Andrea Kropáčová

V roce 2004 sestavila první světovou komunitou oficiálně uznaný tým typu CSIRT v České republice. Zkušenosti z vybudování tohoto akademického týmu uplatnila v letech 2007 až 2010 při budování pracoviště CSIRT.CZ až po jeho přerod v Národní CSIRT České republiky zůstala v roli representativa.

S rostoucí počítačovou gramotností neroste schopnost uvědomovat si rizika

Prvního ledna nabyl účinnosti zákon o kybernetické bezpečnosti. Co to pro národní CSIRT fakticky znamená?

V první fázi, tzn. v průběhu ledna, se jedná o sběr kontaktních informací od povinných osob definovaných § 3 zákona o kybernetické bezpečnosti. K tomu jsme v závěru roku 2014 zřídili na stránkách CSIRT.CZ (www.csirt.cz) formulář pro hlášení kontaktních informací. Subjekty podřazené pod písmena a) a b) § 3 zákona o kybernetické bezpečnosti tak mají možnost splnit svou povinnost a ohlásit kontaktní údaje národnímu CSIRT ČR touto cestou. Od 1. ledna 2016 budou mít některé subjekty povinnost hlásit národnímu CSIRTu zjištěné kybernetické bezpečnostní incidenty.

Probíhá už nějaké reportování incidentů?

Reportování incidentů probíhá a probíhalo vždy. Je to jedna ze základních činností infrastruktury bezpečnostních týmů. Reportování se děje dobrovolně, na denní bázi a s cílem eliminovat problém, informovat se o probíhajících útocích, nových zranitelnostech atd. Směrem k národnímu CSIRTu se reportují především takové problémy, u kterých je žádoucí, aby národní CSIRT ČR nějakým způsobem jako „poslední instance“ zasáhl. Tedy tehdy, kdy už se všechny ostatní cesty řešení problému vyčerpaly, nebo jedná-li se o problém, který má širší dosah a může zasáhnout velké spektrum uživatelů českého internetu a je potřeba, aby někdo koordinoval pomoc a vhodným způsobem distribuoval informace směrem k uživatelům (potenciálním obětem) a správcům, kteří mají možnost uživatelům pomoci. Samozřejmě jsou ještě další důvody, kdy a proč poslat report národnímu CSIRT týmu, ale to si nechme do samostatného článku věnovanému problematice reportování.

„Dnešní výpočetní výkon umožňuje využít potenciál internetu, analyzovat data, která uživatelé o sobě zveřejňují (nejčastěji prostřednictvím sociálních sítí), a připravit útoky uživateli na míru.“

Takovým pěkným příkladem role týmu typu národní CSIRT byly třeba loňské phishingové kampaně. Uživatelům chodily poplašné zprávy s informací o dluhu, že je na ně uvalena exekuce apod. Zde je právě velký prostor pro činnost národního CSIRTu, který se na problém podívá globálně, zveřejní na svých stránkách varování a domluví s provozovateli sítí a služeb vhodnou formu základní obrany a péče o uživatele tak, aby se jich nachytalo co nejméně, případně aby rychle došlo k jejich identifikaci a nápravě škod.

Dá se na tomto případě ukázat, jakou konkrétní reakci od vás mohou čekat ti, kdo vám reportují?

V případě výskytu další podobné masivní phishingové kampaně zasahující velké množství uživatelů je žádoucí, aby se o problému co nejrychleji dozvěděl národní CSIRT. Např. od správce, kterému problém nahlásil jeho uživatel, nebo od jiného bezpečnostního týmu. Tak to i obvykle probíhá. Infrastruktura bezpečnostních týmů ví, jaké problémy a proč je žádoucí hlásit, takže informace proudí. Phishingové kampaně mají navíc takový charakter, že se to národní CSIRT dozví z „vlastních zdrojů“, protože cílem jsou i zaměstnanci sdružení, takže informace probublá na správné místo poměrně rychle.

Když se o problému tohoto typu relevantní osoby dozvědí včas, existují způsoby, s jejichž pomocí lze ochránit uživatele, k nimž poplašná zpráva ještě nedoputovala nebo se k ní nedostali, a samozřejmě i ty, kteří už se kompromitovali. Třeba se podaří deaktivovat ono závadné URL, takže uživatel se nemá jak nakazit, protože zdroj nákazy v době přístupu už není aktivní, apod. Z provozních údajů se zase dají identifikovat uživatelé, kteří se již nakazili, a je možné jim pomoci.

Když se mi tedy stane, že dostanu takový e-mail, mám vyplnit váš formulář hlášení, i když jsem běžný uživatel, fyzická osoba?

Ano, pokud jste si jistý, že se jedná o podvodný mail, řekněte to nám nebo správci, se kterým běžně spolupracujete. A samozřejmě podle možností varujte své okolí.

Když se podíváte zpátky na zakládání CSIRT týmu, co je důležité pro to, aby začal správně fungovat?

Existuje mnoho dokumentů, návodů a postupů, které říkají, jak CSIRT tým

vybudovat. Na začátku je nejdůležitější dát dohromady vhodné lidi, členy bezpečnostního týmu. Osobně si myslím, že minimem pro založení CSIRT týmu jsou tři osoby, aby od počátku bylo možné budovat týmovou spolupráci a byla zajištěna zastupitelnost. Členové bezpečnostního týmu by měli být odborně dostatečně na výši, měli by mít globální náhled a vědomosti o tom, jak funguje internet, sítě, počítače, služby a co je možné čekat od uživatelů. Důležitá je také mentální kompatibilita členů týmu, vzájemná důvěra a komunikační schopnosti. Co má plnit bezpečnostní tým typu CSIRT, je poměrně jasně definované. Existuje také řada dokumentů typu best practices apod. Samotní aktéři tedy od začátku vědí, co mají dělat.

Aby se bezpečnostní tým mohl vůbec nazývat CSIRT týmem, musí naplnit základní povinnost, která je zanesena do samotného názvu CSIRT – Computer Incident Security Response Team. To nejpodstatnější, co každý bezpečnostní tým typu CSIRT musí dělat, je naplňovat myšlenku response, tzn. re-

agovat na zjištěnou hrozbu, nahlášený bezpečnostní incident a vědět, co dělat. Proto je zapotřebí, aby se členové týmu orientovali v principech fungování internetu, analyzovali, co je jim vlastně reportováno, a dokázali si za tím něco představit. Protože u reportu je potřeba nejdříve identifikovat, čeho se problém týká, koho se může týkat a v čem problém spočívá. Velmi důležité při zakládání CSIRT týmu je také jeho ukotvení v organizaci. Proto je nutné, aby od počátku budování týmu probíhal dialog s managementem (zřizovatelem) a dobře se vyjasnila pozice týmu v organizaci, rozsah jeho působnosti, zodpovědnost a pravomoc. Tým se nesmí ocitnout v situaci, kdy by byl nucen jednat „na vlastní pěst" a přejímat zodpovědnost za rozhodnutí, která má učinit někdo jiný.

Mluvili jsme o odbornosti a o začlenění do organizační struktury. Je tam ještě něco, na co je dobré si při budování týmu dávat pozor?

Celou dobu je potřeba dbát na to, aby byl tým budovaný transparentním způsobem, tj. aby bylo jasné, kdo jej zřizuje, provozuje, jaké je jeho pole působnosti, jaké poskytuje služby atd. Pokud se bezpečnostní tým chce stát oficiálním CSIRT týmem, je jeho budování ve finále završeno procesem, kdy se napojuje na světovou infrastrukturu CERT/CSIRT týmů. Tým se světové komunitě představí a požádá o zapojení do infrastruktury. To se děje buď prostřednictvím získání členství v organizaci FIRST[1], nebo žádostí o přiznání statusu „listed" u úřadu Trusted Introducer[2].

[1] www.first.org
[2] www.trusted-introducer.org

FIRST i Trusted Introducer si informace sdělené týmem ověří a následně vyzvou již etablované týmy, aby nový tým podpořily nebo vznesly námitky proti jeho připojení do infrastruktury. Pokud se v komunitě najde dostatečná podpora a nikdo nevznese námitky (např. z důvodu nejasné působnosti týmu), může být tým napojen na světovou infrastrukturu a ocitne se v databázích existujících CSIRT týmů.

Jak se vám spolupracuje s vládním CSIRTem?

Dobře. Komunikace je nastavená, výměna informací probíhá, spolupracujeme na rozvoji obou vrcholových týmů, zúčastňujeme se společně cvičení, organizujeme národní cvičení. Těch činností, kde se oba týmy potkávají, je opravdu hodně. Vládní CSIRT je o něco mladší než národní CSIRT. Aktuálně se soustředí na svou hlavní sféru působnosti, což je státní správa a kritická infrastruktura státu. Snažíme se vládnímu CERTu pomoci know-how, svými zkušenostmi a také informacemi, které se k nám dostanou právě díky reportování bezpečnostních incidentů a z bezpečnostní komunity a týkají se státní správy.

„Když je zařízení dostupné prostřednictvím internetu, je možné jej na dálku ovládat servisovat, vyměnit firmware, aktualizovat... To je docela lákavé. Ale ruku v ruce s tím jde i větší zranitelnost."

Když se ohlédnete zpět, vidíte nějaké změny v chování uživatelů? Jsou obezřetnější než před lety?

S každou novou generací uživatelů skutečně roste gramotnost využívání výpočetní techniky. Ta je dnes velmi dobrá. Ale obávám se, že se tím nezvyšuje schopnost uvědomovat si rizika a čelit jim.

Navíc jsou metody útoků sofistikovanější. Dnešní výpočetní výkon umožňuje využít potenciál internetu, analyzovat data, která uživatelé o sobě do prostředí internetu zveřejňují (nejčastěji prostřednictvím sociálních sítí), a připravit útoky uživateli na míru. Hovořila jsem s řadou lidí, kteří se nechali nachytat na zmiňovaný podvodný e-mail s informací o dluhu (phishingový útok). Říkali: „Jak můžu vědět, jestli třeba děti opravdu někde nenadělaly nějaký dluh, bály se to přiznat, pak na to zapomněly a dluh narostl do takových rozměrů, že se toho ujala exekuční firma?" Takže když přijde e-mail, který je gramaticky takřka dokonalý, má všechny náležitosti toho, jak by oficiální oznámení mělo vypadat (oslovení, podpis, použití věrohodných nebo existujících jmen např. exekutorů), uživatel má silnou motivaci kliknout na uvedené URL nebo otevřít přiložený soubor. Z obsahu souboru se nic kloudného nedozví, buď hledá další informace a obsah si ověří, nebo se uklidní, e-mail smaže a na celou záležitost zapomene. Ale už v okamžiku, kdy ten soubor rozbaloval, se mu v počítači mohl uhnízdit malware. A o to šlo – nasadit uživateli do počítače malware, zapojit ho do botnetu atp. Malware pak může pozorovat, co uživatel píše na klávesnici, a tyto informace posílat útočníkovi. Nejzajímavější jsou samozřejmě citlivé přístupové údaje, např. do internetbankingu.

Je otázkou, jestli člověka napadne, že šlo vlastně jen o transportní mechanismus něčeho nekalého do jeho počítače, a zda se zamyslí nad tím, proč to někdo udělal a jaká rizika by to po něj mohlo skýtat. Osobně mám často lepší pocit ze starších uživatelů, kteří k výpočetní technice přistupují s větším respektem a obezřetností. Ne jako mladí, kteří internetbanking ovládají z mobilu, tabletu, internetové kavárny a hojně využívají funkci „zapamatovat heslo".

Kdo by měl být za informační bezpečnost odpovědný? Někdo říká, že stát by se měl starat o bezpečnost v kyberprostoru podobně jako

o bezpečnost na ulicích. Někdo by zase ponechal odpovědnost na uživatelích. Je možné stanovit nějaké optimální rozložení odpovědnosti?

Každý musí přiložit ruku k dílu. To máte stejné jako u automobilové dopravy. Je tu nějaká silniční infrastruktura a nějací uživatelé, kteří si koupí auto a usednou za volant. Co dělá společnost, aby uchránila životy svých občanů, jejich majetek a celkově zajistila, že dopravní infrastruktura bude funkční a bezpečná? Silnice jsou dobře spravované, značené, máme svodidla, osvětlení, omezení rychlosti, systémy varující před námrazou atp.

Jenže to nestačí. Další vrstvou jsou řidiči. Každý člověk, který má usednout za volant, musí projít školením, prokázat schopnost auto ovládat a znalost pravidel silničního provozu. Ve finále je pak samozřejmě na něm, jak tohle všechno uplatní v praxi. Ale právě na automobilové dopravě je krásně vidět, že jak společnost nebo stát, tak uživatel musí udělat něco pro to, aby to fungovalo a nedocházelo k haváriím.

V kybernetickém prostoru je to velmi podobné. Organizace, která provozuje síť, by se měla postarat o to, aby síť byla zabezpečená. To samé by měli udělat programátoři, kteří píšou software. Další díl práce by měli udělat poskytovatelé služeb, svou roli hrají bezpečnostní týmy. Ale ani při všem tomto aparátu si uživatel nemůže říci, že se o jeho bezpečnost někdo kompletně postará a že to není jeho věc. Měl by svým výpočetním prostředkům věnovat potřebnou péči, aktualizovat operační systém, přemýšlet, kam zadává přístupové údaje, zda není něco podezřelého na stránce, na kterou přistupuje. Zase je to podobné jako na silnici. Když vidím, že začíná zácpa, nedupnu na plyn a nezvýším rychlost na 200 km/h, ale přizpůsobím tomu svou jízdu. Prostě gramotné a zodpovědné chování jak za volantem, tak při práci s výpočetními prostředky.

Můžete stručně představit projekt FENIX?

Projekt FENIX vznikl na půdě českého peeringového uzlu, sdružení NIX.CZ, v roce 2013 jako reakce na sérii DDoS útoků, kterým byly v březnu roku 2013 vystaveny webové portály některých významných českých médií, bank a operátorů. Cílem projektu je umožnit v případě DDoS útoku dostupnost internetových služeb v rámci subjektů, které se do této aktivity zapojily a staly se jeho členy. Byl navržen mechanismus, pomocí nějž se část infrastruktury může schovat do jakéhosi „ostrova důvěry“, který zajistí, že uživatelé českého kyberprostoru budou i v případě útoku moci přistupovat k napadené službě. Podrobněji je to vysvětleno na stránkách projektu FENIX (www.fe.nix.cz).

> „Uživatel si nemůže říci, že se o jeho bezpečnost někdo kompletně postará. Měl by svým výpočetním prostředkům věnovat potřebnou péči…přemýšlet, kam zadává přístupové údaje, zda není něco podezřelého na stránce, na kterou přistupuje…“

Představte si, že jste uživatel, přistupujete na nějaké webové stránky a ony v určitý moment přestanou být dostupné, protože proti nim právě probíhá útok typu DDoS. A ten útok je takového charakteru, že operátor ani provozovatel si s ním neumí poradit. Nicméně služba je tak významná, že je žádoucí, aby byla dostupná. Provozovatel tedy využije prostředí vytvořené v rámci projektu FENIX a služba se „přesune do ostrova důvěry“. Tím zajistí, že uživatelé připojující se z českého kyberprostoru se k dané službě dostanou.

Do projektu jsou aktuálně zapojeni významní hráči českého internetu NIX.CZ, CZ.NIC, sdružení CESNET, Seznam.cz, O2 Czech Republic, Casablanca INT, Active24, Dial Telecom, ČD-Telematika, Coolhousing. Projekt je také o tom, jak motivovat provozovatele sítí v ČR, aby se bezpečností zabývali.

Jaké bezpečnostní výzvy nás teprve čekají?

Stále více se mluví o „internetu věcí“. Za pár let např. můžeme mít tak chytré přístroje, že lednička při otevření řekne: „Zkazilo se mléko, kup nové.“ Jenže pak se může objevit poťouchlý hacker, který vám tu ledničku nakazí, a ona pak prohlásí za zkažené všechno uvnitř. Nebo se vypne, protože usoudí, že v ní není nic, co by stálo za chlazení. Zkažené jídlo je jen nepříjemnost, ale jsou tu i takové záležitosti, jako je bezpečnost domů nebo už zmíněná automobilová doprava. Tam se dají vymyslet hodně černé scénáře. Když je zařízení dostupné prostřednictvím internetu, je možné jej na dálku ovládat (třeba zapnout topení v rekreačním objektu a přijet už do tepla), servisovat, vyměnit firmware, aktualizovat, pokud se našla chyba atd. To je docela lákavé. Ale ruku v ruce s tím jde i větší zranitelnost.

Dokážete si představit, že by mohly přijít útoky tak závažné, že tento vývoj zastaví?

Dokážu. Ale já mám velmi bohatou fantazii :-).

Ptal se Petr Hampl