Zjištění zabezpečení sítě a navrhnout lepší bezpečnostní politiku

Miroslav Smejkal

SOUČASNÝ STAV ZABEZPEČENÍ

- Neexistující bezpečnostní politika
- Špatný návrh sítě
  - Žádný firewall
  - Nečlenění do podsítí
- Žádná aktualizace softwaru - prošlé licence
- Slabá hesla a na stanicích jen jeden uživatel a to administrátor
- Wifi síť bez zabezpečení

NÁVRH

- Rozdělení sítě
  - DMZ – firewall, proxy
  - Podsíť 1 – řadový pracovníci – přístup pouze na port 80 a povoleny pouze stránky , které potřebují k práci
  - Podsíť 2 –sekretářka, ředitel – povoleny všechny porty

NÁVRH II

- PC stanice
  - MS Vista
  - Osobní firewall(kerio), antivir(avast, nod 32), spyware(ad-ware)
  - Firefox 3.0 – zakázány pop-up okna, javascript.
  - Thunderbird
  - Vytvořit uživatele s omezenými pravomocemi
  - Automatická aktualizace softwaru

NÁVRH III

- WIFI
  - Změna defaultního SSID a defaultního hesla
  - Skrýt broadcastové vysílání SSID
  - Použít zabezpečení WPA 2 s autentizaci Radius
  - Omezit možnost přístupu MAC adresami

NÁVRH IV

- Bezpečnostní politika
  - Uživatel si zvolý dostatečné bezpečné heslo – minimálně 8 znaků s jedním číslem a jedním speciálním znakem
  - Uživatel si nepíše svá hesla na papír a nelepí si je na monitor
  - Uživatel neotvýrá neočekávanou poštu a nekliká na případné odkazy v e-mailu

Poděkování

Děkuji za pozornost