Ochrana PC v síti

Ochrana počítače v počítačové síti. Bezpečnostní zásady práce s výpočetní technikou. Antivirové programy.

Ing. Lukáš Macura
UIT

Obsah

- Počítačová bezpečnost
- Kybernetická bezpečnost
- Mýty o bezpečnosti
- Informační bezpečnost
- Pojmy
- Typické útoky
- Zásady bezpečnosti

Počítačová bezpečnost

- Zabývá se odhalováním a eliminací rizik spojených s používáním počítačů
- Zabezpečení před neoprávněnou manipulací systému
- Zabezpečení před neoprávněnou manipulací dat (nechtěnou i chtěnou)
- Zabezpečení proti krádeži nebo modifikaci dat
- Dnes už nestačí

Počítačová bezpečnost

- Bezpečný přenos dat (kryptografie)
- Bezpečné uložení dat (ochrana proti odcizení i proti poškození)
- Dostupnost
- Celistvost
- Nepopíratelnost

Kybernetická bezpečnost

- Nad počítačovou bezpečností
- Svět plný elektronických zařízení
- Sami zanecháváme elektronické stopy všude
- Zdaleka není jen o technice

Mýty o bezpečnosti

- „Je to vše jen o IT“
- „TOP management nemá s cybersecurity co dělat“
- „Investice půjdou jen do technologie“
- „Bezpečnost nemá vliv na ROI“
- „Kybernetická bezpečnost je jednorázový projekt“
- „Dokumentace je mýtus“

Mýty o bezpečnosti
Bezpečnost se mě netýká

- **29.12.2014** Čeští uživatelé internetu – obětí phishingových e-mailů
- **30.12.2014** Česká spořitelna - varuje před nebezpečným virem
- **01.12.2014** Exekutorská komora – spear phishingové e-maily
- **03.12.2014** Společnosti z oborů energetiky, dopravy a infrastruktury – napadeny íránskými útočníky
- **12.12.2014** Centrální databáze obyvatel Srbska – odcizení dat
- **16.12.2014** V centru Osla – nalezeny falešné BTS stanice
-
- Zdroj: nckb

Informační bezpečnost

- Kontinuální ochrana informací
- ISO 27000
- HW
- SW
- Produkty
- Služby
- Komunikace
- Lidi

Autentizace

- Proces ověření identity
- Nemusí to být pouze člověk
  - Stroj, Aplikace, Zvíře, ..
- V našem případě jméno a heslo
- Může být složitější/vícefaktorová

Autorizace

- Proces udělení práv k něčemu
  - Práva na síťový disk
  - právo změnit soubor
  - právo přihlásit se ke zkoušce
  - ...

Accounting

- Proces měření zdrojů a času
- Pro daného ověřeného uživatele
- Pro dané právo
- Důležité pro následnou analýzu

Logování

- Každá významná akce v systému musí být uložena tak, aby byla zpětně dohledatelná zpětně. Slouží pak pro případný audit.
- Příklad: Uživatel xyz se zapsal na zkoušku ZK v přesně uvedený čas ze svého WWW prohlížeče
- Příklad: Uživatel se přihlásil do svého emailu
- Příklad: Uživatel se přihlásil do eduroamu

Zranitelnost

- Slabé fyzické nebo logické místo systému
  - Známá
  - Neznámá
  - Zdokumentovaná
  - Nezdokumentovaná
- Například chyba OS (proto aktualizace)
- Například odemknutý trezor

Hrozba

- Důsledek zranitelnosti
- Cokoliv nebo kdokoliv s potenciálem škodit
- Například hrozba napadení útočníkem
- Například hrozba vykradení trezoru

Rizika

- Pravděpodobnost zneužití konkrétního zranitelného místa
- Míra pravděpodobnosti
- **Riziko** = **HA** x **PUH** x **Z**
- hodnota aktiva x pravděpodobnost uplatnění HROZBY x zranitelnost

Typické útoky
Rybaření (phishing)

- Pokus o vytažení informací podvodným mailem
- Nemusí se jednat pouze o mail
- Email se dá podvrhnout, nikdy nedůvěřujte emailu, dokud není ověřen elektronickým podpisem!

Typické útoky
Rybaření (phishing)

Drahoušek Zákazník,

Tato is tvuj funkcionár oznámení dle Ceská Sporitelna aby clen urcitý služba dát pozor pod vule být deactivated a odstranit kdyby nedošlo k obnovit se bezprostrední.

Predešlý oznámení mít been poslaný až k clen urcitý Žaloba Dotyk pridelil až k tato úcet.

Ackoliv clen urcitý Bezprostrední Dotyk , tebe musit obnovit se clen urcitý služba dát pozor pod ci ono vule být deactivated a odstranit.

Obnovit se Ted tvuj SERVIS 24 Internetbanking.

SERVIZ: SERVIS 24 Internetbanking

SKONANI: Leden, 11 2008

Být zavázán tebe do using SERVIS 24 Internetbanking. My ocenit tvuj obchod a clen urcitý príležitost až k sloužit tebe.

Ceská Sporitelna Služba úcastníkum

Lamer.cz

- <*Martinka*> jake mas heslo....chtela bych se na tebe prihlasit...at si muzu prohlidnout ty fotky...:)
- <Kay> lol
- <*Martinka*> ja ho nikomu nereknu
- <*Martinka*> NIKOMU
- <Kay> LOL
- <*Martinka*> heeeeeeeeeeej..."lol" to neni

Zásady bezpečnosti správce sítě

- Musí rozumět SW, HW a principům funkce
- Musí správně nastavit servery a aplikace
- Musí dbát na dodržování pravidel na síti
- Musí zajistit logování všech důležitých akcí
- Musí být schopen dohledat viníka bezpečnostního incidentu
- Musí stále sledovat a opravovat všechny bezpečnostní chyby

Lamer.cz

- <a> tak sem si na komp nainstaloval keylogger, melo by mi to vsechny hesla posilat mailem
- <b> a co? funguje ti to
- <a> nevim, bohuzel sem zapomel heslo na mail

Zásady bezpečnosti uživatel

- „STOP being clicking monkey!“
- Nedůvěřujte všemu co vidíte
- Nikdy nikomu nezasílejte hesla, obzvlášť ne na výzvy emailem
- Hlídejte si své osobní informace
- Nesdílejte vše, co vás napadne
- Udržujte svůj počítač a antivir aktualizovaný

Zásady bezpečnosti uživatel

- Mějte nainstalovaný a zapnutý antivir
- Aktualizujte jej
- Je relativně jedno, jaký antivir, ale důležité je, aby byl aktivní a aktualizovaný
- I ten nejlepší antivir nemusí odhalit hrozbu, pokud je dobře cílená a provedená
- Ale 99% hrozeb většinou odhalí

Zásady bezpečnosti uživatel

- Aktualizujte si svůj operační systém pravidelně
- Mnohdy jsou chyby naprosto kritické (vzdálené ovládání PC bez Vašeho souhlasu, smazání dat, ...)
- Riziko napadení roste s dobou, po kterou neaktualizujete

Zásady bezpečnosti uživatel

- Pozor na sociální sítě
- Propojením dat se dá získat spoustu informací
- Myslete před tím, než cokoliv zveřejníte
- http://pleaserobme.com/
- Osobní data nikdy neposílejte na nedůvěryhodné weby
- Ověřte si, že spojení je https
- Neignorujte výstrahy prohlížeče o bezpečnosti

Děkuji za pozornost

- Dotazy?

- Ing. Lukáš Macura