Jak hlásit počítačové bezpečnostní incidenty na MU

Martin Drašar, Jan Vykopal, ÚVT MU

1 Shrnutí

Efektivní řešení počítačových bezpečnostních incidentů vyžaduje rychlou a cílenou reakci, která je podmíněna bezproblémovou spoluprací mezi uživatelem, který hlásí takový incident, správci dotčených systémů a bezpečnostním týmem organizace.

V tomto článku je nejprve krátce představen bezpečnostní tým Masarykovy univerzity CSIRT-MU. Po vysvětlení, co lze považovat za počítačový bezpečnostní incident, je popsáno, jak a komu má být takový incident nahlášen. Článek uzavírají konkrétní příklady z praxe, které ilustrují odlišnou povahu incidentů, a tím i adresáty hlášení.

2 Co je CSIRT-MU?

Pod zkratkou CSIRT-MU se skrývá anglický název počítačového bezpečnostního týmu Masarykovy univerzity (*Computer Security Incident Response Team at Masaryk University*). Tento tým vznikl v rámci Oddělení bezpečnosti datové sítě ÚVT MU začátkem roku 2009. Posláním CSIRT-MU je pomáhat správcům a uživatelům udržovat univerzitní síť bezpečnou. CSIRT-MU konkrétně poskytuje tyto základní služby:

- detekce síťových průniků,
- osvěta správců a uživatelů,
- řešení nahlášených incidentů.

Posledně zmíněnou službu se snaží přiblížit právě tento článek.

3 Jak poznám bezpečnostní incident?

Na počátku celého procesu řešení incidentu je nutné rozpoznat, že vůbec jde o *bezpečnostní* incident. Poměrně snadno lze poznat porušení zákonů České republiky a dalších právních předpisů prostřednictvím sítě MU, zejména aktivity v rozporu s autorským zákonem, zásahy do osobnostního práva (šíření pomluvy, urážky). Podobně i kybernetické přestupky a zločiny, s kterými se snad každý už někdy setkal, např. nadměrné rozesílání nevyžádané pošty (spamu) či podvodná snaha o vylákání přístupových údajů k informačním a počítačovým systémům (phishing a pharming). Obtížněji a méně často lze zpozorovat neoprávněný přístup k počítačovému systému či útoky, při kterých dochází k zahlcení systému tak, že přestává odpovídat na legitimní požadavky. Výše uvedené lze považovat za bezpečnostní incidenty a je žádoucí je ohlásit.

Ne vždy je však patrné, že došlo k narušení bezpečnosti, a méně zkušený uživatel to nemusí poznat vůbec. V těchto situacích může v případě narušení síťové bezpečnosti pomoci detekce síťových průniků jakožto další služba bezpečnostního týmu univerzity.

Níže jsou uvedeny příklady bezpečnostních incidentů nebo anomálií, které by *neměly být hlášeny*:

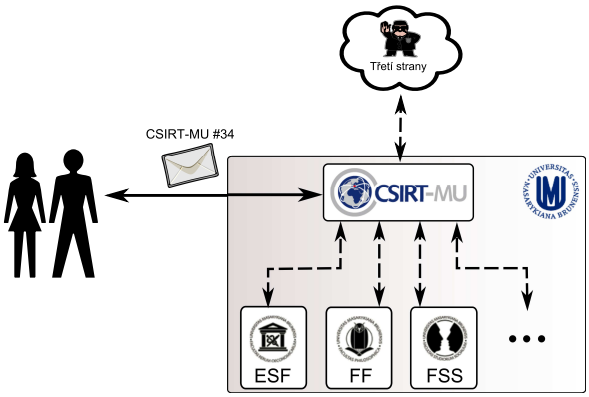
- nález nakaženého souboru antivirem,
- příjem nevyžádané pošty „v obvyklých mezích“
- nemožnost přihlášení k počítači v učebně,
- vyzrazení vlastního hesla,
- „podivně“ se chovající počítač,
- odcizení výpočetní techniky s důležitými daty (vč. USB klíčenek, přenosných disků atp.).

Možnosti předcházení bezpečnostním incidentům jsou přehledně popsány v technické zprávě CESNETu číslo 7/2006 dostupné na stránce `http://www.cesnet.cz/doc/techzpravy/2006/secprev/cz/`.

4 Hlášení incidentů a koordinace jejich řešení

Zjištěný bezpečnostní incident je třeba neprodleně ohlásit odpovědným osobám, aby se minimalizovaly jeho dopady. Fakultní správci a tým CSIRT-MU jsou vybaveni nástroji pro sledování provozu sítě a jsou schopni zajistit i stopy pro hledání pachatele (tzv. forenzní analýzu). Cílem takové analýzy je najít původ útoku, ochránit další stroje v univerzitní síti a příp. i informovat další organizace.

Obecně platí pravidlo, že *každý incident, který by se mohl dotknout více než jedné fakulty, by měl být vždy hlášen týmu CSIRT-MU*, který se postará



Obrázek 1: Komunikační toky mezi ohlašovatelem, CSIRT-MU, fakultami a třetími stranami

o koordinaci jeho řešení (viz Obrázek 1). Formalizace stávající spolupráce týmu CSIRT-MU a fakult v podobě univerzitní směrnice je v přípravě.

Pro potřeby hlášení celouniverzitních incidentů je zřízena e-mailová adresa `csirt@muni.cz`. Ostatní bezpečnostní incidenty jsou v kompetenci laboratoří výpočetní techniky (LVT, CVT, CIKT…) jednotlivých fakult. Každá LVT má obvykle vyhrazenou specifickou kontaktní adresu.

Incidenty, které jsou hlášeny týmu CSIRT-MU jsou zpracovávány automatickým systémem[1], který zajišťuje bezproblémovou spolupráci všech zainteresovaných osob.

Hlášení bezpečnostního incidentu by mělo obsahovat stručný, ale kompletní popis problému. Preferován je jednoduchý textový e-mail odeslaný z univerzitní adresy. Pokud je třeba, tak s přílohou. Předmět zprávy by měl obsahovat adresu nebo doménové jméno postiženého stroje a typ incidentu (např. phishing, spam, porušení autorského zákona). Pokud se hlášení týká e-mailové komunikace, měla by být přiložena také kompletní a nezměněná hlavička a tělo dotyčné zprávy. Hlášení musí obsahovat základní identifikaci ohlašovatele (alespoň jméno). Telefonický příjem hlášení pro případy, kdy není možné použít elektronickou poštu, je v přípravě.

Po každém nahlášení incidentu je ohlašovateli odeslán e-mail potvrzující jeho přijetí, spolu s jedinečným identifikátorem (např. `CSIRT-MU #34`). Tento identifikátor musí být při následující komunikaci přítomen v předmětu zprávy, aby byly jednotlivé zprávy přiřazeny k odpovídajícímu incidentu. Ohlašovatelé se nemusejí o identifikátory nijak zvláštně starat – dostačující je použít v e-mailovém klientovi (Outlook, Thunderbird) odpověď na zprávu (tlačítko „Odpovědět“). Za běžných okolností však ani toto nemusí ohlašovatelé nijak řešit, protože většina incidentů je zpracovávána bez jejich dalšího přičinění. Jedinou související komunikací tak je pouze oznámení o vyřešení incidentu, které je odesíláno ohlašovatelům poté, co byly podniknuty všechny potřebné kroky.

[1] Základem je ticketovací systém RT (`http://bestpractical.com/rt/`).

5 Příklady ze života

5.1 Není to incident, i když by se tak mohlo zdát

V e-mailové schránce uživatele se objeví postupem času několik dopisů s nabídkou pochybných produktů a řada z nich podle všeho pochází od osoby spjaté s univerzitou. Dohledáním podle UČO se ukáže, že jde o studenta přírodovědecké fakulty. Uživatel kontaktuje hříšníka a žádá ho o vysvětlení. Ten však tvrdí, že žádný takový mail nikdy neodeslal. Za předpokladu, že hříšník nelže, je s největší pravděpodobností jeho stroj zavirovaný.

Ačkoliv tento stroj může znamenat omezené ohrožení pro celou univerzitu, nemá smysl jej hlásit jako bezpečnostní incident fakultním správcům, tím méně týmu CSIRT-MU. Nejlepší je hříšníkovi doporučit vyčištění počítače s eventuální pomocí kompetentních osob na fakultě. Jako bezpečnostní incident by mělo smysl situaci hlásit, pouze pokud by i přes upozornění nevyžádaná pošta stále chodila. Fakultní správci už mají dostatečné páky, jak uživatele přesvědčit, aby si svůj stroj spravil.

5.2 Lokální incident

Uživatel zpozoruje, že někdo jiný v počítačové učebně odpojil kabel ze stolního počítače a připojil jej do svého notebooku. Tím tak nejspíš porušil provozní řád učebny a mohl by získat neautorizovaný přístup do síťové infrastruktury.

Tento typ incidentu je vhodné ohlásit lokálním správcům na fakultě či ve studovně.

5.3 Incident dotýkající se celé MU

Uživatel se pokusí přihlásit do Informačního systému MU. Do přihlašovacího formuláře zadá své uživatelské jméno a heslo. Uživatel údaje správně vyplní, avšak místo Informačního systému se objeví stránka s chybou. Uživatel se podívá do adresního řádku a zjistí, že se překlepl a místo adresy `http://is.muni.cz` zadal `http://is.mun.cz`. Je zřejmé, že tato stránka byla vytvořena s cílem podvodně získat přihlašovací údaje uživatelů Informačního systému MU.

V tomto případě jde o velmi nebezpečný incident a je potřeba jej neprodleně oznámit týmu CSIRT-MU, aby byly co nejdříve podniknuty kroky minimalizující ohrožení uživatelů. Ohlášením to pro uživatele samozřejmě nekončí, protože si rozhodně nezapomene změnit zkompromitované heslo. □