ZPRÁVA O ČINNOSTI CSIRT.CZ (NÁRODNÍHO CSIRT ČR) ZA ROK 2022

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 rozhodnutím Ministerstva vnitra České republiky (dále jen MV ČR) a uzavřením Memoranda o provozu Národního CSIRT.CZ 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 ke zrušení Memoranda o provozování CSIRT.CZ, uzavřené sdružením CZ.NIC a MV ČR 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.

Rok 2022 v kostce

Doznívající pandemická situace ukázala, že se i v roce 2022 podařilo týmu obstát v mnoha výzvách, které s sebou změny uplynulých let přinesly. Kromě úspěšného zapojení CSIRT.CZ do evropského předsednictví v rámci úzké spolupráce CSIRT Network a dalších úspěchů na poli mezinárodní spolupráce se nám podařilo zefektivnit interní procesy a spolupráci s externími subjekty navázat na úroveň, která byla dosahována před pandemií.

I v letošním roce jsme úspěšně řešili a koordinovali nahlášené bezpečnostní incidenty ve stanoveném reaktivním čase. Pokračovali jsme ve vylepšení nástrojů a utilit, které týmu umožňují adekvátně reagovat na stále větší počet hlášených incidentů. Nástroj pro predikci a ochranu před kybernetickými incidenty PROKI (*Predikce a Ochrana před Kybernetickými Incidenty* dále jen PROKI) a ticketovací systém OTRS jsou neustále vylepšovány a v letošním roce se podařilo významně zefektivnit fungování obou těchto nástrojů. Zabývali jsme se také návrhem řešení a samotným řešením vlny phishingových útoků. V rámci prevence bezpečnostních hrozeb a rizik jsme průběžně prováděli penetrační testování.

Pokračovali jsme v úzké spolupráci s Národním úřadem pro kybernetickou a informační bezpečnost v několika rozličných oblastech. Díky předsednictví ČR v EU došlo k dalšímu prohloubení spolupráce na národní i mezinárodní úrovni, a to především díky Agentuře Evropské unie pro kybernetickou bezpečnost (ENISA) v rámci CSIRT Network. Spolupráce bezpečnostních týmů probíhala na několika dalších úrovních formou setkávání členů komunity například v rámci pracovní skupiny CSIRT.CZ, při realizaci a účasti na školeních nebo

v rámci největšího evropského cvičení Cyber Europe, jehož realizace se právě kvůli zmíněné pandemii posunula o celé dva roky. Pokračovali jsme také v podpoře bezpečnostních týmů v rámci zapojení do mezinárodních komunit jako je TF-CSIRT, FIRST nebo Fénix.

Členové týmu participovali na projektech, jako je například SIC CZ nebo Skener webu, a úspěšně tak pokračovala činnost, které se tým CSIRT.CZ již léta věnuje na poli prevence a výzkumu. Zároveň jsme se věnovali další práci s výsledky projektů, které proběhly v předchozích letech, jako jsou PROKI či HaaS.

Osvětovou činnost tým realizuje také prostřednictvím pravidelného publikování článků na serveru root.cz s názvem Postřehy z bezpečnosti ve spolupráci se sdružením CESNET, ke kterému se nově přidal ALEF-CSIRT, ČD Telematika a Nettles Consulting. Kromě výše uvedeného se tým zaměřuje na osvětu publikováním krátkých aktuálních zpráv na svých webových stránkách s názvem Aktuálně z bezpečnosti.

Více podrobných informací k jednotlivým službám zmíněným v této kapitole, jež jsou poskytovány týmemCSIRT.CZ, je možné nalézt vždy pod patřičnými názvy následujících kapitol v této výroční zprávě.

1. Incident handling

Z pohledu metodologie řešení incidentů zahrnuje fázi – 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. Statistiky incidentů v roce 2022

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.

V roce 2022 bylo řešeno dohromady 2 067 incidentů, jejich počet tak vzrostl téměř o 20 %. Tým opět dosáhl dosud nejvyššího registrovaného množství řešených incidentů v evidenci vlastních statistik, které vede od roku 2008. Od doby před pandemií se jedná o více než 100% nárůst. Stále vzrůstající počet hlášení nás vede k práci na lepší automatizaci reakcí na incidenty.

STATISTIKA PROCESU ŘEŠENÍ BEZPEČNOSTNÍCH INCIDENTŮ TÝMEM CSIRT.CZ

	2019	2020	2021	2022
Sensor Network*	14 911	16 217	10 284	8 815
Phishing	483	738	1 281	1 485
Spam	128	216	165	220
Malware	85	109	141	224
Other	85	86	54	63
Probe	141	68	66	69
Trojan	0	0	0	0
DOS	16	16	11	0
Botnet	4	2	1	4
Virus	0	0	0	0
Portscan	3	29	7	2
Pharming	9	3	0	0
Celkem	**954**	**1 267**	**1 726**	**2 067**

* Sensor Network není započten do celkového počtu

Jak je patrné z výše uvedené tabulky, v drtivé většině všech incidentů řešíme phishing, spam a malware.

Podařilo se nám nalézt efektivní řešení, které nám pomáhá identifikovat phishingový obsah a okamžitě zabránit jeho šíření. Více informací o tomto postupu popisujeme v kapitole Boj s phishingem v doméně .cz.

Každoroční nárůst počtu incidentů může být způsoben mnoha aspekty a není účelem tohoto dokumentu je určit. Je však zřejmé, že vliv má i stále větší míra digitalizace společnosti, automatizace procesů a čím dál širší využívání informačních systémů v mnoha oblastech.

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). 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 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.

Mezi nejčastěji registrované podvodné aktivity řešené v roce 2022 ve spolupráci s PČR patří:

- phishingové kampaně,
- falešné e-shopy,
- podvodné weby nabízející investice do virtuálních měn,
- podvodné jednání na inzertních portálech,
- falešné webové stránky.

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

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 dále napomáhají k rychlejšímu sdílení informací mezi jednotlivými relevantními subjekty.

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 umožňující automatizovat komunikaci, které se účastní několik stran, práci s kvótami LACNICu a schopnost převodu napříč 50 datovými typy konkrétních hodnot. Dále došlo k zjednodušení instalace, vytvoření doplňku pro prohlížeče pro zrychlení práce s interními aplikacemi – zejména s OTRS, přidání možnosti rekognice a automatického určení jazykové šablony pro odpověď na základě domény příjemce, zobrazení náhledu problematické stránky nebo automatické dopočítávání metadat potřebných pro řešení konkrétních incidentů.

Dalším úspěšným projektem je knihovna Envelope. Vydali jsme verzi 2.0.0 – bezpečnostní update, ten nabízí intuitivnější rozhraní pro SMTP server a podporu vícejazyčných systémů. Dále přibylo dokonce lepší parsování e-mailových adres, než má standardní knihovna Pythonu, a experimentální práce s přílohou typu XARF (která se v bezpečnostní komunitě rozmáhá pro předávání informací).

V tomto roce se nám podařilo obohatit ticketovací systém OTRS o mnoho užitečných automatických operací. Hlavní motivací k tomu je zmíněný nárůst počtu hlášených incidentů a efektivita při nakládání s nimi. Kromě automatického vytvoření hlavičky k příchozím e-mailům a provedení dalších užitečných operací jsme v letošním roce přidali možnost automaticky změnit šifrování pro potřeby předávání incidentů PČR. Dalším vylepšením tohoto systému je možnost automaticky sdružovat e-maily do jednoho ticketu. Možnost automatického přidání partnerského CSIRTu do kopie zahraničních ticketů je novinkou, kterou jsme dříve využívali pouze s hromadnými e-maily posílanými přes Convey. Automatické screenshoty reportovaných URL nám nyní umožňují bez dalšího zdržení rovnou poznat, zda je stránka již například zablokována. Přidání automatického podpisu dle fronty je také s ohledem na různorodost řešených hlášení vítaným krokem. Dále jsme zapracovali na lepším oddělení front, čímž jsme snížili možnost lidské chyby. Částečně jsme zautomatizovali i proces, kterým blokujeme v registru škodlivé domény na základě čl. 17 (více informací k článku uvádíme níže).

1.3. Boj s phishingem v doméně .cz

V posledních třech letech došlo k velkému nárůstu phishingových stránek, které byly nahlášeny národnímu bezpečnostnímu týmu CSIRT.CZ. Zatímco v roce 2018 jsme řešili 518 phishingových stránek, v roce 2019 to bylo „jen" 483, o rok později se jednalo už o 738 stránek, v roce 2021 jsme překročili tisícovku (1 277) a v roce 2022 jsme na čísle 1 485. Naše statistiky přitom odrážejí pouze malou část celkového počtu útoků, protože národní CSIRT funguje jako tzv. „last resort" team, tedy krajní řešení a je nám tak hlášena pouze malá část útoků.

S celkovým nárůstem phishingových útoků došlo také k nárůstu počtu útoků prováděných s využitím .CZ domén, které směřovaly na české uživatele. Tato skutečnost nás donutila častěji využít možnost zrušení delegace doménového jména, kterou nám umožňuje článek 17.1. Pravidel registrace jmen domén v ccTLD .cz. Důležitost této změny lze uvést na reálném případě, kdy doménu s phishingovým obsahem navštívilo před jejím vyřazením 1 489 uživatelů, po jejím vyřazení jsme zaznamenali ještě 7 217 uživatelů, kteří se pokoušeli na doménu dostat, Díky jejímu včasnému vyřazení se tak téměř 80 % potenciálních obětí na falešné stránky již nedostalo.

V roce 2022 jsme na základě interní metodiky provedli zrušení delegace v celkem 110 případech. V osmi případech se jednalo o phishingové stránky přímo napodobující internetové bankovnictví, ve 21 případech jsme vyřadili domény napodobující vzhled stránek České pošty, které uživatele lákaly na údajnou daňovou vratku, a v 81 případech se jednalo o stránky nabízející údajný příspěvek na bydlení.

V případě .CZ domény často řešíme domény, které nám někdo nahlásí, v tomto případě, jsme si však prověřili, jak přínosná může být schopnost přizpůsobit i zaběhnuté procesy v reakci na dynamicky se vyvíjející prostředí. Díky této změně dokážeme domény, které jsou po jejich registraci identifikovány jako potenciálně škodlivé, zařadit do sledování. Tento monitoring nás upozorní, pokud se na webu nebezpečný obsah ukáže. Základní informace o útoku pak doplňují data, která získáváme z projektu ADAM.

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 2022 došlo k testování 18 domén na základě 16 podaných objednávek a v rámci projektu SIC CZ bylo otestováno 5 subjektů.

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 2022 zaznamenali 802 unikátních vzorků malware. Na Windows honeypotech dionaea jsme pak zaregistrovali 132 vzorků. V případě cowrie honeypotů se jedná v porovnání s předešlým rokem o 47% pokles v množství zaregistrovaných vzorků. Oproti tomu u dionaea honeypotů došlo k navýšení o necelých 5 %.

HAAS STATISTIKY

Počet registrovaných uživatelů	4 501
Počet spojení/útoků	33 768 024
Počet provedených příkazů	13 458 397
Počet unikátních útočících IP adres	196 610
Počet zachyceným unikátních vzorků	7 024

4. PROKI

V roce 2015 zahájil Národní bezpečnostní tým CSIRT.CZ realizaci projektu PROKI; VI20152020026, podpořeného v rámci 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 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 pokračoval i po roce 2020. 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 nám podařilo zvětšit diskové kapacity, proběhl upgrade IntelMQ na verzi 2 a v současné chvíli probíhá upgrade na verzi 3.

Nově je také zasílána analýza výstupů z minipotů Turris do separátní části PROKI, kde jsou evidovány desítky milionů událostí za den. Nejčastější útoky evidujeme z Ukrajiny, Bulharska a Rumunska. Nejčastější hesla jsou 123456, 1234567890, 123456789, admin, <prázdné>, password, root, admin123, system a sh.

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 2022	Počet
Počet odeslaných emailů z PROKI	32 449
Počet unikátních příjemců (abuse kontaktů) PROKI hlášení	733
Počet unikátních českých IP adres, které jsme nějakým způsobem zaznamenali	51 177

5. Osvěta a vzdělání

Zřejmě největšími událostmi v oblasti osvěty a vzdělávání bylo zapojení týmu do mezinárodních cvičení Locked Shields a Cyber Europe. Úkolem obou těchto cvičení je rozvíjet schopnosti spolupráce v oblasti kybernetické bezpečnosti. Cvičení Cyber Europe jsme se zúčastnili ve dvou úrovních, jako hráči i jako organizátoři pro českou komunitu, kterou reprezentovalo devět týmů z Česka a zcela výjimečně i jeden tým ze Slovenska.

Na cvičení Cyber Europe, které bylo v letošním roce zaměřené na zdravotnický sektor, volně navázalo cvičení Health Czech, organizované Národním úřadem pro kybernetickou a informační bezpečnost. Členové našeho týmu seznámili účastníky s možnostmi identifikace podezřelé e-mailové komunikace a z pozice odborné komise sledovali, jak si krizové týmy poradily s jednotlivými „injecty".

V oblasti školení a vzdělávání bylo 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 prevence a seznámení uživatelů s aktivními a pasivními digitálními stopami, zásadami bezpečného chování a soukromím a anonymitou na Internetu.

V souvislosti s osvětou a vzděláváním jsou také spojeny přednášky a školení veřejnoprávních, neziskových i komerčních subjektů v rámci projektu SIC CZ. Znalosti, zkušenosti a aktivity jsou publikovány na blogu sdružení CZ.NIC. Seriál Myš je pro kočku byl publikován po celý rok, a ačkoliv se netýká bezpečnosti přímo, dokáže čtenářům pomoci dosáhnout větší efektivity nejen v linuxovém prostředí.

CSIRT.CZ se také již tradičně věnoval prezentaci vlastních zkušeností na nejrůznějších fórech a konferencích. Z vystoupení pro odbornou veřejnost lze jmenovat například konferenci Cyber Attacks nebo odborný seminář Výzkum v oblasti kyberkriminality a kyberbezpečnosti pořádaný Institutem pro kriminologii a sociální prevenci. Z akcí pro širokou veřejnost se pak jednalo o prezentaci práce CSIRT.CZ na akci Den Evropy, Festivalu bezpečného internetu či v pořadech Nový den na CNN Prima News a Dobré ráno v České televizi.

6. Aktuálně z bezpečnosti

Mezi 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, aktuality, stejně jako i zranitelnosti, kterým by měla být věnována pozornost. V roce 2022 tým publikoval celkem 12 příspěvků. Oproti předchozím rokům se zdánlivě jedná o pokles, ve skutečnosti však došlo k propojení spolupráce odborníků z významných organizací zabývajících se kybernetickou bezpečností, konkrétně se jedná o spolupráci s týmy ALEF-CSIRT, ČD Telematika, Nettles

Consulting a již tradiční spolupráci se sdružením CESNET. V rámci tohoto seriálu bylo publikováno celkem 55 článků.

Kromě seriálu *Postřehy z bezpečnosti* je možné sledovat na webových stránkách týmu CSIRT.CZ sekci *Aktuálně z bezpečnosti* (dále jen AZB), která je určená 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. V roce 2022 bylo v rámci této sekce publikovaných 33 aktualit.

7. Národní a mezinárodní spolupráce

V roce 2022 se tým CSIRT.CZ díky své úzké spolupráci v rámci CSIRT Networku stal součástí evropského předsednictví a jako „chair trio handover" převzal, kromě jiného, odpovědnost nad zajištěním kontinuity činností s Agenturou Evropské unie pro kybernetickou bezpečnost (ENISA), organizací CNW Meetingů a přípravou reportu pro Cooperation Group. V rámci předsednictví ČR v EU probíhala od 1. června úzká spolupráce s GovCERT.cz, s francouzským vládním týmem (ANSSI), švédským vládním a národním týmem (CERT-SE) a aktuálním předsedou tria (SI-CERT).

Další důležité činnosti na poli mezinárodní kybernetické bezpečnosti jsou obligatorní aktivity vyplývající ze směrnice NIS a zákona o kybernetické bezpečnosti. Jedná se o aktivní zapojení do CSIRTs Networku, prohloubení spolupráce s ENISA či účast v pracovní skupině WG Training a WG Cyber Weather, kterému členka našeho týmu v průběhu roku předsedala.

I nadále podporujeme bezpečnostní týmy a zapojení do mezinárodní komunity Trusted Introducer (dále jen TI, 59 zapojených týmů) a FIRST (7 zapojených týmů). Zájem o členství v TI je podpořen také projektem FÉNIX. V rámci mezinárodní komunity FIRST jsme provedli tři návštěvy, jichž účelem byla kontrola splnění požadavků pro vstup nových týmů do organizace. Všechny tři týmy dané podmínky naplnily.

V souvislosti s vývojem událostí na Ukrajině se CSIRT.CZ zapojil do diskuse o možných „partnerech" a o vytvoření kanálů do budoucna pro spolupráci s Velkou Británií, USA a Kanadou. Výsledkem této diskuse je sestavení reportu a výzva CNW ke spuštění specifické platformy pro podporu řešení incidentů za účelem zvýšené pozornosti k dění na Ukrajině a škodlivým aktivitám proti Ukrajině a jejím spojencům.

Specifickým druhem spolupráce je pravidelná a úzká součinnost mezi národním bezpečnostním týmem CSIRT.CZ a vládním týmem 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 založená 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 informování o práci a činnosti jednotlivých týmů, pravidelná konzultace a případná koordinace spolupráce. Ta v letošním roce vyústila v celorepublikové cvičení pro zástupce zdravotnických zařízení Health Czech, díky kterému se účastníci dozvěděli důležité informace, postupy a novinky v oblasti kybernetické bezpečnosti. Národní a vládní tým se pravidelně spolu účastní nejrůznějších mezinárodních kybernetických cvičení. Tým CSIRT.CZ aktivně pracuje na organizaci a plánování mezinárodního kybernetického cvičení Cyber Europe.

Proběhla také pracovní skupina CSIRT.CZ, které se zúčastnilo 70 členů bezpečnostní komunity, kteří si vyslechli řadu zajímavých přednášek.

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

Závěr

Tým CSIRT.CZ čelil v roce 2022 mnoha výzvám. Problémy doznívající pandemie se ukázaly jako velice dobře zvládnuté a tým čekaly další výzvy. Začátek konfliktu na Ukrajině, přípravy volebních kampaní, stále se zvyšující počet incidentů a předsednictví v rámci TRIO CNW jsou hlavním výčtem významných událostí roku 2022, které mnohdy udávaly směr, kterým se ubírala pozornost a zdroje národního CSIRT týmu.

Soustředili jsme se především na další rozvoj již existujících nástrojů a služeb a hledali jsme nové možnosti, jak zefektivnit práci pro řešení stále vzrůstajícího počtu hlášených incidentů. Těší nás, že se nám díky projektům PROKI a OTRS podařilo některé procesy významně optimalizovat.

Jedna z největších výzev roku 2022 v podobě naplnění úlohy v rámci předsednictví EU vyústila ve stanovení strategických, provozních a taktických cílů, které jsou postupně naplňovány. Účastnili jsme se také cvičení Health Czech, které bylo věnováno osvětě pracovníků ve zdravotnictví.

Těší nás také navázání nové spolupráce s odborníky v komunitě v rámci publikace osvětových článků, poskytování podpory ostatním týmům, úspěch obou našich knihoven na GitHubu, díky kterým se nám daří rychleji sdílet informace mezi jednotlivými relevantními subjekty, i další výše popsané projekty a výstupy naší činnosti.