

Typy bezpečnostních incidentů a jejich řešení

10. května 2007, Blue Room, Karolinum

Andrea Kropáčová

andrea@cesnet.cz

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

Stávající stav a vývoj situace na poli počítačové bezpečnosti

- Roste počet uživatelů
- Uživatelé jsou čím dál horší a méně vzdělaní
- Roste počet připojených prvků
 - ==> Roste počet bezpečnostních incidentů*
- Počet správců moc neroste, jen se jim rozšiřuje zodpovědnost a přibývá práce :-)
- Hrozí ztráta a zneužití citlivých dat
- Zlepšuje se legislativa
- Dobré jméno = peníze

Proč v akademických sítích?

- Výkonná síť
- Výkonné servery
- Zajímavé zdroje dat
- Velké množství počítačů
- Velké množství neznalých uživatelů
- Velké množství “experimentujících” uživatelů
- Akademická povaha :-)

Bezpečnostní incident

- **Bezpečnostní incident** = narušení bezpečnosti IS/IT a pravidel definovaných k jeho ochraně (bezpečnostní politika)
- Zjištěné BI (nebo i jen podezření na BI) musí být ***nahlášeny osobám zodpovědným za chod sítě***, ve které se podezřelý prvek nachází
- Každý vzniklý BI musí být co nejrychleji prošetřen a odstraněn
- Aby možnost vzniku BI ***musí být připraveni*** správci i uživatelé

Bezpečnostní incident

- Neautorizovaný přístup do systému
- Ovládnutí cizího stroje
- Znemožnění řádného provozu sítě
- Odposlech utajovaných dat
- Rozesílání hromadné nevyžádané pošty
- **Porušování autorských práv**
- **Phishing**
- **Pharming**

Řešení bezpečnostního incidentu

- **Identifikace BI:**
 - Detekujeme správce sám
 - Je ohlášen = přijmeme *hlášení bezpečnostního incidentu*
- **Odstranění problému – co nejrychleji!!!**
 - Odpojení prvku od sítě
 - Zazálohování dat
- **Zvážení rizik:**
 - Možná kompromitace hesel a privátních dat
 - Rizika kompromitování dané služby by správci měli zvážit předem, ne až k tomu dojde (*disaster-recovery*)

Řešení bezpečnostního incidentu

- **Obnovení chodu služby**
 - Po odstranění příčiny selhání ochrany systému
 - Po zvážení rizik
- **Uzavření kauzy**
 - Informování kolegů (nadřízených)
 - Odpověď na hlášení bezpečnostního incidentu
 - Archivace kauzy

Vytvoření hlášení BI

- Jedna IP adresa (jeden síťový blok) na jednu stížnost
- Měla by obsahovat:
 - Důkazní materiál (log, zdrojový kód, hlavičku zprávy)
 - Pomocné informace – časová zóna, doba útoku
 - Identifikaci odesilatele
 - Požadovanou reakci
- Obecně:
 - Slušné mravy - oslovení, věcný tón, podpis
 - Stručně, žádné romány
 - Vhodně zvolit jazyk = defaultně **anglicky**

Hlášení BI elektronicky

- Výstižný **Subject** obsahující:
 - IP adresu, síťový blok
 - Typ reportovaného incidentu
- Zpráva = prostý text s přílohou
- Zprávu je nutné sestavit tak, ***aby ji nevyřadila antispamová nebo antivirová ochrana na straně příjemce***
- Podpis (identifikace odesilatele)
- Doporučujeme **elektronický podpis!!!**

Elektronická komunikace

- Je ve své podstatě *nešifrovaná*
- K obsahu zpráv se může dostat kdokoliv, kdo
 - Má potřebné vědomosti
 - Má možnosti – správce poštovního serveru nebo sítě
- Hlavičky je možné podvrhnout a do položek **From:** a **To:** dát jakoukoliv adresu
- **Ochrana:**
 - obsahu zprávy = *šifrování obsahu*
 - identity odesílatele a integrity zprávy = *el. podpis*

Elektronický podpis

- V el. světě supluje vlastnoruční podpis na papíře
- Měl by zajistit, že:
 - Uvedená osoba podepsala data vědomě
 - Podepsaná osoba je el. podpisem dostatečně ověřena
 - Dokument je pravý a nebyl následně modifikován
- Je možné použít:
 - PGP klíče
 - X.509 certifikáty
- CESNET CA (<http://www.cesnet.cz/pki>)
 - Poskytuje PKI služby akademické komunitě ČR

Kam ohlásit zjištěný BI

- Každý přidělený adresový blok (= každá IP adresa) musí mít definovanu a zveřejněnu adresu pro hlášení ***bezpečnostních incidentů***
- RFC2142 doporučuje tvar *abuse@doména.tld*
- Základní doporučení pro provoz *abuse* adresy:
 - Rozumná antivirová a antispamová ochrana
 - Více příjemců
 - Archivovat veškerou korespondenci **z** a **na** tuto adresu

Kam ohlásit zjištěný BI

- Zdrojem informací jsou veřejné DB, které provozují:
 - Regionální internetoví registrátoři (**RIPE**, ARIN, APNIC, AFRINIC, LACNIC)
 - Pro Evropu **RIPE NCC** (<http://www.ripe.net>)
 - Registrátoři národních domén (*cz, uk, sk, de, ...*)
 - Správce domény “**cz**” je **CZ.NIC** (<http://www.nic.cz>)
- Prohledávání veřejných DB:
 - Whois služba dostupná přes www
 - RIPE - <http://www.ripe.net/whois>
 - CZ.NIC - <http://www.nic.cz/cz/domeny/whois>
 - Utility *whois, jwhois* v prostředí OS

Bash\$ **whois -h whois.ripe.net 147.230.16.1**

inetnum: 147.230.0.0 - 147.230.255.255
netname: TUL-TCZ
descr: Technical University of Liberec
descr: Liberec
country: CZ
admin-c: **PS32-RIPE**
tech-c: **PA56-RIPE**
status: ASSIGNED PI
mnt-by: TENCZ-MNT
mnt-lower: TENCZ-MNT
remarks: **Please report network abuse -> abuse@tul.cz**
source: RIPE # Filtered

person: Pavel Satrapa
address: Technical University of Liberec
address: Department of Information Technology
address: Halkova 6, Liberec 1
address: The Czech Republic
phone: +420 485353685
fax-no: +420 485352229
abuse-mailbox: abuse@vslib.cz
nic-hdl: PS32-RIPE
source: RIPE # Filtered

person: Petr Adamec
address: Technical University of Liberec
address: Department of Information Technology
address: Halkova 6, Liberec 1
address: The Czech Republic
phone: +420 485353674
fax-no: +420 485352229
nic-hdl: PA56-RIPE
abuse-mailbox: abuse@tul.cz
source: RIPE # Filtered

% Information related to '147.228.0.0/14AS2852'

route: 147.228.0.0/14
descr: ZCU-TCZ + VUTBR-TCZ + TUL-TCZ + CAS-TCZ
origin: AS2852
mnt-by: AS2852-MNT
remarks: Please report abuse -> abuse@cesnet.cz
source: RIPE # Filtered

Adresa pro hlášení BI

- Za její funkčnost zodpovídá **administrativní kontakt** daného adresového bloku
- V případě **nefunkčnosti** nebo při **absenci abuse** adresy odešlete hlášení:
 - na adresu **tech/admin** správce daného adresového bloku
 - na **abuse** adresu nadřazenou – obvykle abuse adresu AS
 - Na kontaktní adresy doménového jména
- Zjištěnou **nefunkčnost** nebo **absenci abuse** adresy v síti CESNET2 ohlašte:
 - CESNET-CERTS, CESNET NIC

CESNET NIC

- **Sít'ové registrační a informační centrum**
- Členové – Pavel Vachek, A. Kropáčová, P. Kácha
- Přiděluje a spravuje IP rozsahy sítě CESNET2
- Základní kontaktní informace:
 - <http://www.cesnet.cz/nic>
 - ***nic@cesnet.cz***
- Udržuje validitu kontaktních informací uvedených v databázi RIPE

Vytvoření hlášení a reakce na hlášení BI

- **Vždy by měl zajistit správce dané sítě!**
- **Nikdy by neměl provádět koncový uživatel!!!**
- **Proč?:**
 - Vystresovaný “pachatel” může zvolit nevhodnou formu odpovědi a tím poškodit sebe nebo celou síť, nebo se dopustit OOÚ apod.
- **Proto:**
 - **Správce by neměl předávat originál stížnosti “viníkovi”**

Zázemí pro úspěšné vyřešení BI

- **Připravenost:**

- Archivovat logy o provozu služeb
- Základní dokumentace služeb a sítě
- Zástupnost správců a sdílení know-how
- Existence základní “disaster-recovery”
- Mít k dispozici náhradní řešení

- **Aby logy k něčemu byly, doporučujeme:**

- Nepodporovat anonymní užívání sítě!!!
- Provozovat jednoznačnou autentizaci uživatel
- Logovat přístupy do sítě a ke službám

Zázemí pro úspěšné řešení BI

- Je potřeba vytvořit takové zázemí, abyste vždy byli schopni dohledat minimálně následující:
 - kdo byl v danou dobu přihlášen na daném PC
 - kdo měl v danou dobu přidělenou danou IP
- Je potřeba vytvořit takové zázemí, aby všichni **uživatelé** a **správci** věděli
 - jaká je jejich role
 - co musí udělat v případě zjištění BI
- Potřebné zázemí se dobře buduje v prostředí **bezpečnostního týmu**

?

Otázky