Směr, kterým se ubírá Národní bezpečnostní tým CSIRT.CZ

Objem práce a složitost úkolů CSIRT/CERT (Computer Security Incident Response Team/Computer Emergency Incident Response Team[1]) týmů v uplynulých letech výrazně narostly. Proč jsou však dnes úkoly, jejichž plnění se od týmů očeká, o tolik složitější a proč tak výrazně narostl počet týmů v českém soukromém sektoru?[2]

V každé IT firmě jsou již tradičně zastoupeny pozice či týmy zabývající se řízením, administrací systému, vývojem, každodenním provozem či marketingem. S provozem každého systému vystaveného do Internetu však jde ruku v ruce i bezpečnost. Řešení bezpečnostních incidentů či provozních záležitostí souvisejících s bezpečností však nikde do tradičního modelu řízení IT společností nezapadá. Právě proto se postupně vytvářejí CSIRT/CERT, které si již své formální či neformální místo našly v každé větší organizaci. Cílem každého takového týmu je dosáhnout pokud možno nejvyšší míry bezpečnosti. O CSIRT týmech a konkrétně o Národním týmu CSIRT.CZ se dočtete také v článcích Andrey Kropáčové v DSM 2015/1 a 2015/2.

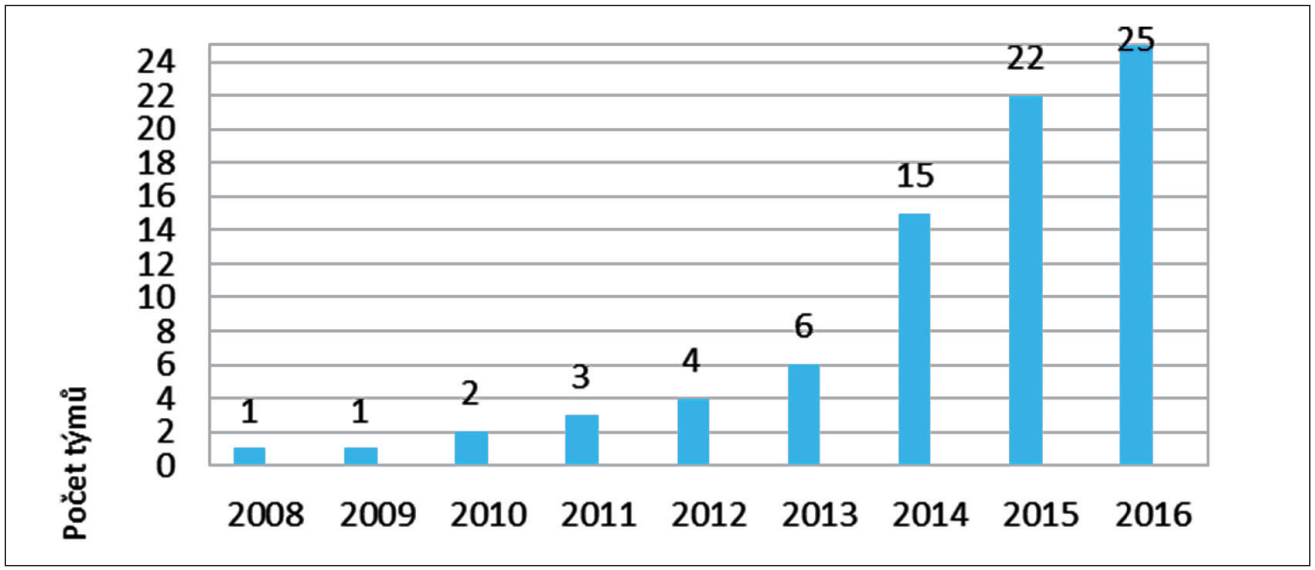
Bezpečnost je velice širokým pojmem a CSIRT týmy se od sebe výrazně liší nejen podle velikosti, ale hlavně zaměřením a oblastí působnosti, resp. konstituencí. Zpravidla rozeznáváme několik druhů bezpečnostních týmů: vládní, národní, interní a produktové. I když se velká část práce těchto týmů odlišuje, zdrojem jsou stále bezpečnostní incidenty. Vládní týmy jsou zpravidla provozovány ministerstvem nebo jiným státním úřadem, který má ve své gesci problematiku kybernetické bezpečnosti. Do pole působnosti těchto týmů spadají většinou vysoké státní úřady, ministerstva a vybraná část kritické infrastruktury.

V případě České republiky má kybernetickou bezpečnost v pověření Národní bezpečnostní úřad, který provozuje vládní tým GovCERT. V oficiální gesci tohoto týmu jsou podle Zákona č. 181/2014 Sb. (Zákon o kybernetické bezpečnosti – dále jen ZKB) povinné subjekty uvedené §3. písm. c) správce informačního systému kritické informační infrastruktury, d) správce komunikačního systému kritické informační infrastruktury a e) správce významného informačního systému. Konstituencí národního týmu bývají veškeré IP rozsahy přidělené firmám a institucím z daného státu. Pokud v daném státě působí také jiné týmy, např. vládní tým nebo speciální

[1] Computer Emergency Incident Response Team byl vytvořen na Carnegie Mellon University v roce 1988. Pro používání názvu „CERT“ je potřebné mít ochrannou známku od dané univerzity.

[2] Článek vznikl v rámci projektu „Predikce a ochrana před kybernetickými incidenty (PROKI)“ (VI20152020026) realizovaného v rámci Programu bezpečnostního výzkumu ČR na léta 2015–2020.

tým pro kritickou infrastrukturu, rozsahy daných organizací jsou z konstituence týmu vyňaté. V případě České republiky spadají do oficiální konstituence dle ZKB povinné subjekty uvedené §3. písm. a) poskytovatel služby elektronických komunikací a subjekt zajišťující síť elektronických komunikací, pokud není orgánem nebo osobou podle písmene b), a b) orgán nebo osoba zajišťující významnou síť, pokud nejsou správcem komunikačního systému podle písmene d). Interní týmy mají na rozdíl od dvou předešlých pevně danou oblast působnosti a bývá to adresní prostor, který daná organizace spravuje. Produktové týmy se starají o zabezpečení produktů. Jsou většinou v USA, kde probíhá vývoj největších softwarových firem, jako je Windows, Apple, Adobe apod. Tyto týmy se zaměřují pouze na bezpečnost vlastních produktů, což vzhledem k produktovému portfoliu některých společností může být dost náročné.



Obr. 1: Nárůst počtu CSIRT/CERT týmů v České republice v uplynulých letech

Jaké týmy máme v prostředí českého Internetu?

Česká republika je v otázce rozvoje CSIRT týmů poměrně vyspělá. Již několik let stabilně funguje národní i vládní tým. Pod celou akademickou sítí pak působí odděleně další tým. Než se podíváme na výzvy, kterým čelí Národní bezpečnostní tým CSIRT.CZ, je třeba říci, jakou cestou může CSIRT tým dát najevo, že existuje a je připraven podílet se na řešení incidentů v rámci své konstituence.

V současné době existují dva různé způsoby, jak se zapsat do mezinárodní komunity CSIRT týmů. Komunita organizace FIRST[3], kde dominují americké, produktové a světové týmy, a komunita týmů v rámci Trusted Introducer[4], která je tvořená téměř výlučně evropskými týmy a převažují v ní akademické, národní a vládní týmy. Pro zapsání se do jednoho z těchto seznamů je nutné splnit kritéria, která si toto společenství bezpečnostních týmů zvolilo. Pro týmy je nejjednodušší získaní statusu „listed“, tudíž jenom zapsání se do seznamu týmu Trusted Introducer. Získání tohoto statusu je bezplatné. Této možnosti již využilo dvacet českých týmů z komerčního sektoru. Dalších pět týmů má vyšší status, a tudíž splnily více formálních podmínek pro členství. Na rozdíl od prostého zapsání týmu do databáze je udržování statutu akreditovaného týmu zpoplatněno ročními poplatky za členství.

Vyšší počet oficiálních týmů než Česká republika má jen Německo, a to o jeden tým. Trend nárůstu zájmu o založení oficiálního CSIRT týmu se začal objevovat po roce 2013, kdy byla část významných tuzemských služeb vyřazena z provozu v důsledku DDoS (Distributed Denial of Service) útoků. Tehdy byly v rámci útoků vyřazeny servery českých médií, bank a operátorů, což se odrazilo ve výrazné publicitě problematiky DDoS v České republice. Pod nárůst počtu týmů se podepsal také projekt FENIX, který vznikl na půdě sdružení NIX.CZ[5] jako reakce na tyto útoky z roku 2013. I když je primárním cílem projektu řešení DDoS útoků, v zásadní míře řeší členové i základní bezpečnostní standardy, k jejichž dodržování se zavazují. I když existují různá technická pravidla, která zabezpečují provoz sítí, chybí tu autorita, jež by jejich dodržování kontrolovala. Právě uskupení FENIX se snaží výměnou za dodržování různých pravidel technického a organizačního charakteru nabídnout sítím

[3] Forum of Incident Response and Security Teams – https://first.org
[4] Trusted Introducer provozuje databázi oficiálních CSIRT týmů a poskytuje prostor na výměnu zkušeností mezi bezpečnostními týmy, http://tf-csirt.org/
[4] Sdružení NIX.CZ představuje neutrální hardwarovou platformou pro vzájemné propojování sítí. Propojuje 140 sítí a v celkovém přenášeném množství dat dosáhlo maxima přes 446 Gbps.

v případě útoku odpojení se od sítě Internet a výměnu dat jen se sítěmi, kterým skutečně důvěřují a které dodržují pravidla bezpečného provozu. Jedním z organizačních pravidel je také vytvoření CSIRT týmu a jeho registrace, tj. zalistování v evropském sdružení CSIRT týmů TF-CSIRT. Právě toto pravidlo se podepsalo pod výrazný nárůst CSIRT týmů v České republice (viz obrázek 1 na předchozí straně).

Úkoly, které plní CSIRT.CZ – český národní CSIRT tým BOX 1

- tým CSIRT.CZ je provozován sdružením CZ.NIC, správcem domény .CZ
- tým funguje pod hlavičkou CZ.NIC od roku 2011
- roli národního týmu vykonává na základě veřejnoprávní smlouvy s Národním bezpečnostním úřadem
- tým je provozován pro stát bezúplatně a jeho činnost je financována sdružením CZ.NIC a grantovými projekty

Jak se mění úloha národního týmu CSIRT.CZ v průběhu posledních let?

Úloha národního týmu se v prostředí České republiky za uplynulé roky výrazně měnila. Základní úlohou měl být tzv. last resort. To znamená, že tým měl řešit primárně případy a incidenty, které se nevyřešily domluvou mezi dvěma provozovateli síťové infrastruktury: té, od níž útok přichází, a té, která je cílem útoku.

Pokud se provozovatelé síťové infrastruktury nedomluví nebo na výzvy nereagují, do řešení by se měl zapojit právě národní tým, který plní úlohu „poslední záchrany“. Zpravidla minimálně jeden z dotčených provozovatelů musí mít působnost v České republice. Tato základní úloha je přirozeně doplňována dalšími úkoly, které národní tým na sebe bere. Na národní tým se obracejí často různé výzkumné a projektové týmy pracující s honeypoty – hledají a testují nové zranitelnosti nebo pracují na plošném odhalování nových botnetů. Pro ně je výrazně jednodušší a efektivnější zasílat seznamy škodlivých nebo nakažených IP adres přímo národnímu týmu, který se postará o jejich distribuci do koncových sítí. Jedná se o seznamy adres, na nichž se problém již vyskytl, a jde tehdy o reaktivní činnost. Nebo jde o seznamy adres, které hostují něco zranitelného či byly detekovány honeypotem, a tehdy jde spíše o proaktivní činnost.

Seznamy adres jsou zasílané národnímu CSIRTu ze dvou důvodů:

- Národní tým často nejlépe zná infrastrukturu v daném státě, a umí tak rozeslat hlášení do koncových sítí rychleji a efektivněji.
- Předpokládá se, že národní tým má v daném státě určitou autoritu a jeho hlášení mají relevantní váhu. Minimálně by e-maily od národního týmu neměly padat do spamu, což se může stát v případě hromadných hlášení ze zahraničí.

Výhodou národních týmů je, že bez ohledu na stát jsou jejich aktivity velice podobné a do značné míry je stejná i jejich agenda. Právě proto se systémy, které CSIRT týmy vytvářejí, zveřejňují pod open source licencí a jejich využití se umožňuje také dalším týmům. Zveřejnění pod open source licencí pak umožňuje týmům poupravit si systém podle vlastních požadavků, protože každý tým má nějaké speciální požadavky.

Další změnou, kterou jsme v uplynulých letech zaznamenali nejen u národních, ale také u různých jiných týmů, je řada placených nebo neplacených zdrojů dat, jež začaly týmy o své síti odebírat. Vzniká řada projektů vedená CSIRT týmy, které mají za úkol velké množství dat v co nejefektivnější formě sbírat a zpracovávat. Vzhledem k tomu, že každý používá jinou metodiku sběru dat, ideální je kombinovat několik různých zdrojů dat, tzv. feedů. Nekomerční CSIRT týmy nebo projekty zveřejňují zdroje bezplatně, a to buď na vyžádání dle konstituence (většinou ASN), nebo veřejně. Existují také placené zdroje dat. Vzhledem k prve zmíněné metodice sběru dat je však porovnávání placených a neplacených zdrojů dat velice náročné.

Na podobném systému pracuje také český národní tým CSIRT.CZ (jeho úkoly popisuje Box 1), který si z několika jiných systémů na sběr a zpracování většího počtu zdrojů dat vytvořil vlastní systém, který vyhovuje konkrétním požadavkům. Tento systém nazvaný PROKI umožňuje sledování několika desítek různých zdrojů dat, což týmu CSIRT.CZ umožňuje jejich hlubší analýzu. Tento proaktivní přístup ke sběru dat umožňuje provádět hlubší analýzy incidentů a poskytuje více informací o jednotlivých koncových sítích a incidentech, které se nejčastěji vyskytují. Např. můžeme sledovat, zda se problémy na konkrétní síti nebo adrese neopakují. Zároveň to řeší problém různých formátů datových výstupů, které ztěžují strojovou zpracovatelnost a do značné míry práci týmu. Po ukončení testovací části, která již ve spolupráci vybranými poskytovateli běží, by měl být schopný tým CSIRT.CZ zasílat souhrnné zprávy o škodlivých aktivitách přímo koncovým sítím.

CSIRT týmy, které dostávají větší množství informací o škodlivých aktivitách ve své konstituenci, musí příchozí reporty zpracovávat poloautomaticky s pomocí vlastních skriptů. To se týče hlavně týmů, pod které spadá několik desítek či stovek různých sítí. Např. národní, vládní či akademické týmy. Tento způsob práce do značné míry ztěžuje různost datových reportů. Nejde přitom jen o různost formátů, ale také o různost zápisu či názvu polí. I když vzniklo již několik iniciativ, které se snažili tento systém zápisu a výměny dat sjednotit, podařilo se to pouze částečně. Jedna z úspěšnějších iniciativ je popsaná v boxu č. 2.

Celkově se incidenty, které jsou bezpečnostním týmům zasílány, dají rozdělit do dvou kategorií. Některé problémy, které bezpečnostní týmy pravidelně řeší, mají spíše přetrvávající charakter nebo se ve významné míře pravidelně opakují. Jde např. o phishing způsobený nedostatečným zabezpečením webových stránek nebo nakažené stroje, které jsou součástí botnetů a podílejí se na DDoS útocích. Problémy řeší pravidelně i národní bezpečnostní tým. Těmto aktivitám je možné alespoň z části zamezit osvětou a vzděláváním koncových uživatelů a správců systémů. To může být realizováno různými způsoby – od přednášek přes publikování různých článků až po pořádání školení. Cílem je předejít incidentům všude tam, kde je to možné.

Na druhou straně se totiž často objevují nové zranitelnosti a útoky (zero-day vulnerability/attack – viz Box 3), kterým je téměř nemožné se vyhnout. V tomto případě lze využít jen reaktivní přístup. Pokud se na danou zranitelnost dělají nějaké plošné scany sítí, národnímu CSIRT týmu jsou často zasílány seznamy IP adres, na kterých se zranitelné stroje nacházejí. Ten pak přeposílá informace o nakažených strojích do koncových sítí. Národní CSIRT nemá na rozdíl od interního týmu výkonné pravomoci, takže nemá přístup k daným strojům, a tudíž sám danou situaci nemůže napravit.

Co je STIX (Structured Threat Information eXpression) **BOX 2**

- jedna z iniciativ, jejímž cílem je standardizace způsobu označování hrozeb
- jde o strukturovaný jazyk pro popis hrozeb takovým způsobem, aby bylo jejich sdílení, ukládání či analýza možné v co nejkonzistentnější míře bez ohledu na zdroj dat

Co je Zero-day zranitelnost (útok) **BOX 3**

- využívá zranitelnost, pro kterou zatím neexistuje obrana, např. v podobě záplaty software
- délka ohrožení je závislá na dvou proměnných: času, který je potřebný pro vytvoření záplaty, a schopnosti záplatu implementovat do zranitelných systémů

Závěr

Způsob práce a fungování bezpečnostních týmů typu CSIRT se za posledních pár let výrazně zlepšil. Co bylo ještě nedávno možné dělat ručně, je hlavně pro týmy spravující větší sítě, národní a vládní týmy dnes již nemožné; velkou část práce s incidenty bylo nutno automatizovat. Zásadním způsobem narostlo v posledních letech množství dat, která jsou týmům zasílána nebo která týmy aktivně sbírají o svých sítích.

Změnilo se také vnímání kybernetické bezpečnosti nejen v soukromém sektoru, ale také z pohledu státu. Každý stát Evropské unie má dnes vypracovaný nějaký právní předpis ohledně kybernetické bezpečnosti nebo na něm v důsledku schválení Směrnice o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii (NIS směrnice[6]) pracuje. Stále více CSIRT týmů dnes působí nebo začíná působit jako nezbytná součást řízení větší sítě či státních systémů. Vzhledem k nárůstu ceny aktiv informačních systémů to je však nezbytný a přirozený krok.

Zuzana Duračinská
? ? ? @ ? ? ?

Zuzana Duračinská

Bezpečnostní analytik sdružení CZ.NIC, které provozuje Národní bezpečnostní tým CSIRT.CZ

[3] Směrnice o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v EU byla schválena 6. července 2016 Evropským parlamentem. Jde o vůbec první dokument na úrovni EU, který se snaží zasáhnout do řízení kybernetické bezpečnosti na celoevropské i národní úrovni. Směrnice vstoupila do platnosti v srpnu 2016. Od srpna běží členským státům lhůta 21 měsíců na implementaci směrnice do národních legislativ.