ZPRÁVA O ČINNOSTI CSIRT.CZ (NÁRODNÍHO CSIRT ČR) ZA ROK 2024

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 s řadou subjektů, se kterými si na základě vzájemné důvěry vyměňuje informace o jednotlivých incidentech a jejich řešeních.

Rok 2024 v kostce

Rok 2024 byl pro CSIRT.CZ obdobím hned několika významných změn ať již provozních, či organizačních. Poprvé od počátku pandemie COVID-19 jsme zaznamenali pokles řešených incidentů. To může být důsledkem kombinace několika faktorů: ať již pozitivních ve smyslu lepší informovanosti uživatelů, tak i negativních ve smyslu útoků, které mohou být natolik sofistikované a nové, že je současné nástroje nejsou schopny detekovat.

Osvětu považujeme za důležitý pilíř kybernetické bezpečnosti, a proto jsme se již po dvanácté stali koordinátorem Česka pro mezinárodní cvičení Cyber Europe. Současně jsme se věnovali přípravě na přijetí nového zákona o kybernetické bezpečnosti, který ovlivní mnoho činností a služeb a vyžádá si úpravy procesů i technologií.

Další významnou změnou byl přechod na nový ticketovací systém, který se nám podařilo implementovat natolik precizně, že si jeho uživatelé této jinak velmi významné změny téměř nevšimli, a mohli jsme tak nadále nerušeně pokračovat v zefektivňování správy incidentů a

zlepšovat komunikaci s našimi partnery. Pokračovali jsme v rozvoji našeho komunitou velmi ceněného projektu PROKI i v osvětové činnosti v podobě školení, účasti na přednáškách a akcích či formou publikování odborných článků a novinek, v rámci kterých jsme sdíleli klíčové poznatky z naší činnosti a upozorňovali na nové hrozby v kybernetickém prostředí.

Kromě dalšího zlepšování již existujících nástrojů byla v roce 2024 vytvořena nová utilita, která usnadňuje přidávání nových nebezpečných domén do nástroje Deny listy.

Výroční zpráva 2024 přináší detailní pohled na naši činnost, výzvy, kterým jsme čelili, a kroky, které jsme podnikli pro posílení bezpečnosti českého internetu.

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.

V roce 2024 jsme čelili výzvě, kterou byla změna ticketovacího nástroje - OTRS, jehož poslední open-source verze již nebyla udržována a představovala potenciální bezpečnostní hrozbu. Po pečlivé analýze jsme přešli na alternativní software, který vyhovuje našim požadavkům, umožňuje integraci všech našich doplňků, jež potřebujeme pro efektivní zvládání hlášení, a zároveň je vydáván pod svobodnou licencí. Do budoucna by mělo nasazení tohoto nástroje usnadnit také integraci systémů národního CSIRT a systémů Národního úřadu pro kybernetickou a informační bezpečnost, která bude nezbytná po přijetí nového zákona o kybernetické bezpečnosti.

1.1. Statistiky incidentů v roce 2024

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.

Kromě incidentů, které v rámci naší působnosti řešíme na základě zákona, řešíme také hlášení veřejnosti týkající se incidentů a událostí. V roce 2023 jsme provedli optimalizaci klasifikace bezpečnostních incidentů s cílem dosáhnout lepšího porozumění a přehlednějšího rozřazení incidentů. Změna taxonomie se do jisté míry odrazila v celkové statistice incidentů, avšak neměla vliv na to, že se celkový počet námi řešených incidentů snížil.

Dohromady bylo řešeno 2 283 incidentů, jejich počet se tak poprvé od roku 2019 snížil, a to o více než 17 %. Od přepracování statistik se na našem webu zobrazuje pouze pět posledních let, ale celou historii incidentů je možné si stáhnout v .csv formátu pod tabulkou se statistikami. I přes mírný pokles incidentů pokračujeme s vývojem a automatizací pro incident response tým.

STATISTIKA PROCESU ŘEŠENÍ BEZPEČNOSTNÍCH INCIDENTŮ TÝMEM CSIRT.CZ

	2021	2022	2023	2024
Sensor Network*	10 284	8 815	8 903	9 682
Phishing	1 277	1 485	2 064	1 690
Malware	163	220	163	108
Spam	141	224	352	260
Other	58	63	35	53
Information gathering	67	69	105	99
DOS	0	0	12	4
Intrusions	11	0	21	69
Celkem	**1 725**	**2 067**	**2 752**	**2 283**

* 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).

Pro podrobnější informace o jednotlivých typech incidentů, které řešíme, odkazujeme na veřejné materiály dostupné na našem webu.

Od roku 2019 docházelo každoročně k výraznému nárůstu počtu námi řešených incidentů. Letošní rok je tedy od pandemie poprvé pozitivní změnou. Jak však ukazují celosvětové statistiky, mírný pokles unikátních phishingových stránek se může velmi rychle proměnit v opačný trend.

Díky naší synergii se sdružením CZ.NIC máme možnost proaktivně vyhledávat potenciálně škodlivé domény v zóně .CZ a rozvíjet naši schopnost rychle eliminovat phishingové weby tak, abychom útočníky odradili od jejího využívání. Statistiky nám nahlášených incidentů korespondují s mírným poklesem kybernetické kriminality a ostatní kriminality páchané v kyberprostoru, kterou uvádí Policie ČR. S tou na řešení incidentů úzce spolupracujeme a stejně jako v minulých letech jsme i letos řešili především phishingové kampaně, podvodné jednání na inzertních portálech, falešné e-shopy a také falešné investiční platformy.

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, o které se více rozepisujeme v kapitole č. 8 – Národní a mezinárodní spolupráce.

Neoddělitelnou součástí řešení bezpečnostních incidentů je spolupráce s dalšími bezpečnostními týmy nejen v rámci působnosti ČR. V rámci národní a mezinárodní spolupráce sdílíme s ostatními bezpečnostními týmy informace o zranitelnostech, incidentech a další důležité informace o hrozbách a rizicích. Podrobnější informace viz kapitola Aktuálně z bezpečnosti a Národní a mezinárodní spolupráce. Mimo součinnost s dalšími bezpečnostními týmy a PČR spolupracuje CSIRT.CZ při řešení reportovaných incidentů také s dalšími orgány státní správy.

Závěrem této kapitoly upozorňujeme, že ať už se jedná o statistiky incidentů, které jsme řešili my, PČR nebo NÚKIB, tyto statistiky neodrážejí celkový počet incidentů v Česku ani ve světě.

1.2. 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.

Spolupráce na vývoji open-source nástrojů a podpora projektů vydávaných pod svobodnými licencemi je pro nás velmi důležitá. I proto jsme letos učinili významný krok a upgradovali

jsme z již nepodporovaného komunitního vydání OTRS na nový software pro správu incidentů, který je v souladu s naší filozofií. Tomuto kroku předcházela rozsáhlá analýza dostupných nástrojů. Přestože šlo o náročný proces od výběru vhodného softwaru přes jeho implementaci a integraci všech již vyvinutých doplňků až po úspěšné nasazení do produkce, v současné době již vše funguje, jak potřebujeme, a to na zcela nové platformě se svobodnou licencí. Do budoucna by mělo nasazení tohoto nástroje usnadnit také integraci systémů Národního CSIRT a Národního úřadu pro kybernetickou a informační bezpečnost, která bude po přijetí nového zákona o kybernetické bezpečnosti nezbytná.

Tým se také účastní 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 zdokonalovat 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 whoisu a převod mezi 50 datovými typy konkrétních hodnot. Během zmíněného období jsme udělali menší úpravy, díky kterým jsme opět komunikaci o trochu vylepšili.

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

Pro bezpečné zpracování e-mailů používáme knihovnu Envelope. Ta umožňuje ověřování podpisů, šifrování a dešifrování zpráv v souladu s bezpečnostními standardy. V rámci naší snahy o zajištění vyšší spolehlivosti a bezpečnosti jsme přepsali část kódu aplikace, abychom mohli využít robustnější a modernější knihovnu pro S/MIME kryptografii. Tato změna nejenže zlepšila její výkon a stabilitu, ale také zajistila lepší kompatibilitu s aktuálními bezpečnostními požadavky. Knihovna Envelope se již dlouhodobě těší úspěchu napříč bezpečnostní komunitou.

Další projekt našeho týmu není primárně bezpečnostním projektem, na bezpečnost a efektivitu poskytování našich služeb má však přímý dopad. Jedná se o Mininterface, který výrazně zjednodušuje tvorbu uživatelských rozhraní pro Python aplikace. Tento nástroj umožňuje automatické generování CLI, TUI nebo GUI aplikací z běžných datových tříd, jako jsou dataclass, pydantic model či attrs, a to bez nutnosti zásadních úprav kódu či složitého učení. Vývojáři oceňují zejména jeho schopnost minimalizovat množství kódu potřebného pro implementaci uživatelského rozhraní, což potvrzují i pozitivní ohlasy na platformě Reddit. V oblasti bezpečnosti může mininterface usnadnit vývoj nástrojů pro správu konfigurací či monitorování systémů, čímž přispívá k efektivnějšímu a bezpečnějšímu provozu IT infrastruktur a minimalizaci chyb, které by mohly vést k bezpečnostním problémům.

K lepší správě a datové bezpečnosti přispívají i další knihovny. Deduplidog, která pomáhá organizovat soubory odstraněním duplicit, což pomáhá při forenzní analýze, jindy šetří místo a může i zabránit vzniku zmatků s větším počtem verzí citlivých dokumentů. Touch-timestamp potom umožňuje změnu časových značek souborů, což je užitečné při synchronizaci a archivaci souborů.

1.3. Boj s phishingem v doméně .cz

Poprvé od roku 2019 došlo k poklesu počtu námi řešených incidentů spojených s phishingem. Jak jsme zmiňovali výše, pokles je způsoben kombinací poklesu počtu celosvětově zaznamenaných phishingových stránek a naší proaktivní činností týkající se důrazu na bezpečnost v zóně .CZ.

V předchozím roce jsme nejen v naší výroční zprávě uváděli, že svou aktivitu týkající se phishingových kampaní považujeme za velký úspěch. To se nám v letošním roce potvrdilo a můžeme se pochlubit, že se nám podařilo oproti předchozímu roku snížit počet phishingových stránek v doméně .CZ o 80 %.

V roce 2024 jsme zaznamenali oproti 125 z předchozího roku pouze 26 phishingových útoků. Můžeme tedy s jistotou říci, že díky kombinaci informací z projektu ADAM a využití článku 17.1. Pravidel registrace jmen domén v zóně .CZ se nám daří nad očekávání úspěšně potírat phishingové útoky na stránkách v naší zóně.

Ve spolupráci s kolegy z oddělení ověřování domén se nám navíc podařilo znemožnit falešnému kontaktu provozovat v naší zóně více než 90 domén typu help01desk.cz, helpdesk-user.cz, help06desk.cz, help09desk.cz nebo optmail-box.cz.

Již od roku 2022 jsme zlepšovali monitorování podvodných domén a jejich následné vyřazování. Tento proces jsme nastavili natolik precizně, že jsme nyní schopni domény blokovat ještě před tím, než nám přijde první hlášení od uživatelů, a v některých případech dokonce do 15 minut od jejího zpřístupnění.

Důvodem, že se nám daří tak efektivně proti phishingu bojovat je fakt, že za phishingovými útoky stojí lidé, jimž se nevyplatí věnovat nadměrné úsilí vytváření stránek v doméně .cz, když opakovaně zjišťují, že jsme jejich kroky schopni do jisté míry předvídat, a přesouvají tak svou aktivitu tam, kde to pro ně není tak komplikované. Synergie týmu CSIRT.CZ a jeho mateřské organizace CZ.NIC tak nabývá stále většího významu. Dalším důvodem uvedeného poklesu je i zmíněná osvěta – na téma phishingu jsme také my před Vánoci publikovali podařený blogpost detailně popisující modus operandi útočníků.

1.4. Deny listy

V roce 2024 se nám podařilo uvést nový komerční produkt Deny listy. Původně byla tato služba zamýšlena týmem CSIRT.CZ pro nasazení zdarma na ODVR serverech sdružení, díky spolupráci s obchodním oddělením se ovšem podařilo přetavit původní myšlenku do komerčního projektu, kdy jsou výstupy nabízeny za úplatu poskytovatelům internetového připojení a dalším subjektům. Podstatou je produkování seznamu domén, které jsou pro koncové uživatele škodlivé, typicky obsahují phishing, falešný e-shop, podvodnou investiční příležitost a podobně.

Díky své činnosti se o takovýchto doménách dozvídáme jako první. Velmi rychlé reakce jsme však schopní pouze u domény .CZ, v ostatních případech jsme závislí na spolupráci se zahraničními partnery. Proto vítáme možnost pomáhat providerům chránit uživatele v České republice před těmito hrozbami dříve, než dojde k jejich eliminování zahraničními subjekty. Kromě dat získávaných z procesu řešení incidentů tvoří důležitou součást také výstupy z projektu PROKI, u kterého jsou zároveň zpracovávána a vytěžována data z dalších projektů sdružení, jako projekt Turris nebo honeypoty.

S nasazením produktu počítáme i v dalších komerčních projektech sdružení, jako jsou router Turris nebo některé projekty Labs.

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 svých internetových prezentací. Služba je určena 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 návrh konstruktivního řešení. Analýza potenciálních zranitelností vychází nejen z vlastních testů 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 2024 jsme obdrželi 16 žádostí, 11 z nich bylo schváleno, 1 částečně (pouze 1 doména ze 3 poptávaných), 4 žádosti nebyly schváleny. Testováním prošlo 17 domén z 31 a dohromady jsme odeslali 12 výstupů. Důvodem toho, že jsme některým poptávkám prozatím nemohli vyhovět, bylo jejich navrácení k projednání, jelikož žadatelé, kteří objednávku zasílali nebyli držiteli domény ani držiteli zákonného oprávnění za tohoto jednat.

V rámci spolupráce s projektem Zlatý Erb jsme poskytli bezpečnostní audit webových aplikací 12 obcím s rozšířenou působností a dalším webovým portálům měst a obcí a podle předem dohodnutých 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 hodnocena podruhé v historii této soutěže, ovšem v letošním roce jí byla věnována zvláštní pozornost, která se promítla i do názvu soutěže příznačně nazvaného „Ročník kybernetické bezpečnosti“. O této spolupráci naleznete více informací v kapitole č. 6, Osvěta a vzdělávání.

2.1. Automatické testování pro školy

V rámci interní spolupráce na projektu Bezpecnyinternet.cz byla v roce 2023 spuštěna služba 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. Aktuálně probíhá spolupráce s 30 subjekty, které jsou testovány pravidelně po 3 měsících. Dva další subjekty požádaly v průběhu roku 2024 o otestování, které jim sloužilo pouze ke zjištění aktuálního stavu. Po zjištění zranitelností zjednaly subjekty v systémech nápravu a další spolupráci nepožadovaly.

3. Honeypoty

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

Na linuxových honeypotech Cowrie jsme díky postupnému vylepšování zaznamenali desítky tisíc vzorků.

HAAS STATISTIKY

Počet registrovaných uživatelů	12 211
Počet spojení/útoků	50 403 867
Počet provedených příkazů	23 550 142
Počet unikátních útočících IP adres	115 730
Počet zachycených unikátních vzorků	35 107

4. PROKI

V roce 2015 zahájil Národní bezpečnostní tým CSIRT.CZ realizaci projektu PROKI,, podpořeného v rámci Programu bezpečnostního výzkumu České republiky 2015–2020 (VI20152020026). 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.

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 vlastním kódem 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 úspěšný upgrade na verzi 3.

V roce 2024 došlo v týmu k personálním změnám, kvůli kterým byl vývoj okolo projektu částečně omezen. I přesto se podařilo do PROKI implementovat funkcionalitu, která tvoří jeden z pilířů naší nové služby Deny listy.

Kromě toho byl také realizován průzkum mezi adresáty výstupů projektu. Konkrétně do něj byli zahrnuti ti, kteří během předchozích tří měsíců obdrželi ze systému PROKI hlášení. Jednalo se o 893 kontaktů, z nichž dotazník vyplnilo 120 respondentů, tedy 13 % oslovených.

Reakce dostáváme nejen od subjektů, které se přímo bezpečností a IT zabývají, ale také od řady dalších subjektů. Cílem dotazníkového šetření bylo zjistit užitečnost výstupů pro zapojené subjekty. Shrnutí výstupů je následující:

- pravidelně využívá výstupy více než 75 % respondentů;
- za užitečné považuje výstupy přes 62 % a dalších 32 % částečně;
- téměř 79 % respondentů vyhovuje četnost zasílání výstupů;
- více než polovina příjemců uvedla, že se ve výstupech nikdy nesetkala s false positives;
- o využití API uvažuje téměř 40 % respondentů.

Kromě kvantitativních údajů průzkum přinesl i řadu návrhů na vylepšení systému, kterými se plánujeme dále zabývat.

Stejně tak jako v předchozích letech jsme i v roce 2024 pokračovali v analýze výstupů z minipotů Turris pomocí separátní části PROKI, ve které evidujeme denně miliony útoků. Tyto útoky pocházejí nejčastěji z Rumunska a Bulharska. Nejčastější hesla, která útočníci používají při pokusech o průnik do systémů, jsou 123456, admin, password a root.

Pomocí minipotů byly mezi jinými detekovány velmi rozsáhlé systémy, které útočí ze stovek zdrojových IP adres a používají velmi objemné slovníky o velikosti desítek tisíc kombinací jména a hesla. Útok je přitom velmi pomalý. Odzkoušení celého slovníku trvá několik týdnů a zdrojové IP adresy se neustále obměňují.

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 2024	Počet
Počet e-mailů odeslaných z PROKI	44 599
Počet unikátních příjemců (abuse kontaktů) PROKI hlášení	911
Počet unikátních českých IP adres, které jsme nějakým způsobem zaznamenali	154 043

5. Penetrační a zátěžové testování

I v roce 2024 bylo úspěšně provedeno penetrační testování. Prováděli jsme testy komerčních subjektů i veřejné správy. Penetrační testování podstoupily i dva významné projekty sdružení CZ.NIC.

6. Osvěta a vzdělání

V oblasti osvěty a vzdělávání byl rok 2024 pestrý nejen co do aktivit týmu CSIRT.CZ, ale také proto, že došlo k ukončení pronájmu prostor, které dosud sloužily právě i pro vzdělávací akce. Kolegům z Akademie CZ.NIC proto na tomto místě patří poděkování, jelikož nové prostory zvládli sehnat tak, že to neomezilo poskytování našich služeb.

I nadále se CSIRT.CZ věnoval již zavedenému 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. Školení je pravidelně aktualizováno, aby uživatelé vždy získali přehled o aktuálně používaných praktikách útočníků.

Kromě uvedeného školení jsme realizovali školení pro zaměstnance Ministerstva průmyslu a obchodu, zaměstnance VŠE či Akademie věd.

Zkušenosti z vlastního vývoje, automatizace a úprav jsme již v roce 2023 přetavili do kurzu programovacího jazyka Python v Akademii CZ.NIC. Tento kurz trvá šest týdnů a koná se jednou týdně.

Ve spolupráci s Evropskou agenturou pro kybernetickou a informační bezpečnost (ENISA), jsme organizovali dvoudenní kurz pro bezpečnostní pracovníky a architekty bezpečnosti, kteří chtějí přejít na model Zero Trust Architecture.

CSIRT.CZ se také již tradičně věnoval prezentaci vlastních zkušeností na nejrůznějších fórech a konferencích. Z vystoupení pro odbornou veřejnost lze jmenovat například prezentace nově vznikajícího projektu na konferenci C2S2, náš přístup ke komplexnímu zabezpečení webu a domény jsme prezentovali na konferenci CyberCon nebo na akci Internet a Technologie, která byla i v letošním roce součástí LinuxDays 2024. Co se týká mezinárodních konferencí, na evropské úrovni jsme prezentovali hned několikrát v rámci pracovních skupin TF-CSIRT. Na této akci kolega z týmu Turris navíc nabídl své know-how pro odborný workshop o tom, jak využít router jako bezpečnostní sondu. Na mezinárodní konferenci FIRST se nám podařilo dostat mezi přednášející v rámci doprovodné akce pro národní bezpečnostní CSIRT týmy NatCSIRT s příspěvkem o tom, jak jsme řešili DGA botnety.

Několikrát jsme vystupovali v tradičních médiích, a to jak ve veřejnoprávních, tak v soukromoprávních, především před Vánoci byl kolega Edvard Rejthar přizván, aby se vyjádřil k problematice podvodů na internetu.

Na blogu zaměstnanců CZ.NIC publikoval tým celkem 10 blogpostů, které slouží k osvětě a vzdělávání, nabízejí možnost porozumět kontextu činnosti CSIRT.CZ a vysvětlují synergie týmu v rámci sdružení CZ.NIC, Česka i v oblasti mezinárodní spolupráce.

Reprezentativním příkladem může být blogpost, ve kterém jsme informovali o přístupu správců webů k informacím o kompromitovaných webech, který je často velmi laxní, a to i přesto, že o kompromitaci existují jasné důkazy.

Po snahách kontaktovat správce webových stránek, kteří nemají o informace od nás zájem i přes zjevnou nebezpečnost těchto stránek, je pro nás spolupráce se subjekty, které si naopak informací od nás cení, zadostiučiněním. Příkladem takové spolupráce je naše zapojení v rámci soutěže Zlatý Erb. V tomto blogpostu se dočtete o našem zapojení i přínosu nejen pro soutěž, ale i pro zúčastněné subjekty.

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.

Další novinkou, na které spolupracoval náš tým s Akademií CZ.NIC, bylo školení týkající se povinností plynoucích z nového zákona o kybernetické bezpečnosti, které bylo realizováno pro členy Sdružení. Toto školení nyní nabízíme i pro další zájemce.

7. Aktuálně z bezpečnosti

Na již zmíněném seriálu Postřehy z bezpečnosti kromě nás spolupracují autoři ze sdružení CESNET, ALEF-CSIRT, ČD Telematika, Nettles Consulting a nově se do týmu připojila Monika Kutějová, zakladatelka neziskové organizace TheCyberValkyrez a spoluzakladatelka portálu CYBULE.

Publikované informace poukazují na nejzajímavější události, aktuality, ale i zranitelnosti, kterým by měla být věnována pozornost. Stejně jako v předchozích letech se díky naprosto bezproblémové spolupráci týmu autorů publikovalo přesně padesát dva 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 oblasti národní i mezinárodní spolupráce jsme i nadále rozvíjeli spolupráci se zástupci bezpečnostních týmů v rámci naší konstituency i mimo ni, úzce jsme spolupracovali s PČR a Národním úřadem pro kybernetickou a informační bezpečnost a mezinárodními organizacemi TF-CSIRT, FIRST, CSIRTs Network a Evropskou agenturou pro kybernetickou bezpečnost (ENISA). Kromě obvyklé zákonem stanovené činnosti se tým aktivně podílel například na připomínkování Národní strategie kybernetické bezpečnosti. V oblasti národní i mezinárodní spolupráce byla i nadále rozvíjena spolupráce se zástupci bezpečnostních týmů v rámci konstituency CSIRT.CZ.

V rámci preventivní činnosti a zvyšování povědomí o problematice kybernetické bezpečnosti jsme zajišťovali školení, přednášky a workshopy. Ty se týkaly, jak jsme zmiňovali v kapitole číslo 6 (Osvěta a vzdělávání), například soukromí a bezpečnosti na internetu, povinností vyplývajících z nově chystaného zákona o kybernetické bezpečnosti, využití routeru Turris v kybernetické bezpečnosti, možností komplexního zabezpečení domény či prezentace projektů týmu CSIRT.CZ.

V rámci CSIRT.CZ a pracovní skupiny FÉNIX jsme uspořádali setkání s více než 90 účastníky, kde vystoupili odborníci z akademické, soukromé i veřejné sféry. Kromě toho jsme se zapojili do pilotního testování aplikace Inject pro realizaci table-top cvičení. Významným prvkem

spolupráce bylo také předávání informací ze setkávání v rámci skupiny CSIRT Network vládnímu bezpečnostnímu týmu, který spadá pod NÚKIB.

V oblasti mezinárodní spolupráce bylo klíčové obhájit status certifikovaného týmu v rámci organizace Trusted Introducer. K získání tohoto stupně důvěry je nutné projít komplexním auditem, který se týká organizačního, technického a procesního zajištění a zajištění získávání a rozvoje lidských zdrojů. Tento audit vychází z modelu vyspělosti řízení bezpečnostních incidentů (SIM3).

Již po dvanácté jsme byli koordinátorem Česka pro největší cvičení svého druhu v Evropě: Cyber Europe 2024, do kterého v letošním roce byly zapojeny všechny státy EU kromě Francie a dále také Velká Británie, Norsko a Švýcarsko. Naše činnost spočívá v definování cílové skupiny pro Česko, oslovení určených subjektů a následnou koordinaci a proškolení zástupců přihlášených organizací. V letošním roce se do cvičení zapojilo 16 organizací ze státní, akademické i soukromé sféry, včetně klíčových subjektů energetického průmyslu, datacenter a státní správy. Přímých cvičících bylo 110. Podařilo se nám také zajistit místo pro zástupce NÚKIBu v roli pozorovatelů přímo v hlavním sídle Evropské agentury pro kybernetickou bezpečnost (ENISA) v Aténách, odkud jsme cvičení pro Česko v průběhu jeho dvoudenního konání koordinovali.

Dalšími důležitými činnostmi na poli národní, ale především 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, která byla vytvořena na základě této evropské směrnice a sdružuje národní a vládní CSIRT týmy členských států EU. Spolupráce těchto dvou českých týmů je založena zejména na společném řešení incidentů, sdílení nezbytných informací a odborných konzultacích. V rámci CSIRTs Network pravidelně spolupracují s dalšími evropskými národními a vládními týmy a několikrát ročně se setkávají při různých příležitostech, což umožňuje efektivní výměnu informací a koordinaci činností. Pracovní skupina CSIRTs Network v roce 2024 uspořádala několik jednání a přibližně dvacet online setkání, kterých se kromě zástupců členských států EU účastnili také zástupci organizací, aby řešili dopady incidentů s mezinárodním přesahem. Hlavním cílem těchto setkání bylo sdílení aktuálních informací mezi členskými státy a efektivní spolupráce na eliminaci dopadů kybernetických incidentů a událostí.

V Akademii CZ.NIC jsme společně s Evropskou agenturou pro kybernetickou bezpečnost spoluorganizovali událost Learning, Exercise and Training. Té se zúčastnili zástupci bezpečnostních týmů z několika zemí EU.

Pokračovali jsme s výkonem činností spojených s naší rolí v řídícím výboru organizace TF-CSIRT. Tato komunita sdružuje profesionály z řad kybernetické bezpečnosti napříč sektory. Česká republika má i díky podpoře FÉNIXu v současné době 71 členských týmů, z toho 4 certifikované, 20 akreditovaných, 41 zalistovaných. 2 zcela nové týmy čekají na udělení

certifikace, 2 týmy na akreditaci a další 2 týmy jsou v procesu recertifikace. Oproti roku 2023 se jedná opět o zvýšení počtu členských týmů. V rámci mezinárodního sdružení incident response týmů FIRST má Česká republika stále totožný počet zapojených týmů jako v předchozím roce. V rámci TF-CSIRT setkání byla v průběhu roku 2024 prezentována komunitě kromě průběhu cvičení Cyber Europe také přednáška na téma řešení phishingu v doméně .CZ.

Nově jsme si také vyzkoušeli, jaké to je moderovat panelovou diskusi. V rámci té byl oznámen společný americký a evropský přístup k harmonizaci Incident reportingu v rámci kritické infrastruktury a zároveň představena dohoda o spolupráci USA a EU v této oblasti. Práci našeho týmu v oblasti kybernetické bezpečnosti jsme prezentovali také v rámci mezinárodní návštěvy delegace z demokratické republiky Kongo.

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

Závěrem můžeme konstatovat, že i přes změny, které uplynulý rok přinesl, jsme dokázali nadále plnit naše cíle a poskytovat kvalitní služby. V průběhu roku jsme se přestěhovali, uspořádali několik odborných kurzů a školení. Přešli jsme na nový ticketovací nástroj se svobodnou licencí, úspěšně jsme zorganizovali Cyber Europe, které poskytlo platformu pro otestování schopností a připravenosti týmů spadajících do kritické infrastruktury. Pomohli jsme účastníkům vyzkoušet si, zda by dokázali efektivně zvládat, řešit a komunikovat rozsáhlé kybernetické incidenty s mezinárodním dopadem. Náš tým se také aktivně podílel na konferencích, soutěži Zlatý Erb a dalších odborných akcích, kde jsme sdíleli naše znalosti a zkušenosti nejen s bezpečnostní komunitou. Úspěšně jsme prošli několika audity, připravovali jsme se na přijetí nového zákona o kybernetické bezpečnosti a pokračovali jsme taképři tom všem ve vývoji nových nástrojů a utilit, které nám pomohly zefektivnit naši činnost a posílit naši schopnost efektivně reagovat na bezpečnostní incidenty. Naším cílem je i nadále inovovat a poskytovat řešení, která budou odpovídat aktuálním potřebám nejen našich konstituentů, ale všech uživatelů internetu, a přispívat tak ke zlepšení jejich bezpečí nejen v Česku.