ZPRÁVA O ČINNOSTI CSIRT.CZ (NÁRODNÍHO CSIRT ČR) ZA ROK 2025

CSIRT.CZ

Obsah

O CSIRT.CZ 3
Rok 2025 v kostce 3
1. Incident handling 4
1.1. Statistiky incidentů v roce 2025 4
1.2. Vývoj open-source nástrojů a utilit 7
1.3. Boj s phishingem v doméně .CZ 8
2. Skener webu 8
2.1. Automatické testování pro školy 9
3. Honeypoty 9
3.1. HaaS 9
3.2 Minipoty Turris 10
3.3 Linuxové honeypoty Cowrie 10
4. PROKI 11
5. Penetrační a zátěžové testování 12
6. Osvěta a vzdělávání 12
7. Aktuálně z bezpečnosti 13
8. Národní a mezinárodní spolupráce 13
Závěr 14

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 s tehdejším 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.

1. listopadu 2025 nabyl účinnosti nový zákon o kybernetické bezpečnosti (č. 264/2025 Sb.), který v § 43 upravuje podmínky fungování národního CERT a vymezuje jeho základní úkoly.

Cílem týmu CSIRT.CZ je především řešení incidentů, které se týkají kybernetické bezpečnosti v sítích provozovaných v České republice, a s přijetím nového zákona se jeho role a především potom zákonná povinnost rozšířila na všechny poskytovatele regulovaných služeb spadajících do režimu nižších povinností.

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 nebo zákona vyměňuje informace o jednotlivých incidentech a jejich řešeních.

Rok 2025 v kostce

V roce 2025 se bezpečnostní tým CSIRT.CZ věnoval přípravám na zvládnutí požadavků nové legislativy a na nové povinnosti plynoucí z nového zákona o kybernetické bezpečnosti, č. 264/2025 Sb., rozvoji komunity CSIRT a dalších bezpečnostních týmů v oblasti kybernetické bezpečnosti v Česku a v evropském regionu, kromě toho také osvětě a vzdělávání. Možná si někteří vzpomenou, že jsme v minulém roce s potěšením konstatovali snížení počtu nám nahlášených incidentů, tento pozitivní pokles se v letošním roce však neopakoval, naopak došlo k významnému nárůstu incidentů, a to o více než 30 %.

V průběhu roku jsme dále rozvíjeli naše technické nástroje a služby podporující řešení incidentů i prevenci kybernetických hrozeb. Důležitou roli v této oblasti sehrál systém PROKI, který slouží ke shromažďování, vyhodnocování a automatizovanému předávání informací o bezpečnostních událostech správcům sítí. Nadále jsme také rozvíjeli vlastní open-source nástroje a utility, které podporují každodenní operativní činnost týmu a usnadňují spolupráci v rámci bezpečnostní komunity.

Významnou součástí naší práce zůstala prevence a ochrana uživatelů před phishingem a dalšími podvodnými aktivitami. V doméně .CZ se nám díky úzké spolupráci v rámci sdružení CZ.NIC daří dlouhodobě velmi rychle reagovat na škodlivé domény a omezovat jejich dopad na uživatele.

Také jsme věnovali značné úsilí osvětě a vzdělávání. Realizovali jsme odborná školení, vystupovali na konferencích a odborných akcích a publikovali články zaměřené na aktuální bezpečnostní hrozby, zranitelnosti i praktické zkušenosti z naší činnosti. Nově jsme začali rozvíjet také koncept table-top cvičení, které organizacím umožňuje lépe prověřit jejich připravenost na řešení rozsáhlých kybernetických incidentů.

Významným momentem roku 2025 bylo také zvolení členky našeho týmu do čela řídícího výboru evropské komunity bezpečnostních týmů TF-CSIRT, což posiluje naše zapojení do mezinárodní spolupráce v oblasti kybernetické bezpečnosti.

Výroční zpráva přináší podrobnější přehled těchto aktivit.

1. Incident handling

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

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

1.1. Statistiky incidentů v roce 2025

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. Do listopadu tohoto roku se náš tým CSIRT.CZ podílel na řešení a koordinaci bezpečnostních incidentů, které měly původ nebo cíl v sítích provozovaných v České republice nebo se obecně dotýkaly jejího kyberprostoru. Tento rámec naší působnosti byl 1. listopadu tohoto roku významně konkretizován. Neznamená to však, že bychom přestali řešit incidenty, které nám nahlásí subjekty, které do současné regulace nespadají.

Tým CSIRT.CZ slouží i nadále jako kontaktní místo pro hlášení incidentů i mimo oblast regulace a řeší problémy (tzn. reportované 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 souvislosti s účinností zákona č. 264/2025 Sb., o kybernetické bezpečnosti, došlo k významnému rozšíření a novému vymezení naší působnosti. Samotné poskytování našich služeb se nemění.

Zásadní změny se týkají především regulovaných subjektů. Ty jsou nově povinny splnit zákonné požadavky, zejména ohlásit regulovanou službu, zavést stanovená bezpečnostní opatření a hlásit kybernetické bezpečnostní incidenty s významným dopadem. Nesplnění těchto povinností může vést k uložení sankcí podle § 59 zákona č. 264/2025 Sb.

V roce 2025 řešil náš tým 3005 incidentů - to představuje nárůst o více než 30 % oproti roku 2024. Domníváme se, že se do tohoto nárůstu promítlo intenzivní projednávání nového zákona, po němž nám začaly reportovat incidenty subjekty, které doposud tuto povinnost neměly, ale na základě nové legislativy předpokládají, že se jich bude týkat, a na tuto skutečnost se tak včas připravily. Dále se do celkového počtu incidentů promítla proaktivní snaha zákazníků Deny listů, kteří nám předávají své poznatky.

Statistiky za posledních pět let si můžete zobrazit na našich webových stránkách.
Celou historii incidentů je možné stáhnout v .csv formátu pod tabulkou se statistikami.

STATISTIKA PROCESU ŘEŠENÍ BEZPEČNOSTNÍCH INCIDENTŮ TÝMEM CSIRT.CZ

	2022	2023	2024	2025
Sensor Network*	8 815	8 903	9 682	6 853
Phishing	1 485	2 064	1 689	2 003
Spam	220	352	260	483
Malware	228	163	108	179
Other	24	35	53	84
Information gathering	71	105	99	126
DOS	0	12	4	5
Intrusions	39	21	69	125
Celkem	**2 067**	**2 752**	**2 282**	**3 005**

* 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 naše veřejně dostupné materiály dostupné na našem webu.

Z uvedené tabulky je patrné, že phishing dominuje celkovému počtu námi řešených incidentů. Počet nahlášených incidentů koresponduje s tím, že se jedná o jednu z nejvýznamnějších kybernetických hrozeb. Dle reportu, který k tématu vydává pracovní skupina APWG, významně rostl počet phishingových útoků na sociálních sítích, prostřednictvím SMS (smishing) a také se zvětšil objem útoků prostřednictvím SMS a e-mailů cílených na firemní e-maily, tzv. Business Email Compromise (BEC).

Na řešení bezpečnostních incidentů spolupracujeme s Policií ČR a jejich specializovanými pracovišti. Neoddělitelnou součástí řešení bezpečnostních incidentů je také samozřejmě spolupráce s dalšími bezpečnostními týmy nejen v rámci působnosti ČR, ale také v distribuci důležitých informací o zranitelnostech, útocích a dalších důležitých informacích potřebných pro ochranu nejen našich konstituentů. 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 orgány státní správy a dalšími relevantními subjekty.

Díky naší synergii se sdružením CZ.NIC máme v zóně .CZ možnost proaktivně vyhledávat potenciálně škodlivé domény a rozvíjet naši schopnost rychle eliminovat phishingové weby tak, abychom útočníky odradili od jejich využívání.

Závěrem této kapitoly je třeba zdůraznit, že naše statistiky zdaleka neodrážejí celkový počet incidentů v Česku, řada z nich stále zůstává neohlášena. Přijetí nového zákona by mělo tuto míru latentnosti snížit, avšak i přes výrazné rozšíření působnosti a odpovědnosti se jeho aplikace nevztahuje na všechny subjekty. Nadále proto poskytujeme naše služby i subjektům mimo zákonnou regulaci a současně se zaměřujeme na zvyšování povědomí o bezpečném chování v kyberprostoru.

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 naše schopnost vyvíjet k tomu potřebné nástroje a utility. Ty se snažíme vždy vyvíjet jako open-source, což je v souladu s politikou a přístupem našeho sdružení. Účelem tohoto vývoje je zkvalitňování řešení procesu incident handlingu a usnadnění a zefektivňování spolupráce na národní i mezinárodní úrovni, kde dochází k neustálému vývoji systémů, nástrojů a doplňků, které tým CSIRT.CZ používá.

Také v tomto roce pracoval CSIRT.CZ na dalším zefektivnění postupů při řešení incidentů. Hlavní motivací byla příprava na nárůst počtu reportovaných incidentů, který očekáváme v souvislosti se značným rozšířením množství subjektů spadajících do působnosti CSIRT.CZ. V rámci těchto příprav jsme pracovali na aplikačním rozhraní pro komunikaci s Portálem NÚKIB a další automatizaci práce s našimi nástroji.

Vyvíjeli a udržovali jsme i nadále všechny naše open-source nástroje. Knihovna Mininterface, která poskytuje obecné uživatelské rozhraní, má přes 30 000 stažení a nasadili jsme ji jak do mnoha backendových skriptů, tak do našich open-source nástrojů, kde to dává smysl, např. Convey (slouží k hromadné analýze incidentů, které se týkají velkého množství konstituentů a automatizaci komunikace) a Deduplidog (pomáhá organizovat soubory odstraněním duplicit, což nejen šetří místo, ale může i zabránit zmatkům s větším počtem verzí citlivých dokumentů). Jejich kód se tedy ztenčil a část poskytující uživatelské rozhraní se vyvíjí jen jednou, nikoli pro každý program zvlášť. Každé její zlepšení se tím automaticky dostává do všech ostatních našich i dalších programů, které knihovnu využívají. Ta byla v minulém roce opatřena stabilním aplikačním rozhraním s velkým množstvím funkcí, například webovým rozhraním, každý program je tak nyní plně ovladatelný i přes webový prohlížeč. Pro bezpečné zpracování e-mailů používáme knihovnu Envelope. Nástroj Touch-timestamp potom umožňuje změnu časových značek souborů, což je užitečné při synchronizaci a archivaci souborů.

1.3. Boj s phishingem v doméně .CZ

Jak je patrné z tabulky uvedené v kapitole 1.2 (Statistiky incidentů v roce 2025), zaznamenali jsme 2 003 phishingových incidentů. Ve srovnání s rokem 2024 to představuje nárůst o více než 18 %. Většina phishingových stránek však není hostována v doméně .CZ. U té jsme schopni velmi rychlé reakce. 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. Od roku 2022 jsme zlepšovali monitorování podvodných domén a jejich následné vyřazování. Tento proces jsme nastavili natolik precizně, že jsme již druhým rokem schopni doménu blokovat ještě předtím, než nám přijde první hlášení od uživatelů, a v některých případech dokonce do 15 minut od jejího zpřístupnění. Za phishingovými útoky samozřejmě stojí lidé, kterým se nevyplatí věnovat nadměrné úsilí do 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. Důkazem je to, že pouhé 1 % z celkového počtu nahlášených phishingových domén je s koncovkou .CZ. Tyto zaznamenané domény byly samozřejmě bezodkladně vyřazeny ze zóny.

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 odhalit potenciální zranitelnosti jejich 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 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).

Služba byla v tomto roce nově zpoplatněna, a to s cílem zajistit efektivnější využívání našich kapacit ve prospěch širšího okruhu konstituentů. Zároveň tím došlo k jejímu zpřístupnění také komerčním subjektům, které o ni projevily zájem. Typicky se jedná o menší společnosti, pro něž není komplexní penetrační testování vhodné nebo ekonomicky dostupné. V daném období náš tým obdržel šest žádostí, z nichž byly schváleny čtyři. Neziskové a veřejně prospěšné organizace mohou po individuální domluvě s obchodním oddělením získat pro skenování svých webových stránek zvýhodněné podmínky.

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.

3. Honeypoty

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

3.1. HaaS

Projekt Honeypot as a Service (HaaS) je služba umožňující provoz distribuované sítě honeypotů, které zachycují automatizované útoky na internetu a poskytují data pro analýzu chování útočníků a jejich nástrojů. Do výzkumného projektu HaaS se může dobrovolně zapojit kdokoliv, a přispět tak ke zlepšení kybernetické bezpečnosti a připravenosti na kybernetické útoky. Zapojeným uživatelům zároveň poskytujeme zajímavé informace o útocích, které byly zaznamenány na jejich zařízení. V rámci této služby máme registrovaných několik tisíc uživatelů, kteří nám tak pomáhají s monitoringem provozu. Níže uvádíme statistiky za reportované období:

Z celkového počtu 197 901 zachycených unikátních vzorků se ve 174 529 jednalo o HTML

HAAS STATISTIKY

Počet registrovaných uživatelů	12 325
Počet spojení/útoků	50 687 590
Počet provedených příkazů	45 494 729
Počet unikátních útočících IP adres	72 886
Počet zachycených unikátních vzorků	197 901

dokument. Namátková kontrola těchto dokumentů ukázala, že jejich velká část představuje především reklamní nebo přesměrovávací stránky propagující různé služby, typicky například nabídky síťových proxy nebo podobných nástrojů.

3.2 Minipoty Turris

Vedle projektu HaaS provozujeme na našich Turris routerech také sadu mini honeypotů (minipotů), ty simulují vybrané běžně napadané internetové služby. Konkrétně se jedná o služby SMTP, Telnet, FTP a HTTP. Slouží především k dlouhodobému sledování automatizovaných útoků, které se zaměřují na veřejně dostupné služby, a k získávání dat pro další analytické zpracování.

Získaná data využíváme zejména k detekci nových typů útoků a k sestavování slovníků nejčastěji používaných hesel a přihlašovacích kombinací, které útočníci využívají při pokusech o prolomení autentizačních mechanismů. Nejčastější hesla, která útočníci používají při pokusech o průnik do systémů, jsou 123456, 123qwe!@#, root@123, Admin123!@#, 1qaz@WSX, admin@123. Tyto kombinace byly použity vícekrát než ještě o něco jednodušší hesla ve formátu 12345, 1234, 123 či 111111.

Statistiky z těchto minipotů za sledované období ukazují vysokou míru automatizovaného skenování a pokusů o přihlášení.

MINI_HONEYPOT STATISTIKY

Počet útoků na smtp honeypoty	6 000 000
Počet útoků na telnet honeypoty	600 000
Počet útoků na ftp honeypoty	100 000
Počet útoků na http honeypoty	30 000

Analýza zdrojových IP adres ukazuje, že významná část útoků pocházela ze sítí lokalizovaných například v Íránu, Rumunsku a Německu. Ve velkém množství případů se jednalo o automatizované skenování internetu, jehož cílem je vyhledávání zranitelných zařízení nebo služeb s výchozími či slabými přihlašovacími údaji.

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

3.3 Linuxové honeypoty Cowrie

Dalším zdrojem dat jsou pro nás linuxové honeypoty Cowrie. Ty simulují kompromitované systémy dostupné přes SSH a umožňují detailně sledovat chování útočníků po úspěšném přihlášení. V průběhu roku se nám podařilo díky rozšíření infrastruktury a zlepšení sběru dat zachytit 2 687 016 unikátních vzorků souborů, které se útočníci pokusili do honeypotů nahrát nebo spustit.

4. PROKI

V roce 2015 zahájil Národní bezpečnostní tým CSIRT.CZ realizaci projektu PROKI, podpořeného v rámci Programu bezpečnostního výzkumu České republiky v letech 2015 až 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.

CSIRT.CZ spolupracuje s projektem Turris Sentinel, který pomáhá detekovat útočníky skrze vyhodnocování firewallových logů, provozováním tzv. minipotů (tedy miniaturních honeypotů) a také plnohodnotných honeypotů (HaaS), o kterých jsme psali v předcházející kapitole. 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 roce 2025 systém PROKI zpracovával události pocházející z 33 veřejných i neveřejných zdrojů dat a nadále sloužil jako nástroj pro agregaci informací o bezpečnostních incidentech a jejich automatizované předávání správcům sítí. Na základě těchto dat systém generuje hlášení zasílaná na příslušné abuse kontakty, aby bylo možné na incidenty včas reagovat a přijmout odpovídající bezpečnostní opatření. Souhrnné statistiky systému PROKI za rok 2025 jsou uvedeny v následující tabulce.

Statistika k PROKI za rok 2025	Počet
Počet e-mailů odeslaných z PROKI	43 047
Počet unikátních příjemců (abuse kontaktů) PROKI hlášení	832
Počet unikátních českých IP adres, které jsme nějakým způsobem zaznamenali	360 394

Statistiky ukazují, že význam systému PROKI spočívá především ve schopnosti automatizovaně zpracovávat velké objemy dat týkající se bezpečnostních událostí a efektivně předávat relevantní informace správcům sítí, kteří mohou na jejich základě identifikovat zranitelná nebo kompromitovaná zařízení a přijímat odpovídající bezpečnostní opatření.

5. Penetrační a zátěžové testování

V průběhu roku jsme poskytovali penetrační testování jak komerčním subjektům, tak veřejné správě. Penetrační testování podstoupily i dva významné projekty sdružení, DNS Portál a DNS Patrol.

6. Osvěta a vzdělávání

CSIRT.CZ se i nadále věnoval již zavedeným školením Bezpečnost a soukromí na Internetu a Forenzní analýza paměti. Kromě toho jsme spustili dva další kurzy. První z nich, Základy penetračního testování webových aplikací, poskytuje základní přehled o penetračním testování webových aplikací, a to s důrazem na praktické dovednosti. Druhý z kurzů je určen pro všechny společnosti, které plánují založit oficiální CSIRT tým a získat členství v některé z mezinárodních organizací, jež tyto týmy sdružují.

Nadále byla také realizována školení na míru pro zaměstnance MěÚ Mikulov, pro sdružení Slezská brána – zaměstnance místních úřadů nebo pro Státní ústav radiační ochrany.

Připravili jsme také zcela nový koncept školení v podobě takzvaného table-top cvičení. Jedná se o formu cvičení, v rámci které si organizace testují procesní připravenost na řešení rozsáhlého kybernetického incidentu.

Zástupci týmu CSIRT.CZ také několikrát vystupovali v tradičních médiích, ve veřejnoprávních i v soukromoprávních. Na blogu zaměstnanců má náš tým v top 10 nejčtenějších článků sdružení CZ.NIC hned tři příspěvky. Dále publikují členové týmu články o aktuálních tématech, 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.

CSIRT.CZ se také tradičně věnoval prezentaci vlastních zkušeností na různých fórech a konferencích. Z vystoupení pro odbornou veřejnost lze jmenovat například vystoupení na akcích jako TF-CSIRT, C2S2, ICANN nebo LinuxDays 2025 či Alternativo Security Days.

7. Aktuálně z bezpečnosti

I v roce 2025 jsme pokračovali v aktivní spolupráci se serverem Root.cz s vlastním seriálem *Postřehy z bezpečnosti*. Jedná se o pravidelný bezpečnostní přehled uplynulých dní. Na tom spolupracují kromě nás autoři ze sdružení CESNET, ALEF-CSIRT, ČD Telematika, Nettles Consulting a zakladatelka neziskové organizace TheCyberValkyrez a spoluzakladatelka portálu CYBULE, Monika Kutějová.

Publikované informace poukazují na nejzajímavější události, aktuality, stejně jako i zranitelnosti, kterým by měla být věnována pozornost. Stejně tak jako v předchozích letech se podařilo díky naprosto bezproblémové spolupráci týmu autorů publikovat 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 byla i nadále rozvíjena spolupráce se zástupci bezpečnostních týmů v rámci konstituence CSIRT.CZ i mimo ni a pokračovala úzká spolupráce s Policií ČR a NÚKIB. Kromě obvyklé zákonem stanovené činnosti probíhala intenzivní jednání k přípravě provozování CSIRT.CZ v rámci nového zákona o kybernetické bezpečnosti a spolupráce na přípravě Cyber Europe 2026.

V rámci preventivní činnosti a zvyšování povědomí o problematice kybernetické bezpečnosti byly zajišťovány školení, přednášky a workshopy. Ty se týkaly, jak již bylo uvedeno v kapitole Osvěta a vzdělávání, například soukromí a bezpečnosti na internetu, povinností vyplývajících z nového zákona o kybernetické bezpečnosti, zkušeností týmu s phishingem v .CZ doméně či prezentace projektů týmu CSIRT.CZ.

V rámci pracovní skupiny CSIRT.CZ a pracovní skupiny FÉNIX bylo uspořádáno setkání s více než 120 účastníky, na kterém vystoupili odborníci z akademické, soukromé i veřejné sféry.

Dalšími důležitými činnostmi na poli národní, ale především mezinárodní kybernetické bezpečnosti, jsou obligatorní aktivity vyplývající ze směrnice NIS2 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 evropské směrnice NIS 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 minulosti vykonávalo naše sdružení roli Standing Representative za Česko, tuto roli si však od roku 2025 převzal NÚKIB, a náš tým se tak účastní setkání v rámci CSIRTs Network především zprostředkovaně a podle aktuální potřeby.

Významným úspěchem letošního roku bylo zvolení členky našeho týmu do čela řídícího výboru organizace TF-CSIRT. Jedná se o komunitu profesionálů z oblasti kybernetické bezpečnosti napříč sektory. Výkon této pozice nám dává možnost aktivně ovlivňovat dění v rámci mezinárodní spolupráce bezpečnostních týmů v evropském regionu. Zástupkyně našeho týmu v uplynulém roce v rámci výkonu této funkce spolupořádala dvě mezinárodní konference s účastí více než 150 týmů z celé Evropy. Díky této roli se naše sdružení zároveň podílí na fungování a strategickém směřování nejen komunity TF-CSIRT, ale i organizace Open CSIRT Foundation, nezávislé nizozemské neziskové nadace zaměřené na posilování kybernetické odolnosti prostřednictvím rozvoje spolupráce a řízení bezpečnostních incidentů. Česká republika má i díky podpoře projektu FÉNIX v současnosti 73 členských týmů, z toho 6 certifikovaných, 20 akreditovaných a 39 zalistovaných. 2 další týmy čekají na udělení certifikace, 1 tým na akreditaci, další 3 týmy čekají na obnovení členství v základní úrovni a 2 zcela nové týmy se chtějí do komunity zapojit. Oproti roku 2024 došlo k opětovnému zvýšení počtu členských týmů.

V rámci mezinárodního sdružení incident response týmů FIRST má Česká republika jednoho nového zájemce o zapojení do komunity.

Zástupcům Argentiny, Ázerbájdžánu a zemí západního Balkánu jsme představili činnost našeho týmu a sdíleli naši osvědčenou praxi.

Kromě výše uvedeného tým v oblasti zajištění národní i mezinárodní bezpečnosti pokračuje ve spolupráci s dalšími bezpečnostními týmy a subjekty prostřednictvím konzultací a podpory, kterou poskytuje.

Závěr

Závěrem lze konstatovat, že ačkoliv se rok 2025 nesl především ve znamení příprav na změny vyplývající z nového zákona o kybernetické bezpečnosti č. 264/2025 Sb., v rámci kterých jsme se soustředili na přípravu procesů a technických nástrojů tak, aby byl tým připraven na nové povinnosti a širší okruh subjektů spadajících do regulace, věnovali jsme se stále stejně kvalitně naší hlavní činnosti, kterou je řešení a koordinace bezpečnostních incidentů, sdílení informací o hrozbách a spolupráce s provozovateli sítí, bezpečnostními týmy i orgány veřejné správy. Pokračovali jsme v rozvoji technických nástrojů a služeb, které podporují prevenci kybernetických hrozeb a umožňují rychlejší identifikaci a předávání informací o bezpečnostních incidentech tak, aby naše činnost byla co nejefektivnější.

Vedle plnění zákonných povinností jsme se současně věnovali také rozvoji dalších služeb a projektů, které přispívají ke zvyšování bezpečnosti v kyberprostoru. Patří mezi ně například systém PROKI nebo provoz honeypotů, jejichž cílem je včasná identifikace škodlivých aktivit, sdílení informací o hrozbách a podpora prevence bezpečnostních incidentů. Těší nás, že na těchto aktivitách spolupracujeme s mnoha partnery z řad provozovatelů sítí a dalších organizací, které sdílejí přesvědčení, že systematická prevence je účinnější a efektivnější než následné řešení dopadů kybernetických incidentů.

Důležitou součástí naší práce v reportovaném roce byla rovněž osvěta a vzdělávání, publikování odborných informací a aktivní zapojení do národní i mezinárodní spolupráce v oblasti kybernetické bezpečnosti.