet tak vzrostl o více než 33 %. Jak je zmíněno výše, došlo k přepracování stávajících statistik, které jsou veřejně dostupné na našem webu. Zároveň jsme optimalizovali zobrazení, které nyní nově zobrazuje pouze pět posledních let, ale celou historii incidentů je možné si stáhnout v .csv formátu pod tabulkou se statistikami. Takto vysoký nárůst incidentů by nebylo možné zvládat bez pokračujícího vývoje ticketovacího systému a další automatizace prováděných úkonů.

STATISTIKA PROCESU ŘEŠENÍ BEZPEČNOSTNÍCH INCIDENTŮ TÝMEM CSIRT.CZ

	2020	2021	2022	2023
Sensor Network*	16 217	10 284	8 815	8 903
Phishing	738	1 277	1 485	2 064
Malware	216	163	220	163
Spam	109	141	224	352
Other	86	58	63	35
Information gathering	68	67	69	105
DOS	0	0	0	12
Intrusions	16	11	0	21
Celkem	**1 267**	**1 725**	**2 067**	**2 752**

* Sensor Network není započten do celkového počtu

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

Jak je patrné z výše uvedené tabulky, objevuje se Phishing mezi nahlášenými incidenty nejčastěji, prudký nárůst tohoto typu útoku pociťují organizace po celém světě.

Významnou kategorií je také Information Gathering, který pomáhá útočníkům identifikovat slabá místa a zranitelnosti v informačních systémech a technologiích. Řešili jsme několik kompromitovaných e-mailových účtů.

Se zmíněným Phishingem se nám daří díky naší domovské organizaci CZ.NIC a jejím pravidlům registrace vypořádávat v doméně .cz velice efektivně, více o tom uvádíme v kapitole 1.3.

Každoroční nárůst počtu incidentů je v letošním roce doprovázen ještě zvýšenou aktivitou tzv. APT (Advanced Persistent Threat). Jedná se o kybernetické útoky, které využívají sofistikovaných technik k infiltraci sítě. Útočníci, kteří jsou do APT útoků zapojeni mají čas i prostředky k tomu, aby si mohli dovolit udržovat nepozorovaný přístup do infrastruktury organizace po dlouhou dobu. Mezi hlavní cíle těchto útoků patří kromě shromažďování citlivých informací, krádeže dat, špionáž a sabotáž. Aktivně tyto hrozby monitorujeme především na základě mezinárodní spolupráce.

Součástí řešení bezpečnostních incidentů je spolupráce s dalšími bezpečnostními týmy nejen v rámci působnosti ČR, ale také v distribuci důležitých informací o zranitelnostech, útocích a dalších. Podrobnější informace viz kapitola Aktuálně z bezpečnosti a Národní a mezinárodní spolupráce. Mimo součinnost s dalšími bezpečnostními týmy spolupracuje CSIRT.CZ při řešení reportovaných incidentů také s orgány státní správy, s Policií České republiky (dále jen PČR) a dalšími subjekty.

V roce 2023 jsme s PČR spolupracovali na desítkách incidentů s původem především v cizích zemích. Jednalo se podobně jako v minulých letech o:

- phishingové kampaně,
- falešné e-shopy,
- podvodné jednání na inzertních portálech,
- podvodné weby, které nabízejí investice do virtuálních měn.

Řešení bezpečnostních incidentů vyžaduje nejen spolupráci se specializovanými pracovišti PČR, ale s ohledem na to, že většina podvodného obsahu se nachází v zahraničí, také spolupráci mezinárodní.

1.3. Vývoj open-source nástrojů a utilit

Rychlost a efektivitu v otázce incident handlingu a při procesu řešení bezpečnostních incidentů mimo jiné ovlivňuje také samotný pokrok při vývoji open-source nástrojů a utilit. Nově vytvořené či zdokonalené nástroje a utility napomáhají informace mezi jednotlivými relevantními subjekty rychleji sdílet.

Za účelem zkvalitňování řešení procesu incident handlingu, usnadnění a zefektivňování spolupráce na národní i mezinárodní úrovni dochází k neustálému vývoji systémů, nástrojů a doplňků, které tým CSIRT.CZ používá.

Tým se také účastní různých mezinárodních workshopů určených pro vládní a národní týmy zaměřené na best practices. Na základě zkušeností a praktických doporučení vývojářů z jiných evropských CSIRT/CERT týmů můžeme zdokonalit vývoj vlastních nástrojů.

Před několika lety tým vyvinul vlastní open-source nástroj Convey, který nám umožňuje hromadně analyzovat incidenty týkající se velkého počtu konstituentů a automatizovat komunikaci, které se účastní několik stran. Kromě jiného nám umožňuje práci s kvótami LACNICu a převod mezi 50 datovými typy konkrétních hodnot. Během zmíněného období jsme se věnovali rozvoji nových funkcí, které adekvátně reagují na dění v rámci naší konstituence a také potřeby PČR.

Zpřehlednili jsme nakládání s daty obdrženými od policie a rozšířili možnosti práce s textem, což zahrnuje schopnost připojovat k textovým datům i snímky obrazovky. Tato funkce byla klíčová při zpracování várky snímků, které jsme obdrželi a které bylo nutné hromadně distribuovat. Obvykle distribuujeme pouze seznam napadených IP adres, nicméně v tomto případě bylo nezbytné rozeslat i snímky obrazovky napadených e-mailových schránek. Další vylepšení zahrnuje možnost spojování tabulek a podporu pro import formátu XLSX, čímž jsme zjednodušili práci s různorodými datovými soubory. Vylepšili jsme také manipulaci s regulárními výrazy, což přispívá k efektivnějšímu a přesnějšímu zpracování dat.

Convey je podobně jako další nástroje, které vyvíjíme, využíván v rámci práce s incidenty v OTRS.

Knihovna Envelope, která se v roce 2022 v komunitě pyšnila velkým úspěchem, v letošním roce nově pomáhá v rámci našich nástrojů PROKI, OTRS i Convey lépe načítat hlavičky e-mailů v nestandardních kódováních. Novinkou pro efektivní práci s velkým množstvím adresářů a souborů je nástroj s příznačným názvem Orgafold.

Co se týká našeho nástroje pro správu incidentů OTRS, zlepšili jsme detekci textu v obrázcích a .pdf souborech. Byly nám často zasílány pouze snímky obrazovky textových zpráv, ze kterých bylo potřeba extrahovat webové odkazy.

Některé větší společnosti neumožňují přijímat hlášení o problémech prostřednictvím e-mailu a požadují použití svých vlastních webových portálů. Dříve jsme museli manuálně vyplňovat dlouhé formuláře na těchto portálech, nyní je po úspěšné integraci dokážeme automaticky předvyplnit. Vylepšili jsme zobrazování e-mailů pro snazší a rychlejší triage incidentů. Díky již zmíněnému nástroji Convey jsme nyní schopni hromadně posílat obrázky různým adresátům. To nám umožňuje efektivně sdílet snímky obrazovky při vyšetřování napadených e-mailových schránek a podobně.

Pro radost nejen sobě, ale i druhým, kteří čas od času potřebují své zkušenosti sdílet s ostatními například v podobě kurzů, se na závěr této kapitoly s vámi můžeme podělit ještě o online program pro prezentaci Slidershow. Jeho silnou stránkou jsou především média – fotky a videa. Tento program má proti prohlížeči obrázků na Windows, Nomacs na Linuxu nebo VLC několik podstatných výhod: udržuje malou velikost výsledného souboru, který odkazuje na velké množství médií, jednoduše se v něm stříhají videa bez zásahu do originálu, pomůže s organizací obsahu prezentace. My jsme jej využili například pro tvorbu jednoho z kurzů, který nabízíme v naší Akademii.

1.4. Boj s phishingem v doméně .cz

V posledních letech dochází celosvětově k velkému nárůstu phishingových stránek. Tento trend koresponduje i s incidenty nahlášenými Národnímu bezpečnostnímu týmu CSIRT.CZ. Zatímco se v roce 2022 počet námi řešených incidentů v této kategorii zastavil na čísle 1 485, v roce 2023 jsme na čísle 2 064. Naše statistiky přitom odrážejí pouze malou část celkového

počtu útoků, protože Národní CSIRT funguje jako tzv. „last resort" tým, tedy krajní řešení, a je nám tak hlášena pouze malá část útoků.

Za velký úspěch považujeme svou aktivitu týkající se phishingové kampaně napodobující aktivity MPSV a pod něj spadajících institucí. Od ledna jsme zaznamenali 125 phishingových útoků zneužívajících .CZ domény. Díky informacím z projektu ADAM a s využitím článku 17.1. Pravidel registrace jmen domén v zóně .CZ se nám podařilo úspěšně zastavit registrace ve 114 případech. Již od roku 2022 jsme zlepšovali monitorování podvodných domén a jejich následné vyřazování. Tento proces jsme nastavili natolik precizně, že jsme byli brzy schopni doménu blokovat ještě před tím, než nám přišla první hlášení od uživatelů, a v některých případech dokonce do 15 minut od jejího zpřístupnění (v takovém případě nám první hlášení přišla až v době, kdy byl web již zablokovaný). Od ledna do poloviny března jsme tímto způsobem zablokovali 109 domén. Od března jsme obdrželi hlášení už jen na šest podezřelých registrací z nichž pět bylo validních. V srpnu tak byla registrována poslední podezřelá doména (www.1-ibfio.cz). Útočníci po neúspěšných pokusech zjistili, že jsme jejich kroky schopní do jisté míry předvídat a přesunuli svou aktivitu jinam. Nepodloženou domněnkou, která je však z našeho pohledu velmi pravděpodobná, je, že se útočníkům nevyplatí podvodné domény v zóně .CZ i díky synergii týmu CSIRT.CZ a jeho mateřské organizace CZ.NIC již dále registrovat.

1.5. Identifikace kompromitovaných webů

Kromě výše uvedených pravidelných aktivit zaměřených na prevenci jsme v roce 2023 realizovali také jednorázovou preventivní akci zaměřenou na dohledání dlouhodobě kompromitovaných webů v doméně .CZ. Na základě analýzy staršího incidentu se nám s využitím výstupů z projektu ADAM podařilo identifikovat domény, o jejichž kompromitaci jejich provozovatelé vůbec nevěděli. Celkem takovýchto webů bylo nalezeno 95 a všichni jejich provozovatelé byli o jejich kompromitaci informováni.

2. Skener webu

V oblasti prevence tým poskytuje od roku 2013 bezpečnostní službu nazvanou 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 zranitelností 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 2023 došlo k testování 14 webových aplikací, a to na základě 9 podaných objednávek. V rámci spolupráce na soutěži Zlatý Erb jsme poskytli bezpečnostní audit webových aplikací finalistům celostátního kola. Provedli jsme základní bezpečnostní kontrolu 15 webů a podle předem vytvořených kritérií jsme je ohodnotili. Pro každý web jsme sepsali finální zprávu s nálezy, kterou jsme předali jednotlivým správcům sítě. Bezpečnost webů byla v letošním roce v rámci této soutěže hodnocena vůbec poprvé.

2.1. Automatické testování pro školy

V rámci interní spolupráce na projektu bezpecnyinternet.cz jsme spustili službu automatického testování webových prezentací pro instituce, které se věnují práci s dětmi. Primárně se tedy jedná o školy, nicméně o pravidelné testování projevily zájem i další obdobné subjekty. V rámci testů se mimo jiné podařilo odhalit velmi nebezpečnou webovou aplikaci nabízenou na komerční bázi, která obsahovala zásadní zranitelnosti umožňující získat přístup k osobním informacím o dětech i zaměstnancích. Aktuálně se pravidelné testování týká 28 subjektů, v roce 2023 jich bylo 26. Více informací o této aktivitě jsme publikovali v našem blogpostu.

3. Honeypoty

Mezi další aktivity spadající mimo rámec obligatorních činností definovaných Zákonem o kybernetické bezpečnosti patří provozování honeypotů.

Na linuxových honeypotech Cowrie jsme v roce 2023 zaznamenali 77 unikátních vzorků malware. Pravidelné čtenáře našich výročních zpráv může zarazit významný pokles, který je způsoben přechodem na novou verzi, kdy jsme nějaký čas vzorky nemohli sbírat. Dionea v letošním roce přestala být podporována.

HAAS STATISTIKY

Počet registrovaných uživatelů	6 565
Počet spojení/útoků	75 007 272
Počet provedených příkazů	33 081 165
Počet unikátních útočících IP adres	132 749
Počet zachyceným unikátních vzorků	95 843

4. PROKI

V roce 2015 zahájil Národní bezpečnostní tým CSIRT.CZ realizaci projektu PROKI; VI20152020026, podpořeného v rámci Programu bezpečnostního výzkumu České republiky 2015–2020. V technické oblasti vývoje softwarového řešení projekt sleduje tři hlavní cíle.

Prvním cílem 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 naopak 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 ohrožená nebo již kompromitovaná zařízení.

V této analytické činnosti tým i po roce 2020 nadále pokračuje. V případě odhalení nakažených strojů, jejichž kompromitace nebyla na první pohled zřejmá, jsou dle standardního postupu 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.

Informace jsou rozesílány prostřednictvím e-mailu na tzv. abuse kontakt. Je možné, aby se správci dotazovali na data skrze REST API. Přestože rok 2020 formálně znamenal poslední rok běhu projektu, tým CSIRT.CZ i nadále pokračuje v provozování, využívání a rozvíjení PROKI. Za účelem zkvalitňování získaných informací jsou prováděny pravidelné revize zdrojů dat, vyhledávány nové zdroje, případně vyřazovány ty, které již nejsou nadále relevantní. Systém je založen na open-source technologiích vyvíjených komunitou, tým CSIRT.CZ však usiluje o další rozvoj přispěním vlastního kódu a zapojováním se do diskusí o budoucím směřování vývoje.

V roce 2021 začal tým spolupracovat s projektem Turris Sentinel, který pomáhá detekovat útočníky skrze vyhodnocování firewallových logů, provozováním tzv. minipotů (tedy miniaturních honeypotů) a také plnohodnotných honeypotů (HaaS). Do tohoto projektu mohou vlastníci a provozovatelé routerů Turris dobrovolně zapojit svá zařízení, která jsou zapojena v různých sítích a na různých geografických místech, a stát se tak součástí distribuované sítě bezpečnostních sond. V této spolupráci tým pokračoval i v roce 2022, kdy se podařilo zvětšit diskové kapacity, proběhl upgrade IntelMQ na verzi 2 a proběhl úspěšný upgrade na verzi 3.

V roce 2023 jsme se zaměřili na stabilizaci systému a jeho snadnější správu. Byla vytvořena nová dokumentace k IntelMQ a zjednodušena konfigurace. Zároveň došlo k vytvoření nových botů a rozšíření stávajících o nové vlastnosti. Kvůli úspoře místa jsme také zefektivnili ukládání dat v databázi. Zároveň došlo z důvodů úspor k ukončení projektu MDM a přesunutí agendy tohoto systému do projektu PROKI.

Pokračovala také analýza výstupů z minipotů Turris pomocí separátní části PROKI, kde jsou

evidovány desítky milionů událostí za den. Nejčastější útoky evidujeme z Íránu a Rumunska. Nejčastější hesla, kterými se útočníci snaží dostat do systémů, jsou 123456, admin, <prázdné>, anonymous, QWE-!@# či root.

Byly detekovány také některé komplexnější útoky, jako například útoky na WEB servery v českých doménách, kdy docházelo ke snahám odhadnout heslo k ftp úložišti s cílem modifikovat stránky WEB serveru.

Výstupy z projektu Turris Sentinel jsou využívány pro bezpečnostní analýzy v rámci činnosti týmu a jsou ukládány spolu s daty ze systému PROKI.

Statistika k PROKI za rok 2023	Počet
Počet odeslaných emailů z PROKI	34 718
Počet unikátních příjemců (abuse kontaktů) PROKI hlášení	726
Počet unikátních českých IP adres, které jsme nějakým způsobem zaznamenali	50 265

5. Penetrační a zátěžové testování

V roce 2023 bylo úspěšně provedeno penetrační testování několika komerčních subjektů a zátěžové testování významného zákazníka z veřejné správy. Penetrační testování podstoupily i vybrané části registru domény .CZ.

6. Osvěta a vzdělání

V oblasti školení a vzdělávání bylo opět ve spolupráci s Akademií CZ.NIC realizováno školení Bezpečnost a soukromí na Internetu, které je zaměřeno na nejčastější hrozby v oblasti kybernetické bezpečnosti. Rozpoznání hrozeb a rizik směřuje k pochopení, prevenci a seznámení uživatelů s aktivními a pasivními digitálními stopami, zásadami bezpečného chování, soukromím a anonymitou na Internetu. Kromě uvedeného školení jsme realizovali školení na míru pro Státní úřad pro jadernou bezpečnost nebo ve spolupráci se Stoponline školení pro Policii ČR v Karlovarském kraji. Zaměřili jsme se také na zvláště zranitelnou skupinu školením pro seniory, podařilo se nám totiž navázat spolupráci s organizací Stárneme ve zdraví, a také jsme pokračovali v již existující spolupráci s Městskou policií v Mikulově. Zkušenosti z vlastního vývoje, automatizace a úprav jsme pak přetavili do kurzu programovacího jazyka Python v Akademii CZ.NIC.

Znalosti, zkušenosti a aktivity jsou publikovány na blogu sdružení CZ.NIC. V roce 2023 i nadále vycházel seriál Myš je pro kočku. Kromě toho členové bezpečnostního týmu publikovali články popisující naše zkušenosti s bojem s phishingovými doménami, ale v příspěvcích na blogu také reagovali na neustálý nárůst případů sociálního inženýrství, které zdaleka

nezahrnuje pouze phishingové útoky. Jak jsme již v úvodu zmínili do TOP10 blogpostů roku 2023 se tak dostaly hned čtyři články publikované členy našeho týmu.

CSIRT.CZ se také již tradičně věnoval prezentaci vlastních zkušeností na nejrůznějších fórech a konferencích. Z vystoupení pro odbornou veřejnost lze jmenovat například vystoupení na TF-CSIRT meeting akcích, prezentaci pro NatCSIRT, Kam kráčí digitální sítě nebo na akci Internet a Technologie. V rámci aktivit pro širokou veřejnost jsme pak využili možnost zapojit se do akce Czech Digital week, kde jsme prezentovali jak praktické zkušenosti týmů CSIRT.CZ a CZ.NIC-CSIRT, tak i zkušenosti z provozování linky STOPonline.cz. Mezi další osvětové aktivity, kterým se tým dlouhodobě věnuje, patří publikování aktualit ze světa bezpečnosti. Nadále 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 a aktuality.

7. Aktuálně z bezpečnosti

I v roce 2023 jsme pokračovali v aktivní spolupráci se serverem root.cz s vlastním seriálem *Postřehy z bezpečnosti*. Jedná se o pravidelný bezpečnostní přehled uplynulých dní, k jehož publikování jsme se spojili s týmy ALEF-CSIRT, ČD Telematikou, zakladatelem organizace Nettles Consulting Janem Kopřivou a již tradičně nadále spolupracujeme se sdružením CESNET.

Publikované informace poukazují na nejzajímavější události, aktuality, stejně jako i zranitelnosti, kterým by měla být věnována pozornost. V roce 2023 tým publikoval celkem 12 příspěvků. V rámci seriálu bylo publikováno celkem 52 článků.

Kromě seriálu *Postřehy z bezpečnosti* je možné sledovat na webových stránkách týmu CSIRT.CZ sekci *Aktuálně z bezpečnosti* (dále jen AZB), která je určena k rychlému a stručnému šíření nejpodstatnějších informací o aktuálně probíhajících útocích a objevených zranitelnostech. Sekce AZB je 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 běžné uživatele.

8. Národní a mezinárodní spolupráce

V roce 2023 tým CSIRT.CZ pokračoval v intenzivní spolupráci s ostatními týmy zabývajícími se kybernetickou bezpečností, a to jak na národní tak mezinárodní úrovni.

Co se týká národní spolupráce, proběhla dvě setkání pracovní skupiny CSIRT.CZ. První setkání proběhlo v únoru jako reakce na chystanou změnu Zákona o kybernetické bezpečnosti. Zástupci z Národního úřadu pro kybernetickou a informační bezpečnost v jeho rámci členy pracovní skupiny seznámili s hlavními body plánu transpozice NIS2 v České republice. Další setkání proběhlo na podzim a účastníci si v jeho rámci poslechli řadu zajímavých přednášek. Každého setkání se účastnilo okolo osmi desítek členů. Zajímavou akcí na národní úrovni

bylo také Table Top cvičení organizované Úřadem. V rámci tohoto cvičení jsme měli možnost prezentovat zástupcům z telekomunikačního sektoru svou činnost a apelovat na důležitost spolupráce.

Co se týká mezinárodní spolupráce, tak jsme společně s Úřadem prezentovali práci v oblasti kybernetické bezpečnosti v České republice delegacím z Albánie, Islandu, Kolumbie a Estonska.

Dalšími důležitými činnostmi na poli mezinárodní kybernetické bezpečnosti jsou obligatorní aktivity vyplývající ze směrnice NIS a Zákona o kybernetické bezpečnosti. Specifickým druhem spolupráce je pravidelná a úzká součinnost národního bezpečnostního týmu CSIRT.CZ a vládního týmu GovCERT.CZ v rámci sítě CSIRTs Network etablované na základě evropské NIS směrnice. Síť CSIRTs Network sdružuje národní a vládní týmy členských států Evropské unie. Tato tradiční spolupráce mezi národním CERT týmem (CSIRT.CZ) a NÚKIB (vládním týmem GovCERT.CZ) je založena zejména na společném řešení incidentů, sdílení nezbytných informací, stejně jako nejrůznějších odborných konzultacích. Spolu tyto týmy plní povinnosti definované směrnicí NIS 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 sdílení informací o práci a činnosti jednotlivých týmů, pravidelná konzultace a případná koordinace spolupráce. Tým CSIRT.CZ aktivně pracuje na organizaci a plánování mezinárodního kybernetického cvičení Cyber Europe, které proběhne již v červnu 2024. Pracovní skupina CSIRT Network uspořádala v roce 2023 několik pracovních skupin a téměř tři desítky online setkání se zástupci dalších členských států Evropské unie, členů CERT-EU a zástupců Evropské komise. Hlavním cílem těchto setkání je výměna aktuálních informací mezi členskými státy EU.

Zapojení do mezinárodní komunity Trusted Introducer se nám v letošním roce podařilo rozšířit o členství v řídícím výboru organizace TF-CSIRT. Pro CSIRT.CZ a českou bezpečnostní komunitu to znamená, že máme po dobu tří let přímý vliv na směřování, činnost a vývoj komunity která čítá přes 500 týmů zabývajících se kybernetickou bezpečností napříč Evropou. TF-CSIRT sdružuje profesionály z řad kybernetické bezpečnosti napříč sektory. Česká republika má i díky podpoře FÉNIXu v současné době 65 členských týmů, z toho 4 certifikované, 20 akreditovaných a 41 zalistovaných (jeden tým v současné době čeká na recertifikaci). V rámci mezinárodního sdružení incident response týmů FIRST má Česká republika aktuálně šest zapojených týmů a jednoho Liasion člena. V rámci TF-CSIRT setkání jsme v průběhu roku 2023 prezentovali komunitě kromě činnosti týmu přednášku na téma DGA Botnets, DDoS jako služba, kterou nabízíme, ale podařilo se nám ve zkratce představit i projekt Turris Sentinel nebo HaaS.

Podíleli jsme se také na oficiálním překladu TLP protokolu a konzultovali jsme se studenty vysokých škol jejich závěrečné práce týkající se kybernetické bezpečnosti.

Kromě výše zmíněného tým v oblasti zajištění národní i mezinárodní bezpečnosti spolupracuje s dalšími bezpečnostními týmy i subjekty, a to prostřednictvím nejrůznějších konzultací a podpory, kterou poskytuje.

Závěr

Stále se vyvíjející situace v oblasti bezpečnosti spolu s rostoucí profesionalizací hrozeb a sofistikovanějšími útoky nás neustále nutí čelit novým výzvám. Vylepšování našich nástrojů, optimalizace a automatizace procesů a posilování národní i mezinárodní spolupráce a osvěta jsou pro nás nutností a jsme rádi, že jsme i přes enormní nárůst incidentů v uplynulých letech dokázali udržet vysokou kvalitu poskytovaných služeb. Úzká spolupráce s naší mateřskou organizací CZ.NIC, díky které jsme úspěšně bojovali s phishingem v doméně .CZ, a to až do té míry, že se útočníkům přestalo téměř vyplácet registrovat podvodné domény v zóně .CZ, je skvělým příkladem toho, jaký dopad má důsledná, promyšlená, avšak přesto rychlá reakce. A jak moc je takový přístup v současném světě potřebný. V následujícím roce nás pravděpodobně čeká implementace nového Zákona o kybernetické bezpečnosti, která je reakcí na stále se zvyšující negativní dopady na poli kybernetické bezpečnosti. Závěrem nám všem přejeme bezpečný rok 2024 a těšíme se, třeba na setkání pracovní skupiny CSIRT.CZ, na viděnou.