

Bezpečnostní incidenty, jejich charakter a řešení

14. 11. 2005

Andrea Kropáčová, ak@cesnet.cz

7275 7E6F 39E4 261D FF15 8973 BE2B 53A7 D874 7FE5

Bezpečnostní incidenty

Bezpečnostní incident představuje narušení bezpečnosti IS/IT a pravidel definovaných k jeho ochraně (**bezpečnostní politika**).

Zjištěné bezpečnostní incidenty a nedostatky musí být nahlášeny zodpovědným osobám, zaarchivovány, zdokumentovány, prozkoumány a odstraněny s ohledem na příčiny, které je vyvolaly tak, aby mohlo být dosaženo nápravy.

Bezpečnostní politika:

- soubor pravidel a postupů k dosahování a udržení definovaného bezpečnostního standardu
- stručná, jasná, úplná

Typy incidentů

- **Podle cíle** - aktivní (přerušeni dostupnosti, narušení integrity, modifikace), pasivní (odposlech)
- **Podle charakteru** - úmyslné, způsobené, nevědomostí, nedbalostí, neznalostí
- **Podle způsobených škod**
- **Obecně** - vir, červ, trojský kůň, spam, DOS (Denial of service attacks), sniffing, password cracking, zkompromitování uživatelského účtu, phishing a pharming, porušení autorských práv, porušení občanských práv, zákonů a pod.

Následky ...

... narušení bezpečnosti:

- využití napadeného prvku k dalším útokům jako přestupní stanice
- získání důvěrných dat a jejich zneužití
- poškození získaných dat
- zneužití identity – klíče, hesla

Bezpečnostní incidenty

Možnosti předcházení:

- vhodná architektura sítě, privátní sítě, DMZ
- bezpečnostní údržba systému
- vyřazení nebezpečných nebo nepoužívaných služeb (Telnet, FTP, ...)
- zabezpečení serverů, ochrana hesel, šifrované služby, PGP, S/MIME, X.509
- antivirové nástroje a antispamová ochrana
- kontrola proti rootkitům (Rootkit Hunter, chkrootkit)
- auditovací nástroje a kontrola integrity souborů (Tripwire)

Bezpečnostní incidenty

Možnosti předcházení:

- detekční systémy (IDS)
 - firewally, paketové filtry
 - **nepodporovat anonymní** užívání sítě
 - zavést **jednoznačnou autentizaci** uživatelů
 - **logovat akce** uživatelů (přístupy na servery)
 - archivace a zabezpečení logů pro možnost pozdějšího dohledání pachatele
 - směrnice pro provoz sítě
- osvěta uživatelů a správců, aneb člověk je největší slabina!!!**

Osvěta uživatelů

Se učit, se učit, se učit ...

(Zdroj: Jan Amos Komenský)

- vhodná volba a změna hesel
- ochrana hesel a klíčů
- každý systém je nejnapadnutelnější zevnitř!!!
- archivace a šifrování citlivých dat
- používání vhodných nástrojů a utilit
- znalost funkcionality používaných nástrojů a OS (prohlížeče, pamatování hesel, mazání dat)
- vědět o psychologickém nátlaku
- chraňte svoji identitu (heslo, el. podpis, PIN)!!!

Příjem a řešení incidentů

Charakter reportů o bezpečnostních incidentech:

- vyžadující odpověď
- informativní (SpamCop, MynetWatchman, IDS)

Příjem a řešení incidentů

Je nutné reagovat rychle!!!

Vhodný postup:

– ověřit, jestli incident spadá do kompetence adresáta:

- ne, ale pochází z naší sítě – přeposlat

- ne, ale patří do sítě CESNET2 – přeposlat na nadřazenou
abuse adresu, nebo na certs@cesnet.cz

- ne, nepochází ze sítě CESNET2 – odpověď autorovi stížnosti,
že incident do naší kompetence nespadá

Příjem a řešení incidentů

- lokalizovat postižený prvek sítě (stroj, uživatele)
- co nejrychleji zamezit dalšímu škodění
- analyzovat příčinu, zaarchivovat aktuální stav
- odstranit příčinu
- odpovědět na stížnost
- informovat kolegy, uživatele
- podniknout preventivní kroky, aby se útok neopakoval
- zvážit následky incidentu (prozrazení hesel, klíčů ...)

Odpovídání na incidenty

Proč? Protože:

- je to slušné
- přispívá to k informovanosti a tedy k prevenci
- ochrana dobrého jména sítě CESNET2
- shromažďování důkazů o řešení

V jakém případě?:

- když je odpověď žádoucí (= není explicitně uvedeno, že report o incidentu je pouze informativní, např. SpamCop, myNetWatchman ...)
- odpovídáme i na incidenty, které se ukáží být neopodstatněné
- v případě pochybností - požádáme autora o upřesňující informace

Odpovídání na incidenty

- **autoreply** není vhodné jako **jediná odpověď**
- odpověď na incident by měla obsahovat informaci, že se **incidentem zabýváme**, případně že jsme **problém odstranili**
- odpovědět pokud možno na **všechny adresy** uvedené v hlavičce reportu
- odpovědět **autorovi stížnosti** a v kopii tomu, kdo incident přeposlal
- odpovídat na všechny reporty jednoho incidentu

Odpovídání na incidenty

Doporučení:

- motto: “**Uživatelům chceme pomoci**” :-)
- pečlivě zvážit případné přeposlání původní stížnosti koncovému uživateli
- v odpovědi **neuvádět identitu hříšníka**, hrozí porušení OOÚ
- přijaté incidenty a jejich řešení **archivujeme**
- el. podpis
- je **lepší** odpovědět **pozdě, než nikdy!**
- slušnost, vstřícnost, věcnost

Odpoovídání na incidenty

Co hrozí při neřešení a nereagování na bezpečnostní incident:

- zablokování přístupu ze strany poškozené sítě
- žaloba
- ostuda a ztráta dobrého jména

Reportování incidentů

- stručně, jasně, srozumitelně
- definovat očekávanou odezvu
- preferovat angličtinu, případně dvojjazyčně
- jednoduchý textový mail
- připojit důkaz - hlavičku spamu, část logu, ...
- jedna IP adresa nebo adresový blok na jeden report
- výstižný **subject** obsahující:
 - IP adresu nebo adresový blok
 - typ incidentu
- pomocné informace - časová zóna, zdrojová a cílová adresa, porty
- identifikace – signatura, el. podpis

Poštovní etiketa

Dodržování základní poštovní etikety a správné používání poštovního klienta zefektivňuje a zpřehledňuje management příjmu a zpracování reportu o bezpečnostním incidentu (a e-mail komunikaci obecně).

Pavel Kácha