Computer, květen 2011

Týmová práce pro zajištění bezpečnosti komunikačních sítí

Problematiku bezpečnosti sítí a jejich služeb s důrazem na oblast řešení bezpečnostních incidentů řeší profesionální týmy CSIRT (Computer Security Incident Response Team), případně CERT (Computer Emergency Response Team).

Uplynulá dekáda znamenala překotný rozvoj internetu a také jeho masivní komercionalizaci. Zvýšil se počet služeb dostupných jeho prostřednictvím a především počet provozovaných kritických aplikací, a to jak ve sféře komerční (elektronické bankovnictví, elektronické obchody), tak ve sféře státní (systémy bezpečnostních složek, informační servis státní správy a samosprávy). S tím souvisí nejen zvyšující se počet bezpečnostních incidentů, ale i nárůst jejich závažnosti a negativního dopadu na chod firem a soukromý život uživatelů. Proto je nutné, aby na možnost narušení bezpečnosti sítě a služeb na ní provozovaných byli jejich správci a uživatelé připraveni a měli k dispozici funkční struktury, efektivní postupy, pravidla a technické prostředky vedoucí k co nejrychlejšímu odstranění problémů při minimalizaci škod.

První CERT tým vznikl v roce 1988 na Carnegie Mellon University (CMU) jako reakce na jeden z prvních vážných bezpečnostních problémů tehdejšího internetu, tzv. Morissův červ. Nejcennějším výsledkem práce tohoto týmu, který byl zřízen především za účelem nalezení účinné obrany proti jedinému (byť pustošivému) incidentu, bylo poznání, že nejdůležitější je být na možnost narušení bezpečnosti předem připraven a v okamžiku problému spustit předem definovaný a vyzkoušený záchranný plán, a ne teprve začít zkoumat, co je nutné udělat. Výsledek práce prvního ad hoc CERTu na CMU odstartoval éru budování světové infrastruktury týmů tohoto typu. Carnegie Mellon University si zkratku CERT zaregistrovala jako ochrannou známku, a ač se jejímu užití ostatními organizacemi v tomto kontextu nebrání, právě toto bylo příčinou vzniku a zavedení druhého pojmu CSIRT, přičemž obě zkratky vyjadřují totéž.

CERT/CSIRT dané sítě (organizace) tedy představuje záchytný bod, na který je možné se obrátit se zjištěným bezpečnostním problémem (nebo jen podezřením), který by tým měl prozkoumat a podle možností zjednat nápravu. Existence aspoň jednoho oficiálního CERT/CSIRT týmu je žádoucí v každé provozované síti, obzvláště pak v těch velkých (tranzitní, regionální, univerzitní, rozsáhlé koncové apod.), tzn. na úrovni velkých ISP, ale také v bankách nebo u poskytovatelů služeb. Významnou a specifickou roli mají zastřešující vrcholové týmy - tzv. národní nebo vládní, o kterých bude řeč později. Globálně lze pak na

existující CERT/CSIRT týmy nahlížet jako na infrastrukturu, která řeší bezpečnostní problémy Internetu.

Vznik a fungování CSIRT týmu

Organizace, která se rozhodne zřídit tým typu CERT/CSIRT, si musí na začátku jasně a srozumitelně definovat, čeho chce ustavením týmu dosáhnout a jakou roli od nově zřizovaného týmu chce, tzn. definovat jeho pole působnosti a provozované služby.

Aby se tým mohl oficiálně nazývat týmem typu CERT/CSIRT, je potřeba, aby nabízel především službu řešení nebo koordinace řešení bezpečnostních incidentů v rámci definovaného pole působnosti, a tím naplnil slovo „response“ použité ve zkratkách CERT a CSIRT - reakce na bezpečnostní incident.

Polem působnosti je obvykle myšlena oblast kyberprostoru, ve které je tým způsobilý konat a nad kterou má příslušné pravomoci a odpovědnosti definované zřizovatelem. Na základě deklarovaného pole působnosti je potom tým kontaktován např. napadenými a řeší problémy ve sféře svého vlivu. Pole působnosti týmu může být definováno jako konkrétní síť/sítě, autonomní systém(y), jmenná doména/domény.

Na úplném počátku při vytváření týmu typu CERT/CSIRT ale stojí také vybudování jeho zázemí - technické, administrativní a organizační - bez kterého nemůže efektivně fungovat žádný tým.

Technickým zázemím se myslí například nástroj pro efektivní správu hlášení bezpečnostních incidentů, který umožní sledovat celý jeho životní cyklus - kdo se v kterých fázích incidentem zabýval, proč, jak postupoval, koho požádal o spolupráci apod. Pro tuto oblast týmy obvykle používají různé ticketovací systémy, např. RTIR (Request Tracker for Incident Response), OTRS (Open Source Ticket Request System). Dalšími důležitými pomocníky na poli technických nástrojů jsou různé systémy IDS (Intrusion Detection System), systémy pro bezpečnostní audity, forenzní analýzy, sledování provozu sítě (netflow) apod.

Zázemí administrativně-organizační představuje právě onu „připravenost“ na problém, tzn. definování základních pravidel pro chod týmu tak, aby každý člen týmu znal svou roli, povinnosti a zodpovědnost, politiku postupu řešení bezpečnostních incidentů, pravidla pro komunikaci a spolupráci apod. Základem v této oblasti je obecně dobře zvládnutý tzv. incident management, kterým se ovšem v tomto článku

dopodrobna zabývat nebudu.

Spolupráce CERT/CSIRT infrastruktury

V současnosti neexistuje oficiální hierarchie CERT týmů. Tyto týmy vznikaly a vznikají dobrovolně a v samotném jejich zájmu je navzájem efektivně komunikovat, vyměňovat si důležité informace a poznatky a spolupracovat. Sdružují se proto v mezinárodních organizacích. V současnosti nejznámější a nejaktivnější organizace, které se touto problematikou zabývají, jsou následující: TERENA - The Trans-European Research and Education Networking Association, www.terena.org.

FIRST - Forum for Incident Response and Security Teams, www.first.org.
ENISA - European Network and Information Security Agency, www.enisa. europa.eu.

Všechny tři výše zmíněné organizace představují platformu, která umožňuje pravidelná setkávání, výměnu zkušeností a definování základních pravidel spolupráce a komunikace mezi světovými CERT/ CSIRT týmy.

Světovou infrastrukturu CERT/CSIRT týmů v současné době představuje cca 250 týmů, které jsou buď členy organizace FIRST nebo spolupracují s evropsky působícími organizacemi TERENA a ENISA.

Národní a vládní týmy CERT/CSIRT

Jak už bylo řečeno, speciální úlohu v této bezpečnostní infrastruktuře mají týmy národní a vládní.

Národní CERT/CSIRT týmy v prostředí svých zemí obvykle plní především roli národního PoC (Point of Contact) pro sdílení informací s ostatními světovými CERT/ CSIRT týmy a se subjekty a organizacemi země působnosti. Na základě znalostí světové infrastruktury a prostředí dokáže národní tým efektivně nastavit a zprostředkovat komunikační kanály mezi zainteresovanými subjekty, například v okamžiku řešení vážného, často plošného, bezpečnostního incidentu.

Z pohledu stále zdůrazňované služby řešení bezpečnostních incidentů pak národní tým funguje jako tzv. tým posledního útočiště (last resort). To znamená, že tomuto týmu mohou být oznamovány bezpečnostní incidenty, které mají původ v sítích provozovaných v dané zemi, a to v okamžiku, kdy tým (osoba) zodpovědný za síť (zařízení), která je zdrojem problému, problém neřeší, nebo vůbec nereaguje, odmítá

řešit nebo takový kontakt není možné nalézt (nebo není platný). Plní roli poslední možné instance v případě přetrvávajícího problému, od které je možné očekávat pomoc.

Je nutné zdůraznit, že národní CERT/ CSIRT není primárně určen k fyzickému řešení konkrétních zaznamenaných problémů (incidentů). V případě vzniku incidentu je vždy žádoucí, aby byl co nejrychleji kontaktován přímo tým konkrétně zodpovědný za danou síť, který má možnost zasáhnout (třeba i fyzicky a provést odpojení problémové sítě nebo zařízení), a případně následně národní tým až v případě přetrvávání problému v rámci eskalace jeho řešení. Dalším momentem, kde má národní CERT/ CSIRT v této oblasti uplatnění, mohou být útoky většího rozsahu, kdy je potřeba rychlé vyhodnocení situace, koordinace spolupráce mnoha subjektů a varování dalších možných potenciálních cílů.

Další důležitou rolí národního CERT/ CSIRT, kterou pracoviště tohoto typu má plnit, je role fóra pro výměnu zkušeností a navázání bližší spolupráce mezi subjekty typu CERT/CSIRT týmy, poskytovatelé připojení, poskytovatelé obsahu, banky, bezpečnostní složky státu apod. a pomoc organizacím ve vybudování jejich vlastních CERT/CSIRT týmů.

V neposlední řadě se národní CERT/ CSIRT obvykle věnuje šíření osvěty a vzdělanosti v oblasti počítačové bezpečnosti směrem k uživatelům (občanům). Do této oblasti patří pořádání vzdělávacích akcí, informování uživatelů např. o aktuálních hrozbách prostřednictvím médií, webových stránek nebo elektronické pošty. Obecně může národní tým CERT/CSIRT nabízet celou řadu reaktivních i proaktivních služeb v oblasti bezpečnosti, záleží především na jeho provozovateli.

Týmy označované jako vládní jsou obvykle určené pro dohled nad sítěmi státní správy, samosprávy a tzv. kritické infrastruktury země. V některých zemích, za všechny jmenujme například Finsko, jsou týmy tohoto typu zřízené přímo státem na základě zákona, který definuje jejich pravomoc, pole působnosti a zodpovědnost.

V mnoha zemích plní vládní týmy zároveň roli národního týmu. V zemích, kde není ustaven ani národní ani vládní tým, ale existuje zde CERT/CSIRT tým například v prostředí významného ISP nebo v akademickém sektoru, je tento tým světovou infrastrukturou chápán jako de facto národní a tuto roli národního týmu plní. Tuto situaci lze velmi dobře ilustrovat například na známých útocích na Gruzii, kde se role hlavního

koordinátora obrany ujal tým CERT-GE provozovaný organizací GRENA (Georgian Research and Educational Networking Association), jediný v té době existující tým typu CERT.

Situace v České republice

V České republice existují v současné době čtyři konstituované a světovou komunitou oficiálně uznané CERT/CSIRT týmy:

- CESNET-CERTS provozovaný sdružením CESNET, z.s.p.o.
- CZNIC-CSIRT provozovaný sdružením CZ.NIC, z.s.p.o.
- CSIRT-MU provozovaný Masarykovou Univerzitou Brno
- CSIRT. CZ vytvořený v rámci grantu MVČR

Bezpečnostní tým CESNET-CERTS (http://csirt.cesnet.cz/) je zodpovědný za řešení bezpečnostních incidentů v síti národního výzkumu a vzdělávání CESNET2. Uživatelé sítě CESNET2, což jsou především studenti a zaměstnanci českých univerzit a Akademie věd, spadají do pole působnosti tohoto týmu a mohou mu hlásit zjištěné bezpečnostní incidenty. Tým CESNETCERTS je v síti CESNET2 (autonomní systému AS2852) způsobilý konat a řešit bezpečnostní incidenty přímým zásahem.

Pracoviště CSIRT. CZ (www.csirt.cz) vzniklo v rámci plnění grantu Ministerstva vnitra České republiky „Problematika kybernetických hrozeb z hlediska bezpečnostních zájmů České republiky“ (identifikační kód projektu je VD20072010B013). Toto pracoviště je označováno jako modelové a bylo vybudováno za účelem ověření stavu bezpečnostní infrastruktury v ČR a ověření realizovatelnosti distribuované hierarchie pro systematické plošné řešení bezpečnostní problematiky v počítačových sítích ČR prostřednictvím CSIRT týmů. Provoz tohoto týmu byl spuštěn 3. dubna 2008 a v květnu téhož roku byl přijat evropskou infrastrukturou CERT/CSIRT týmů jako pracoviště typu CSIRT s rolí „last resort“ pro Českou republiku.

Další funkční tým typu CSIRT je provozován také Ministerstvem obrany ČR - jedná se o vojenský CSIRT tým určený pro spolupráci s obdobnými týmy v rámci členských zemí NATO.

Je pravděpodobné, že ačkoliv v rámci dalších komerčních organizací nejsou CERT/CSIRT týmy oficiálně ustaveny, existují zde oddělení nebo osoby, které se bezpečností sítí a služeb reálně zabývají a roli

CERT/CSIRT týmu de facto plní. Tato oddělení a týmy nejsou ale napojeny na světovou bezpečnostní infrastrukturu CERT/CSIRT týmů a nezapojují se do spolupráce a výměny informací.

Český národní tým

Česká republika se o vybudování národního nebo vládního pracoviště typu CERT/ CSIRT snaží již několik let. Za první dobrý krok lze v tomto směru považovat vybudování již zmíněného modelového pracoviště CSIRT. CZ, které vzniklo v rámci vědecko-výzkumného grantu MV ČR. CSIRT. CZ položilo základy pro další rozvoj vrcholové úrovně CERT/CSIRT infrastruktury v ČR, a to především v oblasti spolupráce lokální a mezinárodní, protože žádný CERT/CSIRT, obzvláště ne národní nebo vládní, nemůže pracovat izolovaně.

V únoru tohoto roku bylo při Ministerstvu vnitra České republiky zřízeno Oddělení kybernetické bezpečnosti, které má kromě mnoha jiných povinností za úkol zajišťovat provoz vládního pracoviště CSIRT. O dalším vývoji tedy rozhodnou následující měsíce. Nezbývá než doufat, že se Česká republika již brzy připojí k těm zemím EU, které mají oficiálně zřízen funkční národní nebo vládní CERT/CSIRT.

Autor:
Andrea Kropáčová, CZ.NIC, z.s.p.o.