ZPRÁVA O ČINNOSTI CSIRT.CZ (NÁRODNÍHO CSIRT ČR) ZA ROK 2021

CSIRT.CZ

Obsah

O CSIRT.CZ

Tým CSIRT.CZ plní od 1. ledna 2011 roli Národního CSIRT České republiky. Stalo se tak rozhodnutím Ministerstva vnitra ČR a uzavřením Memoranda o provozu Národního CSIRT ČR, které MV ČR a sdružení CZ.NIC podepsalo v prosinci 2010.

Dne 19. října 2011 přijala vláda České republiky usnesení č. 781 o ustavení Národního bezpečnostního úřadu (dále jen NBÚ) gestorem problematiky kybernetické bezpečnosti a zároveň národní autoritou pro tuto oblast. Na jaře 2012 proto došlo k revokaci Memoranda o provozování Národního CSIRT ČR, které uzavřelo sdružení CZ.NIC a MV ČR v prosinci 2010, a bylo podepsáno nové Memorandum mezi sdružením CZ.NIC a Národním bezpečnostním úřadem. Toto Memorandum mělo platnost do konce roku 2012. Dne 19. prosince 2012 bylo – s platností od 1. ledna 2013 – uzavřeno Memorandum mezi sdružením CZ.NIC a Národním bezpečnostním úřadem o provozování Národního CSIRT ČR. Toto Memorandum bylo platné do konce roku 2015 a v souladu se Zákonem o kybernetické bezpečnosti bylo nahrazeno veřejnoprávní smlouvou, uzavřenou dne 18. prosince 2015 s Národním bezpečnostním úřadem. Od 1. srpna 2017 je pak na základě zákona číslo 205/2017 Sb., ústředním správním orgánem pro kybernetickou bezpečnost Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB). Uzavřená veřejnoprávní smlouva automaticky přešla pod tento nový správní orgán.

Rok 2021 v kostce

Rok 2021 navázal na předchozí v otázce nutnosti rychlého přizpůsobování se na změny vyvolané pandemickou situací. Nejistý dlouhodobý vývoj související s epidemií přinesl řadu komplikací pro každého, v různých rovinách a odrazil se vcelku rozmanitými způsoby.

Podíváme-li se na to však z jiného hlediska, situace přinesla týmu novou výzvu, jak zefektivnit spolupráci nejen interně, ale také směrem k externím subjektům.

Tým CSIRT.CZ zvládl promptně reagovat na aktuálně platná nařízení a zároveň na obligatorní záležitosti, tak, aby nedošlo k poklesu reaktivního času ani k jinému negativnímu ovlivnění při řešení a koordinaci nahlášených bezpečnostních incidentů a kvalita a úroveň incident handlingu zůstala zachována na úrovni před pandemií. Mimo toto stanovené východisko tým usiloval o další vývoj a řádné plnění běžně poskytovaných služeb a aktivit. V konkrétní rovině je možné uvést například setkání členů české a slovenské bezpečnostní komunity na Pracovní skupině CSIRT.CZ či realizování nejrůznějších školení – směrem k bezpečnostní komunitě, ale také i směrem k veřejnosti, čímž aktivně a úspěšně tým pokračoval v činnosti, které se již léta věnuje na poli prevence a výzkumu. Osvětovou činnost tým realizuje také prostřednictvím pravidelného publikování článků na serveru root.cz s názvem Postřehy z bezpečnosti ve spolupráci se sdružením CESNET. Krom výše uvedeného se tým se zaměřuje na osvětu také publikováním krátkých aktuálních zpráv na svých webových stránkách s názvem Aktuálně z bezpečnosti.

Za výrazný úspěch považujeme také progresi a novinky ve vývoji nástrojů a utilit, které umožňují týmu adekvátně reagovat na stále narůstající počet hlášených incidentů a efektivně tyto incidenty řešit. Jak ukazuje statistika řešených incidentů, dochází každoročně k markantnímu nárůstu hlášených incidentů – nejen z důvodů vycházejících přímo či nepřímo ze situace související s pandemií, ale například také kvůli rozšiřování tzv. threat surface attack, a je proto potřeba počítat s tím, že množství incidentů bude růst i nadále do budoucna. Proto je velmi podstatné zaměření se na vývoj nástrojů, doplňků a utilit ovlivňujících samotný proces incident handlingu.

V uplynulém roce se týmu podařilo také rozšířit spolupráci s dalšími subjekty a projekty – jako příklad lze uvést spolupráci s projektem Turris Sentinel za účelem vytvoření distribuované sítě bezpečnostních sond. Více viz kapitola PROKI.

V rámci spolupráce s projektem ADAM byla také s předstihem odhalena a sinkholována .CZ doména, vytvořená DGA algoritmem botnetu Qsnatch. To umožnilo identifikovat přes 4 000 unikátních IP adres zapojených do tohoto botnetu. Správci identifikovaných IP adres byli následně o problému informováni.

Mimo to však tým pokračoval tradičně ve spolupráci se subjekty, se kterými se běžně aktivně podílí na řešení incidentů a se kterými spolupracuje dlouhodobě – jako je například NÚKIB (zejména vládním týmem GovCERT), PČR, sdružení CESNET, ALEF NULA a mnohými dalšími.

Více podrobných informací k jednotlivým službám zmíněným v této kapitole, jež jsou poskytovány Národním bezpečnostním týmem ČR CSIRT.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 některou z těchto fází zcela vynechat. Každý incident tak projde tímto určitým cyklem. Na základě reportovaných incidentů tým vede systematicky statistiku řešených incidentů.

1.1. Statistiky incidentů v roce 2021

Služba incident handling a incident response (řešení a koordinace řešení bezpečnostních incidentů) je základní službou, kterou týmy CERT/CSIRT plní a musí plnit v rámci svého definovaného pole působnosti. V případě CSIRT.CZ se jedná o řešení a koordinaci řešení bezpečnostních incidentů, které mají původ nebo cíl v sítích provozovaných v České republice, nebo se obecně dotýkají jejího kyberprostoru. Týmu CSIRT.CZ jsou adresovány problémy (tzn. reportovány incidenty a události) několika typů:

1. Problémy, u kterých byly vyčerpány veškeré známé způsoby řešení, ale problém přesto přetrvává.

2. Problémy, u kterých není jednoduché identifikovat, kdo je původcem incidentu,nebo kdo by se jeho řešením měl zabývat.

3. Problémy, které mají závažný dopad na infrastrukturu v ČR. Tyto problémy mohou mít plošný charakter a negativně ovlivňovat další sítě, služby a uživatele, je tedy nutné, aby se informace tohoto typu co nejrychleji dostaly k těm, kdo mohou zasáhnout a nastavit například vhodné metody obrany apod.

4. Problémy plošného rozsahu, například počítače v botnetu, zařízení s konkrétní zranitelností, zjednodušeně řečeno informace od zahraničních partnerů týkající se více sítí v ČR.

V roce 2021 bylo řešeno dohromady 1 726 incidentů, tzn. meziroční nárůst dosáhl 36,2 %. V porovnání se statistikou incidentů před pandemií je to však nárůst až o 80 %. Tým opět dosáhl dosud nejvyššího registrovaného množství řešených incidentů v evidenci vlastních statistik. Tento nárůst reflektuje mimo jiné také celkový počet reakcí na incidenty. S jedním incidentem nezřídka souvisí až desítky e-mailů. Do výčtu důvodů patří komplexnost útoků, botnety, zranitelná zařízení, kompromitované účty. Tento nárůst reflektuje mimo jiné také celkový počet reakcí na incidenty. Reakcí na incidenty jsme zaregistrovali 17 423, což je o 3 540 více než tomu bylo v roce 2019. S jedním incidentem je nezřídka spojovaná řada emailů – až desítky emailů. Důvodem je komplexnost útoků, botnety, zranitelná zařízení, kompromitované účty.

STATISTIKA PROCESU ŘEŠENÍ BEZPEČNOSTNÍCH INCIDENTŮ TÝMEM CSIRT.CZ

	2018	2019	2020	2021
Sensor Network*	18 435	14 911	16 217	10 284
Phishing	518	483	738	1 281
Spam	144	128	216	165
Malware	135	85	109	141
Other	58	85	86	54
Probe	171	141	68	66
Trojan	0	0	0	0
DOS	7	16	16	11
Botnet	20	4	2	1
Virus	0	0	0	0
Portscan	16	3	29	7
Pharming	10	9	3	0
Celkem	**1 079**	**954**	**1 267**	**1 726**

* Sensor Network není započten do celkového počtu

Jak je patrné z výše uvedené tabulky, v roce 2021 došlo stejně jako v předchozím roce zejména k zásadnímu nárůstu phishingu. Mimo to došlo ke zvýšení počtu incidentů v kategorii malware. Ve všech zbylých kategoriích, tedy u spam, other, probe (kategorie zahrnující brute force útoky), DOS, botnet, pharming došlo naopak k poklesu incidentů. Nárůst incidentů ve výše popsaných kategoriích není náhodný, stejně jako samotný počet incidentů v kategorii phishing. Již loni při podrobném zkoumání počtu jednotlivých incidentů byla explicitně patrná souvislost s pandemií a krizí spojenou s Covid-19. Pandemie Covid-19 přirozeně přinesla a také uměle vytvořila řadu podnětů a aktuálně plošně sledovaných témat, které začali útočníci zneužívat ve velkém pro různé útoky.

Není účelem tohoto dokumentu taxativně jmenovat veškeré prvky ovlivňující nárůst incidentů. Je však nutno uvést, že s vývojem a potřebou neustále se adaptovat na proměnlivé okolnosti, se kterými se již několik let potýká společnost, dochází k rozšíření tzv. threat surface attack, tedy na co všechno je možné zaútočit.

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 zachycovaní informací o strojích, ze kterých byly zaznamenány pokusy o připojení. IDS pracuje na platformě LaBrea, která je distribuována pod licencí GPL. LaBrea využívá adresových bloků, které v Internetu dosud nebyly použity, což znamená, že na nich neexistovaly žádné uživatelské stroje. K takovým adresám nemá „zdravý" stroj důvod se připojit. Systém předstírá, že na těchto adresách běží funkční zdroje, a reaguje na pokusy o připojení přes TCP a ICMP echo (ping). Součástí řešení bezpečnostních incidentů je také spolupráce s dalšími bezpečnostními týmy nejen v rámci působnosti ČR, ale také distribuování důležitých informací o zranitelnostech, útocích a další. Podrobnější informace viz kapitola Aktuálně z bezpečnosti a Národní a mezinárodní spolupráce.

Mimo součinnost s dalšími bezpečnostními týmy spolupracuje Národní CERT při řešení reportovaných incidentů také s orgány státní správy, dále s Policií České republiky a dalšími subjekty.

Mezi nejčastěji registrované podvodné aktivity řešené v roce 2021 ve spolupráci s PČR patří:

- falešné a podvodné e-shopy
- podvodné weby nabízející investice do virtuálních měn
- falešné webové stránky.

Řešení bezpečnostních incidentů vyžaduje také spolupráci se specializovanými pracovišti PČR.

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 také 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 zaměřených na best practices. Na základě zkušeností a praktických doporučení vývojářů z jiných evropských CSIRT/CERT týmů je možné nejen zdokonalovat vyvíjení vlastních nástrojů a utilit, ale je možné využít při jejich dalším vývoji i poznatky ze zahraničí.

Před několika lety tým vyvinul vlastní open-source nástroj Convey umožňující automatizovanou komunikaci, ve které participuje několik stran. Následoval vývoj utility pro možnost práce s s kvótami LACNICu a schopnost převodu napříč 50 datovými typy konkrétních hodnot. Dále došlo k zjednodušení instalace, 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. Na tento vývoj uplynulých let navazuje vývoj utility pythonize (pz) pro Python v Bashi. Přestože současné linuxové distribuce mají k dispozici mnoho efektivních nástrojů pro zpracování vstupu, řada problémů je snadno řešitelná pomocí programovacího jazyka Python. Jedinou překážkou byla jeho integrace do příkazové řádky. Nicméně, díky této utilitě bez závislostí je možné napsat jednořádkový skript Pythonu přímo v příkazové řádce. Bližší technické informace k této utilitě je možné nalézt zde.

Dalším krokem v otázce vývoje používaných nástrojů se stalo vylepšování tiketovacího systému OTRS, který byl upgradován na novou verzi 6. Z hlediska praktického náhledu to znamená, že při příchodu každého e-mailu se automaticky provedou užitečné operace, obohatí se hlavičky. Byl vytvořen asistent, který vyhodnotí a doporučí nejvhodnější akci, tak abychom ušetřili lidskou práci. Tento krok ve vývoji je klíčovým pro řešení pravidelně značně narůstajícího množství incidentů.

V uplynulém roce se dále pokračovalo s vývojem *run-or-raise* doplňku do operačních systémů na bázi Gnome3. Uživatel si může zkratky upravit pomocí modů. Novinkou je, že je možné pro zkratky používat i speciální klávesy, které systém normálně použít nedovoluje (vypnutý/zapnutý Num_Lock). Navíc stejně jako u utility pythonize (pz) byl sestavený podrobný technický návod pro developery.

Na závěr je pak podstatné zmínit spolupráci na provozu nástroje dns-crawler. V rámci projektu ADAM tým ve spolupráci s ALEF NULA prošel z hlediska bezpečnosti statistiky zóny,

analyzoval provoz. Výsledky této spolupráce a výstup projektu pak byly prezentovány na Pracovní skupině CSIRT.CZ.

2. Služba MDM (MALICIOUS DOMAIN MANAGER)

Mezi trvalé aplikace a služby poskytované CSIRT.CZ patří MDM.

V rámci služby MDM tým využívá především veřejně dostupné zdroje informující o doménách s webovými prezentacemi, které byly napadeny a jsou pak útočníky zneužívány k phishingovým útokům či šíření malware. Pomocí této služby jsou tedy vytěžována data z veřejných zdrojů a následně přeposílána osobám zodpovědným za chod napadené domény s žádostí o prošetření a případnou nápravu situace. Na požádání je držitelům domén poskytnutá pomoc s analýzou a řešením incidentu. V případě zájmu je také možnost požádat o otestování odolnosti webové prezentace na dané doméně službou Skener webu. V roce 2021 bylo řešeno 386 URL na 271 doménách.

3. 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 zranitelnosti probíhá ve dvou fázích.

Během první fáze je pomocí automatických nástrojů proveden test webu. Následně je vykonán manuální test webu zkušeným testerem, který mimo jiné vyhodnotí nalezené zranitelnosti v kontextu celého webu a navrhne vhodná řešení a východiska pro zlepšení. Na konci je žadateli zaslána podrobná závěrečná zpráva, která obsahuje nalezené zranitelnosti, jejich posouzení dle závažnosti, a také návrhy konstruktivního řešení. Analýza potenciálních zranitelností vychází nejen z vlastních měření a aplikace zkušeností bezpečnostního týmu, ale také ze zkušeností bezpečnostní komunity. Přihlíží se také k žebříčku Top 10 obecně nejzávažnějších bezpečnostních rizik sestavených v rámci projektu Open Web Application Security (OWASP).

V průběhu roku 2021 došlo k testování 26 domén na základě 18 podaných objednávek. Pro významné subjekty bylo testováno dohromady 9 domén. V rámci projektu Safer Internet Centre bylo testováno 5 subjektů.

4. Honeypoty

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

Na linuxových honeypotech cowrie jsme v roce 2021 zaznamenali 1 509 unikátních vzorků malware. Na Windows honeypotech dionaea jsme pak zaregistrovali 126 vzorků. V případě

cowrie honeypotů se jedná v porovnání s předešlým rokem o 41 % pokles množství zaregistrovaných vzorků, oproti tomu u dionaea honeypotů je tento pokles minimální.

HAAS STATISTIKY

Počet registrovaných uživatelů	3 750
Počet spojení/útoků	0
Počet provedených příkazů	30 556 533
Počet unikátních útočících IP adres	720 141
Počet zachyceným unikátních vzorků	1 205

5. PROKI

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

Prvním 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 ohrožené 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 diskuzí 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.

Výstupy z projektu Turris Sentinel jsou využívány pro bezpečnostní analýzy v rámci činnosti týmu a jsou ukládány spolu s daty ze systému PROKI. Vzhledem k různorodé povaze a množství dat, která získáváme, vyvstala nutnost vytvořit efektivnější způsob jejich ukládání. Tak, aby bylo usnadněno provádění analýz. Výstupem se stalo vytvoření návrhu, který byl následně implementován. I dalších letech bude pokračovat rozvoj tohoto projektu a zefektivňování zpracovávání dat.

Statistika k PROKI za rok 2021	Počet
Počet odeslaných emailů z PROKI	32 454
Počet unikátních příjemců (abuse kontaktů) PROKI hlášení	628
Počet unikátních českých IP adres, které jsme nějakým způsobem zaznamenali	88 871

6. Osvěta a vzdělání

Tým CSIRT.CZ i nadále v roce 2021 pokračoval v oblasti školení a vzdělávání ve spolupráci s Akademií CZ.NIC. Vzhledem k probíhající pandemii a s ohledem na platná nařízení nebylo možné realizovat v určitých kvartálech školení přímo fyzicky v prostorech Akademie CZ.NIC. Ačkoli nebylo možné se účastnit vzdělávacích kurzů in persona, alespoň část školení probíhala virtuálně. Uživatelé se tak mohli zúčastnit online školení na téma *Bezpečnost a soukromí na internetu* zaměřeného na nejčastější hrozby v oblasti kybernetické bezpečnosti. To, jak je rozpoznat, směřuje také k pochopení prevence a seznámení uživatelů s aktivními a pasivními digitálními stopami. Tedy s riziky, zásady bezpečného chování, soukromím a anonymitou na Internetu. K osvětové činnosti, které se tým pravidelně dlouhodobě věnuje patří také již zmíněné publikování dvaceti pěti příspěvků v rámci seriálu *Postřehy z bezpečnosti* a zveřejňování příspěvků v rámci sekce Aktuálně z bezpečnosti. Více informací je možné nalézt v následující kapitole. V souvislosti s osvětou a vzděláváním stojí za zmínku další školení jak veřejnoprávních, tak soukromoprávních subjektů, tak i komerčních subjektů – například školení pro zaměstnance Nestlé Česko s.r.o.

Dalším úspěšným krokem se pak stalo navázání na školení *Základy fungování CSIRT/CERT týmů* a realizování pilotního školení pro nové členy bezpečnostních týmů na území ČR.

7. 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 2021 tým publikoval celkem 25 příspěvků.

Krom seriálu *Postřehy z bezpečnosti* je možné sledovat na webových stránkách týmu CSIRT.CZ sekci *Aktuálně z bezpečnosti*, která je určená k rychlému a stručnému šíření nejpodstatnějších informací o aktuálně probíhajících útocích a objevených zranitelnostech. Sekce AZB se stala vyhledávaným zdrojem spolehlivých informací z oblasti bezpečnosti, a to nejen pro administrátory a uživatele, ale také pro média, díky nimž se pak informace o nových útocích mohou rychle rozšířit mezi další potenciální oběti, především běžné uživatele. V roce 2021 bylo v rámci této sekce publikovaných 39 aktualit.

8. Národní a mezinárodní spolupráce

Rovněž jako v uplynulých letech tým CSIRT.CZ v průběhu roku 2021 aktivně spolupracoval s dalšími bezpečnostními týmy v rámci celé Evropy – zejména v otázce řešení a koordinace řešení bezpečnostních incidentů, sdílení best practices a přípravě převzetí štafety předsednictví v síti CSIRTs Network. Tým CSIRT.CZ se pravidelně účastní mezinárodních virtuálních meetingů, konferencí, hlasování atd.

Činnosti národní a mezinárodní spolupráce je možné rozdělit do několika směrů.

Prvním z nich – na národní úrovni – je seznamování bezpečnostních týmů s různou constituency s možnostmi zapojení do struktur mezinárodní komunity a následné projednávání a realizování kroků vedoucích k přijetí těchto týmů do mezinárodních komunit, potažmo k jejich aktivnímu zapojení.

Dalším směrem spolupráce je pravidelné setkávání členů české národní bezpečnostní komunity na Pracovní skupině CSIRT.CZ. Tu se podařilo zorganizovat v roce 2021 pouze jednou, na podzim.

Kromě zmíněného pravidelného setkávání české komunity se bezpečnostní týmy na území ČR spoluúčastní setkání v rámci TF-CSIRT a dalších mezinárodních komunitních konferencí a meetingů.

I v roce 2021 se podařilo ČR si udržet na úrovni evropské bezpečnostní komunity statut země s nejvíce registrovanými a zapojenými týmy v mezinárodní komunitě *Trusted Introducer*. K 1. 1. 2022 bylo zapojeno v TI celkem 55 bezpečnostních týmů z ČR.

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.I přes opatření související s Covidem-19 a změny, které pandemie přinesla nedošlo k narušení fungující této spolupráce mezi týmem ani z dlouhodobého, ani krátkodobého hlediska. Tato tradiční spolupráce mezi národním CERT týmem (CSIRT.CZ) a NÚKIBem (vládním týmem GovCERT.CZ) je založená zejména na společném řešení incidentů, sdílení nezbytných informací, stejně jako nejrůznějších odborných konzultacích, zejména mezi Národním bezpečnostním týmem CSIRT.CZ a vládním týmem GovCERT.CZ. Spolu tyto týmy plní povinnosti definované NIS směrnici ve vytvořeném CSIRT Networku, v jehož rámci mimo jiné aktivně spolupracují s dalšími evropskými národními a vládními týmy. Národní bezpečnostní tým CSIRT.CZ a vládní tým GovCERT.CZ se několikrát ročně setkávají při nejrůznějších příležitostech. Tím je zajištěn dostatečný prostor pro pravidelné informování o práci a činnosti jednotlivých týmů, pravidelná konzultace a případná koordinace spolupráce.

Rozsah, charakter a frekvenci národní a mezinárodní spolupráce od roku 2020 ovlivnila zásadním způsobem skutečnost, že k 1. 1. 2022 se stala ČR jedním ze členů předsednictva (tria) v rámci sítě CSIRTs Network, jež funguje na principu rotačního předsednictví. Vstupu do předsednictví nutně předcházela několikaměsíční příprava a spolupráce mezi národním týmem CSIRT.CZ a vládním týmem GovCERT.CZ.

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.[1]

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

Závěr

Rok 2021 navázal svými ztíženými podmínkami na rok 2020. Platí však, že stejně jako první rok pandemie je velmi obtížné a náročné komparovat tento rok s předešlými roky. Proto je třeba nahlížet na změny, kroky a dosažené výsledky jinak než před pandemií.

Tým CSIRT.CZ byl i v době pandemie řízen způsobem, který koncepčně i organizačně reagoval na probíhající nařízení a změny tak, že bilance na konci roku potvrdila, že se mu podařilo nejen udržet stávající kvalitu poskytovaných služeb, ale také posunout se vpřed, zejména v oblasti vývoje vlastních služeb a prvků, jež přímo souvisí s kvalitou a efektivitou procesu incident handlingu.

---

1) Technicko-organizační cvičení Cyber Europe 2020 bylo z důvodu pandemie přeloženo na rok 2022.

Uvedenou skutečnost potvrdil také re-certifikační audit TF-CSIRT, ve kterém CSIRT.CZ obhájil nejvyšší možnou úroveň členství v této organizaci.

Za výrazný úspěch lze považovat také skutečnost, že tým dovedl nejen dlouhodobě, od počátku pandemie až do současnosti udržet i paletu služeb, které poskytuje nad rámec obligatorních povinností vycházejících z legislativního rámce ČR, ale také – bez ohledu na ztížené podmínky rozšířit rozsah svých služeb a prohloubit možnosti spolupráce.