Reportování bezpečnostních incidentů

Jaké reportovací povinnosti nově ukládá zákon? Jaké informace musí hlášení obsahovat? Jakým nejčastějším chybám se vyhnout?

Tento článek se zabývá problematikou tzv. reportování bezpečnostních incidentů, pro kterou máme krásný český výraz „hlášení“. Nejedná se o nic jiného než o proces, ve kterém někdo někomu hlásí bezpečnostní incident, na který narazil, je jeho obětí, prostředníkem, cílem apod. Hlášení je buď informativní, nebo má formu žádosti o pomoc a má primárně za cíl bezpečnostní incident eliminovat, zastavit nebo alespoň zmírnit probíhající útok, odstranit www stránku se závadným obsahem, najít a opravit nakažený počítač, odhalit členy botnetu nebo jeho řídicí centrum atp.

Proces hlášení a řešení bezpečnostních incidentů není horkou novinkou, probíhá od začátku budování bezpečnostní infrastruktury tvořené CERT/CSIRT[1] týmy, tzn. zhruba od 80. let, kdy na půdě Carnegie Mellon univerzity v USA vznikl první CERT tým. Jedná se o základní operativu každého týmu a jedinou povinnou službu, kterou týmy typu CERT/CSIRT musí poskytovat. Proto také zkratky CERT/CSIRT obsahují slovo response, tzn. reagovat na bezpečnostní incident.

Aby reakce na hlášení bezpečnostního incidentu mohla být rychlá a efektivní, jsou dána základní pravidla, jak by hlášení mělo vypadat, jaké informace by mělo obsahovat, jak a komu by se mělo adresovat a jak by mělo vypadat jeho zpracování na straně příjemce.

Hlášení bezpečnostního incidentu

Musí obsahovat informace, které dostatečně popisují problém a umožní rychle identifikovat, co se děje, kde se to děje, kdo může být problémem dotčen, kdo může problém řešit apod.:

- IP adresu zdroje útoku a cíle útoku, obecně IP adresu problematického stroje. Někdy není možné nebo žádoucí uvést pouze jednu IP adresu, ale je nutné uvést seznam IP adres, adresový blok, URL, či jiný technický identifikátor.
- Měl by být uveden typ incidentu, tzn. informace, jestli se jedná o virus, scan, DoS, DDoS, hacking, phishing, pharming, malware, botnet atp.
- Měl by být uveden datum a čas (včetně časové zóny), kdy k incidentu došlo, kdy byl zjištěn, ideálně co nejpřesnější časový interval, po který problém trval nebo kdy začal atp.
- Hlášení typu scan, DoS, DDoS apod. by mělo obsahovat část logu obsahující záznamy o útoku – časové známky a časovou zónu, zdrojovou a cílovou IP adresu, zdrojový a cílový port, TCP/UDP/ICMP.
- Hlášení incidentů, kde nosičem je e-mail, by mělo obsahovat kompletní původní zprávu včetně e-mailových hlaviček.
- Hlášení phishing nebo pharming musí obsahovat pokud možno i zdroj webové stránky, malware apod.

Hlášení bezpečnostního incidentu se většinou děje prostřednictvím jednoduchého textového e-mailu, v případě nutnosti s přílohou, nebo www formuláře (ve výjimečných a urgentních případech telefonicky). Mělo by obsahovat základní kontaktní informace toho, kdo hlášení posílá, a také pokyn, co se očekává od příjemce. Hlášení může mít podobu informativního sdělení (informuji,

[1] CERT/CSIRT – Computer Emergency Response Team, Computer Security Incident Response Team. Týmy, jejichž primárním účelem je reagovat na zjištěné bezpečnostní incidenty v prostředí počítačových sítí. Seznamy oficiálních CERT/CSIRT týmů najdete na stránkách organizací FIRST (www.first.org) a úřadu Trusted Introducer (www.trusted-introducer.org).

„Hlášení je buď informativní, nebo má formu žádosti o pomoc a má primárně za cíl bezpečnostní incident eliminovat, zastavit nebo alespoň zmírnit probíhající útok…“

že A útočí/útočilo na B) nebo se jedná o závažnější požadavek (A útočí na B, prosíme o intervenci u A a zjednání nápravy). Hodně záleží na dané situaci, závažnosti útoku, schopnosti cíle útoku nasadit efektivní obranu, době hlášení (už je po problému, stále trvá) apod. Je také nutné zdůraznit, že hlášení bezpečnostního incidentu je jen jedním z kroků při zvládání bezpečnostního incidentu na straně poškozeného. Neboli ten, na koho je útočeno, se v první řadě musí postarat o adekvátní obranu, hlášení bezpečnostního incidentu jej neochrání ani problém nevyřeší.

Při reakci na bezpečnostní incident je důležité jednat rychle. Proto je žádoucí, aby hlášení probíhalo co „nejkratší cestou“ do rukou tomu, kdo s problémem může něco udělat, obvykle tedy správci serveru, sítě nebo služby. Klíčovým při rozhodování, kdo je tou osobou (organizací), je technický identifikátor typu IP adresa, síťový blok, doménové jméno, URL, ke kterému se hlášený problém vztahuje. Někdy ale není jednoduché rozpoznat, kdo tou osobou (organizací) je, nebo takový kontakt není možné či jednoduché najít. V tom případě se problém hlásí na úrovni ISP nebo bezpečnostnímu týmu, do jehož pole působnosti problém náleží, a v krajním případě některému z vrcholových bezpečnostních týmů dané země – vládnímu nebo národnímu CERT/CSIRT, od kterého se očekává, že zná infrastrukturu své země tak dobře, aby dokázal problém adresovat. Při rozhodování „komu incident hlásit“ také záleží na konkrétní situaci a závažnosti problému. Incidenty nižší závažnosti je dobré hlásit přímo správci dané služby nebo sítě, incidenty vyšší závažnosti je rozumné nahlásit všem, kteří mohou nějak zakročit. Incidenty s plošným dopadem na mnoho uživatelů, jako např. nechvalně známé podvodné e-mailové kampaně, by měly být adresovány rovnou národnímu týmu apod.

Je nutné zdůraznit, že proces hlášení bezpečnostního incidentu ani proces jeho zpracování a řešení na straně příjemce nejsou procesy „tesané do kamene“, nemusí tudíž probíhat pokaždé stejně. Právě naopak! Hlášení i řešení bezpečnostního incidentu vyžaduje kreativitu, schopnost vidět problém v širších souvislostech, umět hledat a kombinovat informace, mít povědomí o aktuálních hrozbách a zvažovat, jestli se reportovaný problém netýká problému, který se třeba právě probírá v bezpečnostní komunitě, nebo je dokonce medializován. Také je potřeba přemýšlet nad legislativními aspekty, závažností problému, cílovou skupinou a celou řadu dalších záležitostí.

Hlášení bezpečnostních incidentů Národnímu CSIRT ČR

Hlášení bezpečnostního incidentu se CERT/CSIRT týmu posílá, týká-li se daný bezpečnostní incident jeho definovaného pole působnosti. V případě týmů na úrovni organizace (např. ISP, banky, univerzitní sítě) je pole působnosti obvykle definováno jako číslo autonomního systému (AS), jako IP rozsah (např. 193.192.0.0/16) nebo seznam AS či IP rozsahů. Polem působnosti týmů, které jsou označovány jako národní, je definice pole působnosti o něco složitější. Národní týmy obvykle deklarují, že jejich polem působnosti je celá země, tzn. všechny IP rozsahy přidělené do dané země.

Národní CSIRT ČR, tým CSIRT.CZ (http://www.csirt.cz/) provozovaný sdružením CZ.NIC, správcem české národní domény, také deklaruje, že jeho polem působnosti jsou všechny adresové rozsahy přidělené do České republiky a zde provozované. Z hlediska řešení, tzn. reagování na hlášený bezpečnostní incident, je CSIRT.CZ týmem koordinačním. Nemá přímé výkonné pravomoci zasahovat, nemá právo „něco vypnout“, zakázat, filtrovat provoz, není oprávněn zásahy tohoto typu na straně provozovatelů sítí a služeb v České republice nařizovat. Primárním cílem CSIRT.CZ je pomáhat, včas varovat před problémem, podporovat a rozvíjet komunikaci a spolupráci jak na domácí, tak na mezinárodní úrovni.

Národnímu CSIRT týmu ČR jsou a měly by být hlášeny bezpečnostní incidenty především v těchto případech:

- Nelze identifikovat, kdo je za síť/IP adresu (zdroj/cíl útoku) zodpovědný a koho je vhodné kontaktovat se žádostí o nápravu, nebo to není jednoznačné.
- Na hlášení bezpečnostního incidentu nikdo nereaguje nebo kontaktní informace pro danou síť/doménu nejsou funkční, hlášení se vrátilo jako nedoručitelné, problém přetrvává a stěžovatel již vyčerpal všechny možnosti a eskalační procedury, jak problém řešit.
- Jedná se o závažný problém, který vyžaduje rychlou reakci ze strany původce incidentu, a je vhodné varovat

další potenciální oběti. Intervence Národního CSIRT týmu může zafungovat jako silná motivace zabývat se problémem. Dochází tak k jeho rychlejší eliminaci a nápravě.

- Jedná se o problém, který má velký plošný dosah a ohrožuje velké množství uživatelů, např. objevené zranitelnosti (jako byl v roce 2014 problém HeartBleed), phishingové kampaně, www stránky obsahující malware apod.

- Jeden problém se týká více sítí nebo služeb provozovaných v ČR, např. někdo zjistil, že 1 000 www serverů v .cz doméně obsahuje malware. Ten, kdo toto zjistil, by problém mohl nahlásit přímo správcům daných webů, ale znamenalo by to napsat a poslat 1 000 hlášení. Jednodušší je poslat hlášení se seznamem kompromitovaných strojů Národnímu CSIRT ČR, který už má vytvořené mechanismy na kontrolu, zpracování a distribuci hlášení podobného typu.

Výše uvedený výčet je pouze ilustrativní, tým CSIRT.CZ se zabývá každým hlášením, které mu je adresováno, takže uživatelé nemusí mít strach hlášení poslat, ani když si nejsou jistí, jestli problém zapadá do některé z výše uvedených kategorií. Tým CSIRT.CZ reaguje na všechna hlášení, tedy i na hlášení, která se netýkají jeho pole působnosti. Odesilatele hlášení na toto upozorní a případně jej nasměruje na správné místo.

Jak probíhá zpracování hlášení bezpečnostního incidentu

Po přijetí hlášení bezpečnostního incidentu (reportu) probíhá analýza – ověření odesilatele hlášení, obsahu hlášení a identifikace typu incidentu. Dále se určuje závažnost, zjišťuje se rozsah, tzn. v jaké síti (zemi) má původ, cíl, jestli byl zodpovědný administrátor dané sítě informován. Zvažuje se potřeba provést forenzní analýzu a tým samozřejmě bere v potaz, co se od něj očekává – pouze předání na správné místo, odpověď, informování o vyřízení, tlak na provozovatele, aby se problémem zabýval, širší informování veřejnosti atd.

S každým typem incidentu se pracuje jinak a má jinou časovou náročnost. Např. takový probe (sken portů) zabere několik minut. Obvykle stačí identifikovat, koho o problému informovat, hlášení přeposlat a v případě potřeby poradit. Incident typu DoS, DDoS nebo problém vyžadující forenzní analýzu už ale může zabrat několik hodin, v krajním případě dní.

Pojďme si na několika příkladech ukázat, jak takové zpracování hlášení bezpečnostního incidentu v prostředí týmu CSIRT.CZ vypadá a jaké akce může postupně iniciovat (viz. Příklad č. 1 a 2).

Příklad č. 2 ilustruje, že součástí řešení je kromě samotného řešení a informování správců a držitelů zneužitých domén (URL) také informování veřejnosti o problému formou zprávy na webu,

Příklad č. 1

Tým CSIRT.CZ obdržel hlášení informující o existenci botnetu ABC (název botnetu je fiktivní). Součástí hlášení byl seznam IP adres z České republiky, které se k tomuto botnetu připojovaly, je zde tedy vážné podezření, že jsou kompromitovány.

Zpracování hlášení probíhá v následujících krocích:

a) Ověření odesilatele (ne všechna hlášení, která CSIRT.CZ dostává, jsou seriózní).
b) Ověření informací z hlášení (existence botnetu, příslušnosti IP adres do ČR atd.).
c) Zjištění, ve kterých sítích jsou hostované hlášené IP adresy, tzn. dohledání kontaktních adres správců ke každé IP adrese.
d) Seskupení IP adres podle sítí tak, aby správce, z jehož sítě se do botnetu připojovaly tři adresy, obdržel pouze jedno hlášení a ne tři.
e) Rozeslání hlášení bezpečnostního incidentu se žádostí o prověření správcům daných sítí.
f) Komunikace se správci, kterým bylo zasláno hlášení v případě, že požadovali konzultaci.
g) Vyhodnocení stavu, zpracování odpovědí.
h) Informování odesilatele hlášení.
i) Uzavření hlášení, archivace.

Kroky c), d) a e) probíhají poloautomatizovaně.

Příklad č. 2

Tým CSIRT.CZ obdržel hlášení o podvodné e-mailové kampani, která adresáty informovala o převzetí zásilky. E-maily na první pohled evokovaly, že je odeslala společnost DHL. Ve skutečnosti neměly s DHL nic společného, jen v podpisu byl použit název „DHL Logistic-Team“. Následně byl týmu CSIRT.CZ zaslán seznam cca 300 URL, které se v těchto falešných e-mailech postupně objevovaly.

Zpracování hlášení probíhalo v následujících krocích:

a) O podvodné kampani byla veřejnost informována na stránkách www.csirt.cz (na prvním vzorku byla provedena analýza, viz článek http://csirt.cz/page/2760).
b) Ověření odesilatele (ne všechna hlášení, která tým CSIRT.CZ dostává, jsou seriózní).
c) Ověření existence a dostupnosti všech uvedených URL.
d) Stažení všech souborů z uvedených URL.
e) Analýza získaných souborů – probíhá ověření, jestli se vyskytují v antivirových databázích.
f) Předání informací antivirovým společnostem.
g) Postupné informování všech správců infikovaných URL nesoucích tento malware, tzn. zaslání hlášení správcům a držitelům dotčených domén.
h) Některé e-maily se vrátily jako nedoručitelné, protože kontaktní informace u dané domény nebyly funkční. Tuto informaci jsme předali k řešení na patřičné místo a v druhém kroku jsme informovali správce sítě a serveru.
i) S časovým odstupem byla provedena kontrola, jestli daná URL stále existují a jestli se na nich vyskytuje malware (kontrola, jak správci na hlášení reagovali a jestli se problémem zabývali).
j) Komunikace se správci, kterým bylo zasláno hlášení, pokud požadovali konzultaci.
k) Vyhodnocení stavu, zpracování odpovědí.
l) Informování odesilatele hlášení se seznamem oněch 300 závadných URL.
m) Uzavření hlášení, archivace.

spolupráce s antivirovými společnostmi, snaha o nápravu nefunkčních kontaktních údajů domény atd. Některé kroky probíhají paralelně a do řešení je zapojeno více členů týmu.

Není hlášení jako hlášení. Někdy jeho zpracování trvá hodinu, jindy půl dne nebo klidně i celý den. V počátcích budování služeb a zázemí týmu CSIRT.CZ procházely všechny incidenty ručním zpracováním, to ale po čase, kdy počet hlášení tohoto typu narostl, už nebylo možné. CSIRT.CZ proto jako většina jiných CSIRT týmů implementoval mechanismus, který ulehčuje práci s tzv. hromadnými incidenty, které v sobě nesou informace o stovkách nebo tisících problematických IP adres, domén nebo URL. Doba potřebná pro zpracování takového hlášení byla z několika dní zkrácena na pár hodin.

Co by se mělo hlásit Národnímu CSIRT týmu ČR a proč?

Zákon o kybernetické bezpečnosti (dále ZKB), který nabyl účinnosti 1. ledna 2015, ukládá povinnost hlásit kybernetické bezpečnostní incidenty subjektům podřazeným pod písmena b), c), d) a e) § 3 ZKB, přičemž subjekty podřazené pod písmeno b) § 3 ZKB mají povinnost je hlásit Národnímu CERT týmu ČR, ostatní Vládnímu CERT týmu ČR (viz Box 1).

Nicméně kdokoli, tedy i provozovatelé sítí, kteří podle ZKB povinnost hlásit bezpečnostní incidenty nemají, tak může učinit dobrovolně, s cílem sdílet zajímavosti ze světa bezpečnosti, informace o aktuálních hrozbách a zjištěných problémech, a tím se podílet na celkové informovanosti a rozvoji bezpečnostní infrastruktury v České republice a její schopnosti se s problémem vypořádat.

Národnímu CSIRT ČR by se měly hlásit především takové problémy, u kterých je žádoucí, aby Národní CSIRT ČR nějakým způsobem jako „poslední instance“ zasáhl. Tedy tehdy, kdy už se všechny

BOX 1

V České republice v současné době operují dva vrcholové týmy – Národní CERT (od roku 2011) a Vládní CERT (od roku 2013). Vládní CERT, GovCERT.CZ, byl vybudován a je provozován Národním bezpečnostním úřadem, gestorem za oblast kyberbezpečnosti v České republice. Národní CERT, tým CSIRT.CZ, je provozován sdružením CZ.NIC, správcem české národní domény. Polem působnosti (tzn. oblastí, na kterou soustřeďuje svou činnost) Vládního CERT jsou sítě státní správy a kritické infrastruktury České republiky. Polem působnosti Národního CERT jsou sítě provozované v České republice, řečí technickou „všechny IP rozsahy přidělené k užívání do ČR a všechny služby provozované v doméně .cz“. Oba týmy poskytují řadu služeb v oblasti bezpečnosti, od řešení bezpečnostních incidentů přes služby preventivního charakteru typu testování zranitelností až po různá školení, kurzy a publikační činnost.

Zákon o kybernetické bezpečnosti ukládá jak subjektům spadajícím do působnosti ZKB, tak Národnímu i Vládnímu CERT týmu v oblasti zajišťování bezpečnosti sítí a služeb a řešení bezpečnostních incidentů řadu povinností. Povinnosti subjektů podřazených § 3 ZKB se kromě jiného týkají hlášení kontaktních informací, detekování kybernetických bezpečnostních událostí a hlášení kybernetických bezpečnostních incidentů Národnímu nebo Vládnímu CERT. ZKB dělí organizace spadající do jeho působnosti na dvě skupiny. Jedna skupina má povinnosti vůči Národnímu CERT, to jsou subjekty podřazené pod písmena a) a b) § 3 ZKB. Druhá skupina vůči Vládnímu CERT, to jsou subjekty podřazené pod písmena c), d) a e) § 3 ZKB. Hlášení kybernetických bezpečnostních incidentů ze stran provozovatelů sítí a služeb (obecně subjektů spadajících do působnosti ZKB) se tak v ČR děje ve dvou proudech – část informací je adresována Národnímu CERT, část Vládnímu CERT. Oba týmy musí úzce spolupracovat, o hlášených bezpečnostních incidentech spolu komunikovat a vyměňovat si relevantní informace.

Příklad č. 2

Pěkným příkladem problému, který by bylo dobré ohlásit Národnímu CSIRT týmu ČR, jsou nechvalně známé vyděračské e-mailové (phishingové) kampaně, které se začaly objevovat v roce 2014 a cílí na velké množství uživatelů v České republice. Tyto kampaně mají podobný charakter – adresátům e-mailových zpráv přijde informace, že mají neuhrazenou pohledávku nebo dluh, už proti nim bylo zahájeno exekuční řízení, mají poslední možnost nápravy a více informací naleznou v přiloženém souboru. Vystrašený příjemce obvykle přiložený soubor otevře, z obsahu zjistí, že žádný problém popsaný v těle e-mailu nemá, e-mail i soubor smaže, uklidní se a na celou záležitost zapomene. Ovšem e-mail je v tomto případě pouze transportní mechanismus malwaru do počítače uživatele. Otevřením souboru se v počítači zahnízdí a začne škodit. Např. tak, že „poslouchá“, co uživatel na svém počítači píše, a zajímavé informace – typicky přístupové údaje (login, heslo) – posílá útočníkovi, který pak nešťastnému uživateli může zcizit a zneužít jeho elektronickou identitu, třeba tu k internetovému bankovnictví.

Národní CSIRT sice nedokáže ochránit jednotlivé cílové příjemce těchto zpráv nějakým sofistikovaným přímým zásahem, ale když se k němu informace o takové podvodné kampani dostane včas, tzn. někdo provede hlášení bezpečnostního incidentu, má tým CSIRT.CZ několik možností, jak obětem útoku pomoci a varovat další potenciální oběti, ke kterým e-mail ještě nedorazil nebo jej zatím nečetli.

Zpracování hlášení bezpečnostního incidentu typu vyděračského e-mailu s malwarem pak na straně CSIRT.CZ probíhá zhruba v těchto krocích:

a) Je provedena analýza zprávy, tzn. forenzní analýza malwaru, který je prostřednictvím e-mailu transportován do počítače uživatele. Zjišťujeme, jak se malware v nakaženém počítači chová, na co se zaměřuje (např. odposlech hesel), jak s odchycenými informacemi nakládá, jak komunikuje s útočníkem, jak je možné nakažený počítač identifikovat, jak provést nápravu atd.
b) Co nejdříve o hrozbě varujeme prostřednictvím zprávy na webu, blogu nebo ve spolupráci s médii (která často informace z webu www.csirt.cz přebírají). Toto varování pak obsahuje nejen popis, jak nebezpečný e-mail vypadá, ale také co má uživatel, který už e-mail přečetl a přiložený soubor otevřel, prověřit a co má udělat v případě, že se jeho počítač nakazil.
c) Provozovatelům sítí s koncovými uživateli (firemní sítě, školní sítě apod.) můžeme distribuovat informace, jak malware komunikuje s útočníkem; administrátoři sítí tak mají možnost z provozních informací zjistit kompromitované počítače a zjednat nápravu nebo pomocí filtrace síťového provozu zajistit, aby počítače s útočníkem nemohly komunikovat, a tudíž odchycené citlivé informace uživatele nebyly útočníkovi zaslány.
d) Výsledky analýzy malwaru je také možné předat antivirovým společnostem, aby se signatura dostala co nejdříve do databáze anti-ochran apod.
e) Některé phishingové kampaně postupně malware měnily, takže bylo potřeba provést analýzu nového vzorku.
f) Závadný kód instalovaný do počítače oběti postupně díky změnám jmen v DNS měnil cíl komunikace s útočníkem, což bylo potřeba sledovat a postupně na tuto skutečnost reagovat.

ostatní cesty řešení problému vyčerpaly, nebo v případě, že se jedná o problém s širším dosahem, který může zasahovat velké spektrum uživatelů českého internetu. Je potřeba, aby někdo koordinoval pomoc a vhodným způsobem distribuoval informace směrem k uživatelům (potenciálním obětem) a správcům sítí, kteří mají možnost uživatelům pomoci.

Z výše uvedeného je vidět, že na první pohled jednoduchá kauza „hlásím bezpečnostní incident typu vyděračský e-mail" se pro CSIRT.CZ může stát časově velmi náročným problémem. Bezpečnostní incident tohoto typu vyžaduje opětovná přezkoumávání, sledování změn, řešení individuálních dotazů, formulování doporučení, komunikaci s médii apod. Ale je to činnost, která má smysl a uživatelům může pomoci, což je jednou z misí CSIRT.CZ v roli Národního CSIRT týmu ČR.

Vzhledem k tomu, že tým CSIRT.CZ působí jako „national point of contact" také pro zahraničí, má bohaté zkušenosti s řešením incidentů, které mají tzv. přeshraniční charakter, a tudíž vyžadují spolupráci a komunikaci i s jinými bezpečnostními týmy mimo Českou republiku. Pokud tedy uživatel bude mít problém s řešením incidentu, který přesahuje hranice České republiky, CSIRT.CZ se pokusí incident vyřešit ve spolupráci s jinými CERT/CSIRT týmy. Výhodou intervence národního týmu při řešení bezpečnostního incidentu mohou být nejen jeho zkušenosti a kontakty, ale také samotný fakt, že je týmem národním.

Závěr

Problematika hlášení a řešení bezpečnostních incidentů je velice komplexní, zahrnuje celou řadu činností a vyžaduje celou řadu znalostí a dovedností. Tento článek dokázal obsáhnout pouze malou část (viz Box 2). Snažil se především načrtnout celkové schéma, jak tato oblast v prostředí CERT/CSIRT týmů vypadá a co se při zapracování hlášení děje. Za tým CSIRT.CZ, který v České republice vykonává roli národního týmu (viz Box 3), bychom závěrem chtěli říci, že na reagování na hlášené bezpečnostní incidenty klademe velký důraz. Při jejich řešení děláme maximum a informace, které se k nám touto cestou dostanou, se snažíme co nejvíce zužitkovat pro celkové zlepšení bezpečnosti sítí a služeb provozovaných v České republice, např. formou článků v rubrice AZB (Aktuálně z bezpečnosti), který najdete na www.csirt.cz. Chcete-li se tedy podílet na informovanosti české veřejnosti, neváhejte nám poslat zajímavé incidenty, na které narazíte (viz Box 4). Tým CSIRT.CZ je připraven pomoci a informace dostat tam, kde mohou být užitečné.

Autorský kolektiv týmu CSIRT.CZ,
Národního CSIRT týmu České republiky
Hlavní editorka Andrea Kropáčová
andrea.kropacova@nic.cz

Sdílení informací BOX 2

Hlášení bezpečnostních incidentů je jen jedním z kamenů skládačky nazvané „sdílení zajímavých informací o aktuálních hrozbách, probíhajících útocích a bezpečnostních událostech a incidentech" mezi členy bezpečnostní infrastruktury. Protože přibývá bezpečnostních problémů, přibývá také množství bezpečnostních nástrojů a prvků, které monitorují dění v síti a hlásí zjištěné anomálie v provozu – útoky, zranitelnosti, události, které mohou být předzvěstí problémů (např. přípravou na útok, krycím manévrem) nebo jsou signifikantní z hlediska toho, jestli k dané službě opravdu přistupuje uživatel s příslušnými oprávněními apod. To logicky vede k tomu, že přibývá množství dat typu bezpečnostní událost a bezpečnostní incident, se kterými bezpečnostní týmy musí pracovat. Velké množství dat ale není možné zpracovat ručně. Bezpečnostní infrastruktura se proto už řadu let zabývá problematikou automatické výměny dat a hromadného zpracování dat, kde cílem je sdílet zajímavé informace o aktuálních hrozbách rychle a efektivně a také mít tyto informace validované a oklasifikované např. z hlediska typů incidentů, závažnosti, relevance ke konkrétnímu prostředí apod. Oblast hromadného zpracování dat a systémů pro automatické sdílení informací o detekovaných bezpečnostních incidentech vydá na samostatný článek.

O Národním bezpečnostním týmu CSIRT.CZ BOX 3

Na základě dohody mezi Národním bezpečnostním úřadem (dříve na základě dohody s Ministerstvem vnitra ČR) a sdružením CZ.NIC provozuje správce domény .cz od začátku ledna 2011 Národní CSIRT tým ČR – CSIRT.CZ. Ten se jako národní tým podílí na řešení incidentů týkajících se českého kyberprostoru, tzn. incidentů, které mají původ nebo cíl v sítích provozovaných v České republice. Tým CSIRT.CZ poskytuje především koordinační pomoc při zvládání bezpečnostních incidentů, je místem „poslední záchrany v ČR" pro hlášení bezpečnostních incidentů plošného, závažného nebo opakujícího se charakteru. Více informací o misi a cílech týmu na www.csirt.cz.

Kde lze získat kontaktní informace při hlášení bezpečnostního incidentu BOX 4

Pro členy CERT/CSIRT týmů jsou základními zdroji kontaktních informací typu „kdo je zodpovědný za IP adresu nebo síť a.b.0.0/16", „kdo je držitelem nebo technickým kontaktem domény" databáze RIRů, databáze provozovatelů domén nejvyšší úrovně a katalogy oficiálních CERT/CSIRT týmů.

RIR (Regionální Internetový Registr) drží a zpřístupňuje informace o tom, komu byl přidělen který blok IP adres. Svět je rozdělen na oblasti a každý RIR (aktuálně RIPE, ARIN, APNIC, LACNIC, AFRINIC) přiděluje IP adresy pro svoji oblast. Oblast Evropy, Blízkého východu a části Asie je pod správou organizace RIPE NCC (http://www.ripe.net). RIR provozuje veřejně přístupné databáze, které obsahují údaje o přidělených internetových sítích a jejich správcích. Tyto databáze tak umožňují vyhledat údaje o tom, která organizace a kteří správci jsou zodpovědní za konkrétní IP adresu.

Dalším zdrojem užitečných informací jsou údaje o jmenných doménách, které provozují a zpřístupňují správci domén nejvyšší úrovně, pro TLD doménu .cz je to sdružení CZ.NIC.

A pak je zde oblast CERT/CSIRT týmů, které své pole působnosti obvykle definují pomocí čísel AS (autonomních systémů), IP rozsahů nebo jmenných domén. Vzhledem k jejich počtu, způsobu definování jejich pole působnosti a zejména rozdílům v jejich úrovni není vždy snadné najít tým, který je schopný pomoci. Pro usnadnění orientace mezi týmy proto vznikly jakési „katalogy", o které se starají organizace FIRST (www.first.org) a úřad Trusted Introducer (www.trusted-introducer.org). Tyto katalogy obsahují základní informace o CERT/CSIRT týmech, kontaktech, jejich poli působnosti, poskytovaných službách apod.