

Typy bezpečnostních incidentů

Aleš Padrta

CESNET, z. s. p. o.

Praha

12.12. 2008

Obsah

- Úvodní slovo
- Co je to bezpečnostní incident
- Klasifikace bezpečnostních incidentů
- Pojmy související s bezpečnostními incidenty
- Typy bezpečnostních incidentů
 - Ovládnutí cizího stroje
 - Znemožnění provozu sítě
 - Rozesílání nevyžádané pošty
 - ...
- Shrnutí

Úvodní slovo

- Roste počet uživatelů IT
- Roste počet připojených prvků
- Stále více služeb je dostupných přes Internet
 - ⇒ Vyšší počet napadnutelných cílů
 - ⇒ Větší možnosti (přímého) zisku
 - ⇒ Větší motivace pro útočníky
- Nedostatečné vzdělání uživatelů
 - ⇒ Roste počet bezpečnostních incidentů

Co je to bezpečnostní incident?

- Bezpečnostní incident
 - Narušení bezpečnosti IS/IT nebo
 - Porušení pravidel definovaných k jejich ochraně (bezpečnostní politika)
- Následky
 - Únik informací
 - Ochromení činnosti organizace
 - Poškození dobrého jména

Klasifikace incidentů

- Podle charakteru
 - Úmyslné
 - Způsobené nedbalostí
 - Způsobené nevědomostí
- Podle způsobu provedení
 - Aktivní – s přímým dopadem na cílový systém
(např. nedostupnost, ...)
 - Pasivní – bez přímého dopadu (např. odposlech, ...)

Klasifikace incidentů

- Podle cíle
 - Koncové stanice
 - Zneužití stroje
 - Zneužití obsahu
 - Odposlech činnosti
 - Služby, IS
 - Narušení integrity, dostupnosti nebo důvěrnosti
 - Sít'
 - Omezení funkčnosti
 - Odposlech provozu

Pojmy související s bezpečnostními incidenty

- Malware
 - Malicious software (zákeřný SW)
 - Viry, wormy, trojské koně
- Crimeware
 - Speciální druh malware
 - Krádež identity, finanční kriminalita
- Spyware
 - Špionážní SW (zisk zajímavých údajů)
- Adware
 - Reklamní SW (obtěžuje, zdržuje, ...)

Pojmy související s bezpečnostními incidenty

- Logical bombs
 - Činnost (malware) vázана na událost
 - Datum, spuštění určité aplikace
 - ...
- Back door
 - Zadní vrátka
 - Možnost vrátit se na napadený systém
 - Vytvoření konta, spuštění služby, ...
- Rootkit
 - Sada programů
 - Ovládnutí stroje + ukrytí této skutečnosti

Typy bezpečnostních incidentů

- Běžně se vyskytující typy
 - Ovládnutí cizího stroje
 - Scanování
 - Rozesílání hromadných nevyžádaných zpráv
 - Porušování autorských práv
 - Defacement
 - Phishing
 - Pharming
 - Znemožnění řádného provozu
 - Neautorizovaný přístup a odposlech dat
 - Zneužití identity
 - Cyberstalking

Ovládnutí cizího stroje

- Získání stroje pod svou kontrolu
 - Pracovní stanice i servery
 - Využití pro své (nekalé) potřeby
- Technicky
 - Chyby v SW
 - Špatná konfigurace
 - Malware
- Lidský faktor
 - Neznalost
 - Nízká obezřetnost
 - Důvěřivost \Rightarrow sociální inženýrství

Scanování sítě či systému

- Získávání informací o
 - Připojených strojích
 - Běžících službách
- Hledání vhodných cílů
- Obvykle předzvěst dalších aktivit
- Zdroj = obvykle ovládnuté cizí stroje
- GYM scanning (Google, Yahoo, Microsoft)
 - Informace z cache vyhledávačů
 - Skryté

Rozesílání hromadných nevyžádaných zpráv

- Označováno jako *spam*
 - Internetová fóra – první výskyt
 - Instant messaging – ICQ apod.
 - E-mail – v současnosti nejrošířenější, 98% provozu
 - VoIP – v brzké budoucnosti
- Zdroj = ovládnuté cizí stroje
- Způsobené potíže
 - Technické – zátěž (mail) serverů
 - Sociální – obtěžování uživatelů, sociální inženýrství
 - Finanční – boj se spamem, promarněná pracovní doba
- Hoax

Porušování autorských práv

- Porušování pravidel
 - Autorský zákon
 - Obvykle také směrnice organizace
- Poskytování díla nebo jeho části
 - Nejčastější problém
 - P2P sítě (Direct Connect, eMule, BitTorrent, ...)
 - FTP servery
- Neoprávněné používání SW
 - Nedodržení licenčních podmínek
 - Použití “cracků” ⇒ další bezpečnostní problémy

Defacement

- Napadení webové stránky
 - Ovládnutí serveru
 - Získání přístupu
- Změna obsahu
 - Dle libovůle útočníka
 - Obvykle vystavení vlastní “reklamy”
 - Někdy též nelegální obsah
- Důsledky
 - Ztráta dobrého jména organizace
 - Poškození činnosti

Phishing

- *Alias scam alias link manipulation*
- Cíl = přimět oběť k vyzrazení citlivých informací
- Sociální inženýrství
 - Psychologické metody
 - Manipulace s lidmi
- Nejčastěji
 - Podvržené weby (banky, internetové obchody, ...)
 - Často zdařilé kopie
 - E-maily
 - Přesměrování na podvržený web

Pharming

- Zákeřnější než phishing
 - Cíl – stejný
 - Prostředky – sofistikovanější
- Nespoléhá na podvržené odkazy
- Změna DNS služby
 - Podstrčení falešných záznamů (DNS poisoning)
 - Úprava routeru v místní síti oběti
 - Změna DNS serveru stanice (pomocí malwaru)
- Velmi těžko odhalitelné
 - DNSSEC, důsledná kontrola certifikátů

Znemožnění řádného provozu

- Sítě
 - Vyčerpání přenosového pásma
- Služby
 - Narušení dostupnosti (DoS, DDoS)
 - Narušení integrity (modifikace dat, konfigurace, ...)
 - Narušení důvěrnosti
- Koncových stanic
 - Zneužívání výpočetního výkonu
 - Zneužívání diskového prostoru
 - Zneužívání konektivity

Neautorizovaný přístup a odposlech dat

- Neautorizovaný přístup
 - Mnoho systémů a služeb \Rightarrow únik přístupových údajů
 - Zneužití chyby systému
- Odposlech dat
 - Přenos po síti \Rightarrow možnost odposlechu “kýmkoliv”
 - Např. e-maily
 - Prolomení šifrovacího algoritmu
 - Přesměrování komunikace – Man in the middle
 - Kompromitovaný stroj \Rightarrow monitorování síťové činnosti
 - Jednodušší než prolomení šifry

Zneužití identity

- Elektronická identita
 - Vazba mezi fyzickou a elektronickou “osobou”
 - IS/IT pracuje pouze s elektronickou identitou
- Způsob krádeže
 - Uhodnutí hesla (např. pomocí spyware)
 - Kopie certifikátu
- Možnosti zneužití
 - Přístupy do systému
 - Vydávání se za někoho jiného

Cyberstalking

- Elektronická varianta
 - Pronásledování
 - Úmyslné obtěžování
 - Získání moci nad obětí
- Charakteristické rysy
 - Zneužívání osobních informací (blogy, profily, ...)
 - Vyhrožování a slovní napadání
 - Používání e-mailu, instant messagingu (ICQ, ...)
 - Vytrvalost
 - Systematické deptání oběti

Shrnutí

- Bezpečnostní incidenty
 - Definice
 - Klasifikace
 - Základní pojmy
 - Nejčastější typy
- V současnosti obzvlášť populární
 - Phishing
 - Pharming
 - Porušování autorských práv
 - Ovládnutí cizích strojů \Rightarrow botnety

Děkuji za pozornost