Hrozby, slabá místa, aktiva, škodlivý software

Z FITwiki

Obsah

Hrozby, slabá místa, rizika

Cíle bezpečnosti IS

- Confidentiality – důvěrnost – ochrana proti neoprávněnému prozrazení informace
- Integrity – integrita – ochrana proti neoprávněné modifikaci informace
- Availability – dostupnost – ochrana proti neoprávněnému odepření přístupu k datům nebo ke službám

Hrozby (Threats)
: jsou situace, které mají potenciál způsobit bezpečnostní incident pokud dostanou příležitost (hacker, prozrazení informace o vstupu), jde o vlastnost prostředí, po přesunu IS na jiné místo mohou vznikat jiné hrozby

- **Neúmyslné** (pravděpodobnostní) hrozby – živly, poruchy, chyby v SW, omyly
- **Úmyslné** (algoritmické) hrozby
  - **Cílem nejsou data** (krádež HW, poškození HW, neoprávněné užití HW)
  - **Cílem jsou data** (krádež SW, krádež dat, neoprávněná manipulace s daty)
  - **Cílem je uškodit** (škodlivé programy - viry, červi, logické bomby, trojské koně)

Zranitelná místa (Vulnerabilities)
: jsou slabiny v IS, které je možné použít k útoku na IS

- **Při návrhu** – chyba v architektuře, analýze, návrhu
- **Při implementaci** – chyby v kódu (buffer overflow)
- **Při provozu** – špatný postup (krátká hesla) nebo nastavení

Riziko
: je kombinace zranitelného místa a hrozby (tedy musí existovat slabina a také příležitost nebo motiv ji využít).

Aktiva (Assets)
: jsou složky IS, které mají hodnotu (fyzická i abstraktní) (hardware, software, data, lidé, pověst) - mohou být poškozena bezpečnostním incidentem

Opatření (Measures)

redukují pravděpodobnost vzniku útoku.

- **Preventivní** – před útokem, např. cedule *Zákaz kouření*
- **Reakční** – během / po útoku, např. hasicí přístroj

Systémy Honey Pot
: zkoumají online hrozby v síti (tváří se jako potenciální oběti pro útoky). Pokoušejí se na sebe nalákat útoky a ty pak analyzovat. Typická farma Honey Pot – skupina počítačů s různými verzemi OS připojená k síti

Malware

Malware (škodlivý software)
: bez vědomí a souhlasu uživatele provádí neautorizovanou činnost (autorizovaný - ten, kdo systém vlastní, dal svolení k této činnosti; autentizace - ověření identity člověka)

Virus

: je program, který se replikuje, aby infikoval co největší část cílového systému nebo aplikačního programu. Typicky potřebuje hostitelský program a musí být spuštěn. Nepotřebuje počítačovou síť.

- Replikace mezi soubory i z disku na disk
- Typy virů:
  - **Boot-sector virus** – infikuje MBR
  - **Souborový infektor** – infikuje spustitelné programy (původní koncept)
  - **Makrovirus** – infikuje dokumenty s makry
  - **Skriptovací virus** – virus psaný ve skriptovacím jazyce, šíří se jako zdrojový kód
  - **Multipartitní virus** – kombinuje více typů

Červ

- je samostatný (bez hostitele)
- replikuje ze systému na systém (ne mezi soubory) v počítačové síti
- infikuje systémy, ne soubory

Trojský kůň

- je program, který na pozadí viditelné činnosti vykonává ještě skrytou škodlivou činnost (krádež hesel, mazání souborů, vytváření zadních vrátek)
- neprovádí replikaci

Spyware
: sbírá osobní informace a hesla, posílá je útočníkům.

Logická bomba

: nic neinfikuje, ale na základě jisté podmínky provede destrukční činnost (zašifruje data, odšifruje až po zaplacení). Nereplikuje se.

Rootkit

: je virus, který běží pod OS, je tedy špatně detekovatelný. Je to softwarový balík určený k tomu aby vytvořil, utajil a spravoval prostředí pro útočníka na kompromitovaném stroji.

- **Binary rootkits** – modifikace systémových souborů

- **Kernel rootkits** – modifikace komponent kernelu
- **Library rootkits** – přepisují systémové knihovny

Specificky internetové typy malware

JAVA

- stažený kód interpretovaný na klientské počítaci
- Ochrana pomocí „pískoviště“ – Sandbox

ActiveX

- Nativní spustitelný kód, stažený z internetu
- Může provádět cokoli (žádné pískoviště)
- Ochrana podepisováním

Techniky skrývání

Spofing/Stealth
: filtrace volání operačního systému tak, aby program byl neviditelný

Šifrování
: šifrování kódu programu

Polymorfismus
: Způsobí, že virus vypadá po každé replikaci zcela jinak, Mutační stroje (vyrobí z algoritmu jiné algoritmy, které dělají to stejné, ale vypadají jinak)

Další hrozby

Spam
: je zákonem definováno jako nevyžádané obchodní nabídky, pojem znám jako veliké množství nevyžádaných e-mailů (také pro rozšiřování jiného malwaru)

Phishing
: je využití sociálního inženýrství k získání dat podvodem. Nalákání na podvodné stránky za účelem získat přihlašovací údaje, ...

Boty a botnety/Zombie
: síť infikovaných počítačů, které se posléze využije k útoku, často spojeny do sítě (DDoS). použití: přeposílání spamu, warez …

Kategorie: Státnice 2011 | Bezpečnost informačních systémů

- Stránka byla naposledy editována 29. 5. 2015 v 19:12.