

AZ INFORMATIKAI HÁLÓZATI INFRASTRUKTÚRA BIZTONSÁGI KOCKÁZATAI ÉS KONTROLLJAI



| | |
|-----------------|---|
| Készítő: | MTA SZTAKI |
| Státusz: | <i>Második mérföldkő lezárása; nyilvános!</i> |
| | 2005. június |



© IHM - MTA-SZTAKI, 2005.

*A tanulmány elkészítésében és belső lektorálásában részt vettek:
Becz Tamás, Kincses Zoltán, Lakatos György, Pásztor Szilárd, Rigó Ernő, Tiszai Tamás, Tóth Beatrix*

Tartalomjegyzék

| | |
|--|-----------|
| 1. Bevezető..... | 6 |
| 1.1. A tanulmány felépítése..... | 6 |
| 1.2. Röviden a tartalomról és a célokról..... | 7 |
| 1.3. Szerzői jogi nyilatkozatok..... | 7 |
| 2. Biztonsági politika, fogalmak, írott szabályzatok..... | 8 |
| 2.1. Fogalmak..... | 8 |
| 2.2. Szabályzatok felépítése..... | 9 |
| 3. Egyéb figyelembe veendő szabályok..... | 13 |
| 3.1. Privacy / Adatvédelem..... | 13 |
| 3.2. Deficiency / Segítséggel élők..... | 13 |
| 3.3. Copyright / Szerzői jog, szabadalmi törvény..... | 14 |
| 3.4. Forensics / Törvényszéki bizonyítás..... | 14 |
| 4. Kockázatelemzés..... | 15 |
| 4.1. Előkészület..... | 15 |
| 4.2. Kockázatelemzés módszere..... | 16 |
| 5. Topológia (strukturális hálózati biztonság)..... | 17 |
| 5.1. Funkcionalitás..... | 17 |
| 5.2. Hálózat-menedzsment..... | 17 |
| 5.3. Hálózatbiztonság..... | 17 |
| 5.4. Hálózati struktúra gyengeségeinek kihasználása..... | 18 |
| 5.4.1. Fizikai struktúra..... | 19 |
| 5.4.2. Logikai struktúra..... | 20 |
| 5.4.3. Támadási lehetőségek..... | 21 |
| 5.4.3.1. Megszemélyesítéssel támadások..... | 21 |
| 5.4.3.2. WLAN hozzáférés-védelem..... | 21 |
| 5.4.3.3. VPN-ek, behívások gyengeségei..... | 21 |
| 5.5. Hálózati architektúra megváltoztatása..... | 22 |
| 5.5.1. Logikai struktúra..... | 22 |
| 5.5.1.1. DMZ..... | 23 |
| 5.5.1.2. LAN..... | 23 |
| 5.5.1.3. SERVICE..... | 23 |
| 5.5.1.4. VPN..... | 24 |
| 5.5.2. Fizikai struktúra..... | 24 |
| 5.6. ToReS hálózati infrastruktúra alkalmazási esetei..... | 24 |
| 5.6.1. Publikus Internet hálózat..... | 24 |
| 5.6.2. Kliens hálózat (NAT)..... | 25 |
| 5.6.3. Biztonsági szemszögből felépített hálózat..... | 25 |
| 6. Szolgáltatások biztonsága..... | 27 |
| 6.1. Szolgáltatás szerinti felosztás..... | 27 |
| 6.1.1. Web / Böngészés..... | 27 |
| 6.1.2. E-mail / Elektronikus levelezés..... | 29 |
| 6.1.3. Samba / Windows-Linux fájlmegosztás..... | 37 |
| 6.1.4. FTP..... | 39 |
| 6.1.5. NFS..... | 41 |
| 6.1.6. DNS..... | 44 |
| 6.1.7. DHCP..... | 45 |
| 6.1.8. LDAP..... | 46 |
| 6.1.9. Dialin / Betárcsázás..... | 47 |
| 6.1.10. Távoli elérés..... | 48 |
| 6.1.11. Adatbázis-szerver..... | 50 |
| 7. Hoztók biztonsága..... | 52 |
| 7.1. Általános biztonsági problémák..... | 52 |

| | |
|---|------------|
| 7.2. Telepítési alapelvek..... | 52 |
| 7.3. Alapvető biztonsági követelmények..... | 54 |
| 7.3.1. Windows XP megerősítése..... | 55 |
| 7.3.1.1. A Windows XP környezetei..... | 55 |
| 7.3.1.2. Windows XP mintabeállításainak áttekintése..... | 58 |
| 7.3.1.3. Biztonsági mintabeállítások..... | 69 |
| 7.3.1.4. A Windows XP biztonsági beállításainál alkalmazott eszközök..... | 83 |
| 7.3.1.5. A Windows XP rendszerben használt portok..... | 84 |
| 7.3.2. Linux megerősítése..... | 85 |
| 7.3.2.1. Alapvető biztonsági követelmények..... | 86 |
| 7.3.3. Digitális aláírás alkalmazása..... | 87 |
| 7.3.3.1. Digitális aláírás Windows rendszeren (PGP)..... | 87 |
| 7.3.3.2. Digitális aláírás Linuxos rendszeren (PGP, GnuPG)..... | 87 |
| 7.3.4. Öntesztelés..... | 87 |
| 7.3.4.1. Öntesztelés Windows rendszeren – MBSA..... | 88 |
| 7.3.4.2. Öntesztelés Linux rendszeren..... | 88 |
| 7.3.5. A rendszerelemek kivonása..... | 88 |
| 7.4. Egyéb előnyös biztonsági beállítások..... | 88 |
| 7.4.1. Linux..... | 89 |
| 7.4.2. Windows..... | 89 |
| 7.5. Hozzáférés-védelem (access control)..... | 90 |
| 7.5.1. Hardver..... | 90 |
| 7.5.2. Linux..... | 90 |
| 7.5.3. Windows..... | 90 |
| 7.6. Megfigyelés és elemzés (monitoring)..... | 91 |
| 7.6.1. Linux..... | 92 |
| 7.6.2. Windows..... | 92 |
| 7.7. Integritás-ellenőrzés..... | 93 |
| 7.7.1. Integritás-ellenőrzés Linux rendszeren..... | 93 |
| 7.7.2. Logelemzés..... | 94 |
| 7.7.3. Biztonsági kockázatok felmérése..... | 94 |
| 7.8. Vizsgálat, bizonyíték-gyűjtés, igazságügyi eljárás..... | 94 |
| 7.8.1. Észlelés és lehetséges incidensek..... | 94 |
| 7.8.1.1. A támadás azonosítása..... | 95 |
| 7.8.1.2. Hoszt-alapú vizsgálat..... | 96 |
| 7.8.1.3. Mit keressünk?..... | 97 |
| 7.8.1.4. Kapcsoljuk össze az eredményeket..... | 99 |
| 7.8.2. A cél..... | 99 |
| 7.8.2.1. Eszközfejlesztés..... | 100 |
| 7.8.2.2. Első lépések, a munka kezdete..... | 100 |
| 7.8.2.3. Beépített Windows eszközök..... | 100 |
| 7.8.2.4. Mit keressünk?..... | 101 |
| 7.8.2.5. Behatolás után kutatva..... | 103 |
| 7.8.3. Megoldás..... | 104 |
| 7.8.3.1. Törvények..... | 105 |
| 7.8.3.2. Szabályok és eljárások..... | 105 |
| 7.8.3.3. Naplózás..... | 105 |
| 7.8.3.4. Az eszköztár összeállítása..... | 105 |
| 7.8.3.5. Másolat (image) készítés..... | 106 |
| 7.8.4. Keresés a rendszerben..... | 106 |
| 7.8.5. Mélyebbre ásás – törölt, rejtett, titkosított fájlok..... | 107 |
| 7.8.6. Linux specifikus eszközök és eljárások..... | 108 |
| 7.8.6.1. On-line forensics..... | 108 |
| 7.8.6.2. Off-line forensics..... | 112 |
| 8. Kiegészítő biztonsági elemek..... | 114 |

| | |
|---|------------|
| 8.1. Hardver és környezet..... | 114 |
| 8.2. Smart card / Intelligens kártya..... | 114 |
| 8.2.1. Intelligens kártyákról..... | 114 |
| 8.2.2. Kártyaolvasó telepítése..... | 115 |
| 8.2.3. A kommunikáció első lépései és formátuma..... | 116 |
| 8.2.4. Nyelvek és wrapper-ek..... | 116 |
| 8.3. Biometria..... | 116 |
| 8.4. Honeypot..... | 117 |
| 9. Következtetések, zárszó..... | 118 |
| 10. Mellékletek..... | 119 |
| 10.1. ToReS CD indítása..... | 119 |
| 10.1.1. Hálózati konfiguráció..... | 120 |
| 10.1.2. A rendszer általános használatáról..... | 122 |
| 10.1.3. Állapotmegőrzés, remastering..... | 123 |
| 10.1.4. Tipikus felhasználási lehetőségek..... | 124 |
| 10.2. TOP-listák..... | 125 |
| 10.2.1. SANS topten, what works?..... | 125 |
| 10.2.2. Egyéb listák, előrejelzések, várható trendek..... | 126 |
| 10.3. Zsebsorozat..... | 126 |
| 11. Irodalomjegyzék, ajánlott irodalom..... | 127 |

Táblázatjegyzék

| | |
|--|-----|
| 1. Táblázat: ISO 9001:2000 – ISO 17799 összehasonlítása..... | 10 |
| 2. Táblázat: Eseménynapló beállításai..... | 61 |
| 3. Táblázat: Fiókházirend – jelszóházirend..... | 70 |
| 4. Táblázat: Fiókházirend – fiókszárózási házirend..... | 70 |
| 5. Táblázat: Helyi házirend – Naplórend..... | 71 |
| 6. Táblázat: Felhasználói jogok kiosztása..... | 73 |
| 7. Táblázat: Biztonsági beállítások..... | 78 |
| 8. Táblázat: Eseménynapló házirend..... | 78 |
| 9. Táblázat: Kötött csoportok..... | 78 |
| 10. Táblázat: Rendszerszolgáltatások..... | 80 |
| 11. Táblázat: Fájl engedélyek beállítása..... | 80 |
| 12. Táblázat: Rendszerleíró-adatbázis beállításai..... | 82 |
| 13. Táblázat: Rendszerleíró-adatbázis értékei..... | 83 |
| 14. Táblázat: A Windows XP biztonsági beállításainál alkalmazott eszközök..... | 84 |
| 15. Táblázat: A Windows XP rendszerben használt portok..... | 85 |
| 16. Táblázat: Vizsgálati eszközök..... | 100 |
| 17. Táblázat: Vizsgálat során észlelt gyanús kapcsolódások..... | 102 |
| 18. Táblázat: A ToReS indítás folyamata..... | 119 |

Ábrajegyzék

| | |
|--|-----|
| 5.1. Ábra: a hálózati szolgáltatások kockázatai (SZTAKI)..... | 18 |
| 5.2. Ábra: általános, funkcionálisan felépített, nyilvános, IP alapú hálózat..... | 20 |
| 5.3. Ábra: általános, biztonsági alapon felépített, nyilvános, IP alapú hálózat..... | 22 |
| 7.1. Ábra: Tipikus OKV hálózati architektúra..... | 56 |
| 7.2. Ábra Tipikus vállalati környezet architektúra..... | 57 |
| 10.1. Ábra: A beköszönő ToReS logo..... | 119 |
| 10.2. Ábra: Hálózati elérés típusának kiválasztása..... | 121 |
| 10.3. Ábra: a ToReS hálózatdetektáló folyamata..... | 122 |
| 10.4. Ábra: ToReS eszközök (menüreszlet)..... | 123 |
| 10.5. Ábra: Vizsgálódó eszközök munka közben..... | 126 |