Deloitte.

Kiber-veszélyek

Merre halad a világ?

… és merre az auditorok?

Antal Lajos
Partner

Deloitte Hungary
Bronz Medalist
Global Cyberlympics 2012

Az előadó…

- 17 év információbiztonsági gyakorlattal rendelkezik
- Deloitte középeurópai régió Informatikai Biztonság Üzletág vezető partnere
- Gyakorlott IT biztonsági tesztelő
- IBM mainframe biztonság Subject Matter Expert (SME)

Az előadás témája

Merre halad a világ kiber-fenyegetettség terén és merre haladnak az auditorok a módszertanokkal és az alkalmazott kontrollok ellenőrzésével.

A két világ hol találkozik.

Kiber-nézőpontból mik a kihívások egy pénzügyi és egy IT auditor számára.

Kiber

Kiber-támadás – Bizonyos körülmények között néhány állam háborús tevékenységnek tekinti

Kiber-háború – Kiber-terrorizmus – Elektronikus hadviselés

Kiber-bűnözés – E-bűnözés

Botnetek, Phishing, E-csalás, Személyazonosság-lopás

Amikor még egyszerű volt az élet

Év	Az IT biztonság világa
1998	• Sérülékenységek, sérülékenységek és sérülékenységek • Nagyrészt infrastruktúra tesztelés • Dshield, packetstormsecurity • Klasszikus hálózat alapú behatolástesztek (később infrastruktúra teszt néven) • War-dialing: minden számot megcsöngettünk modemeket keresve
1999-2002	• Web-alkalmazás tesztelés • Weboldal biztonságának növelése betöréssel • Alkalmazásfejlesztők nem tudtak sokat a biztonsági kérdésekről • Levin a bankrabló hacker • Infrastruktúra biztonság még mindig nem volt fókuszban – az xspy még majdnem mindenhol működött • 2000 környékén már az OSSTMM és a pentesztelés kezd eljutni a köztudatba • nmap, superscanner, nessus népszerűvé válnak • Metasploit • john-the-ripper
2003-2004	• WiFi – aircrack, kismet – war-driving • Megszületik az OWASP • Belső tesztelés • Fenyegetettség modellezés, threat agents – a ránk leselkedő veszélyek • SDLC

Amikor az élet kezdett bonyolulttá válni

Év	Az IT biztonság világa
2005-2008	• Penteszt fázisok kezdenek elkülönülni – belső/külső – infrastruktúra/alkalmazás • Fizikai biztonság több figyelmet kap • Phishing – social engineering • Megjelenik az igény a bináris szintű alkalmazástesztelésre • Balti államokat DoS támadás éri
2009-2011	• SCADA tesztelés (2010 stuxnet) • Emberi tényező tesztelése is népszerű lesz / felhasználók továbbképzése • Input validáció még mindig probléma
2012-2013	• APT és ezekkel kapcsolatos tesztelés • Mobil alkalmazások • DDoS • Még mindig web-alkalmazáson és infrastruktúra sérülékenységen keresztül törnek be, bár az utóbbi már nem olyan gyakori

A kiber-történetek általában hosszúak…

Egy kis történelem

Számítógépes bűnözés a kezdetektől létezik, mióta számítógépet használunk, hogy elektronikusan tároljuk adatainkat.

A 60-as években a számítógépes bűnözés leginkább fizikai károkozást jelentett, bár megjelent néhány program is, melyek hasonlítottak a korai vírusokhoz.

Az első vírusnak mondható program, a Creeper, TENEX – PDP-10-en futott. A 70-es években, a hagyományos értelemben vett számítógépes bűnözés az engedély nélküli adathozzáférésen alapult.

A 80-as években, amikor a személyi számítógépek elérhetővé váltak, velük együtt a szerzői jogsértések és egyéb bűncselekmények is elterjedtek. A modemes elérés még egy kicsit megfűszerezte a lehetőségeket, a bűncselekményt már távolról is el lehetett követni.

A 90-es években a számítógépes bűncselekmények sokrétűvé váltak, így a támadási módszerek is: DoS, automatikus scannerek, key loggerek, jelszótörők, www támadások…

A XXI. század vívmányai – WAN, vezetéknélküli technológiák, mobil technológiák.

A Citibank esete

Владимир Левин a Citibank Cash Manager rendszerét támadta 1994-ben. A rendőrség elfogta és letartóztatták. A hírek szerint 10,4 millió dollárhoz fért hozzá, melyet Finnországban, Amerikában, Izraelben és Hollandiában nyitott számláira utalt át.

2005-ben megváltozott a történet, amikor ArkanoiD publikált a Provider.ru-nak.

Hozzáférés kontrollok

50 évvel ezelőtt

- Bárki futtathatott programot, akinek fizikai hozzáférése volt egy számítógép konzoljához
- MULTICS - Honeywell
- Az első, kontrollokkal kapcsolatos kérdések ma is érvényesek

  Támaszkodhatunk egy programra? Támaszkodhatunk egy fordítóra?
- DoD „Narancs könyv”-Orange book

  D (minimal protection),

  C (discretionary protection),

  B (mandatory protection) és

  A (verified protection)

Mai sztenderdek:

ISO27k1, COBIT, CIS guidelines

ENISA

Tervezés

Fizikai biztonság

Logikai biztonság

- Operációs rendszerek
- Adatbázisok – middleware
- Alkalmazások
- Hálózat

Fizikai biztonság

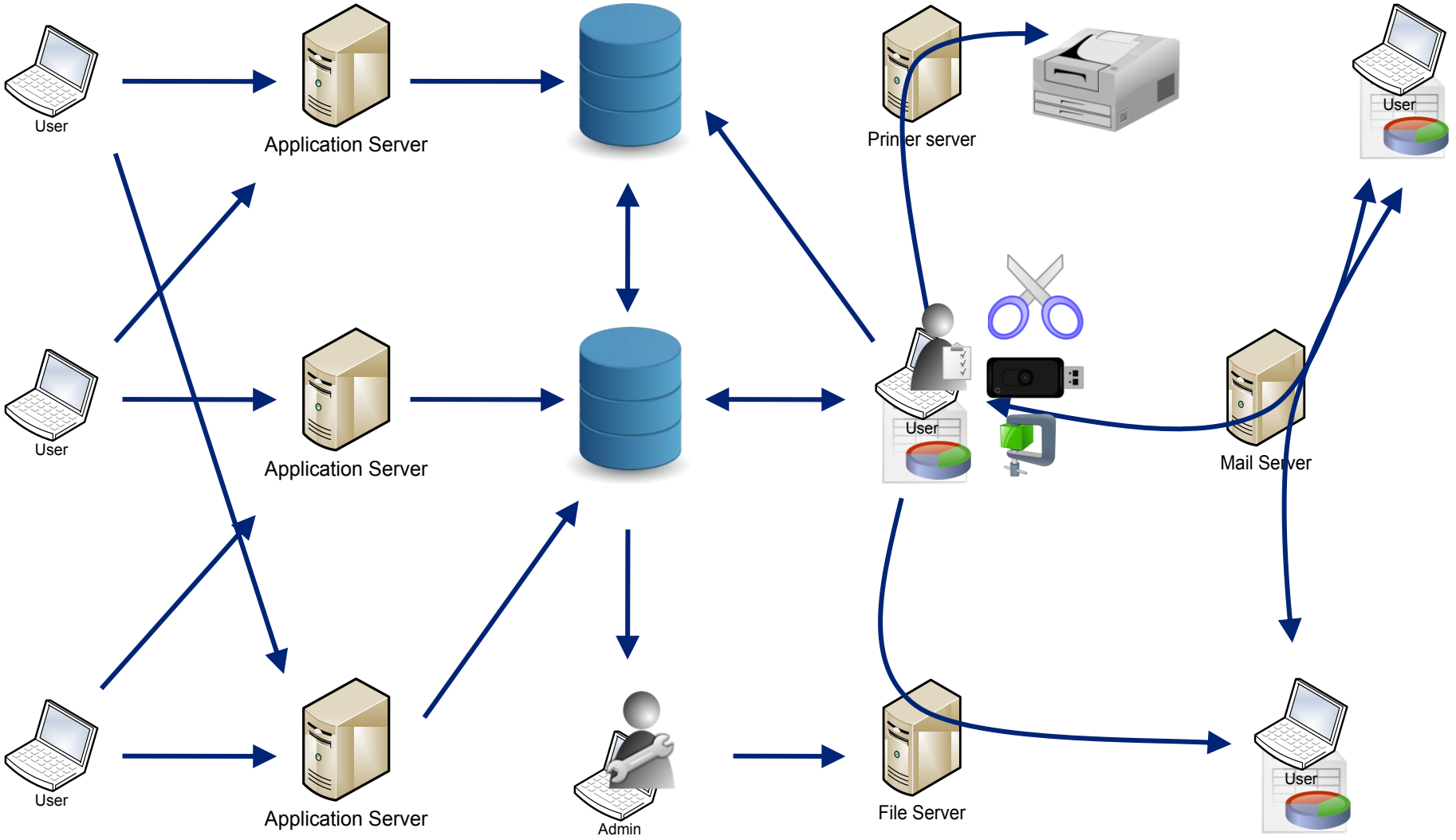
Célja a fizikai eszközök védelme, hozzáférés kontroll – csak jogosultsággal, illetve engedéllyel rendelkezők léphetnek be egy adott területre, ahol ezek az eszközök elhelyezkednek. Az információbiztonság alapköve.

Forrás: Richard Holinski


Source: Wikipedia

Adatvédelem

Hol tároljuk az adatot?



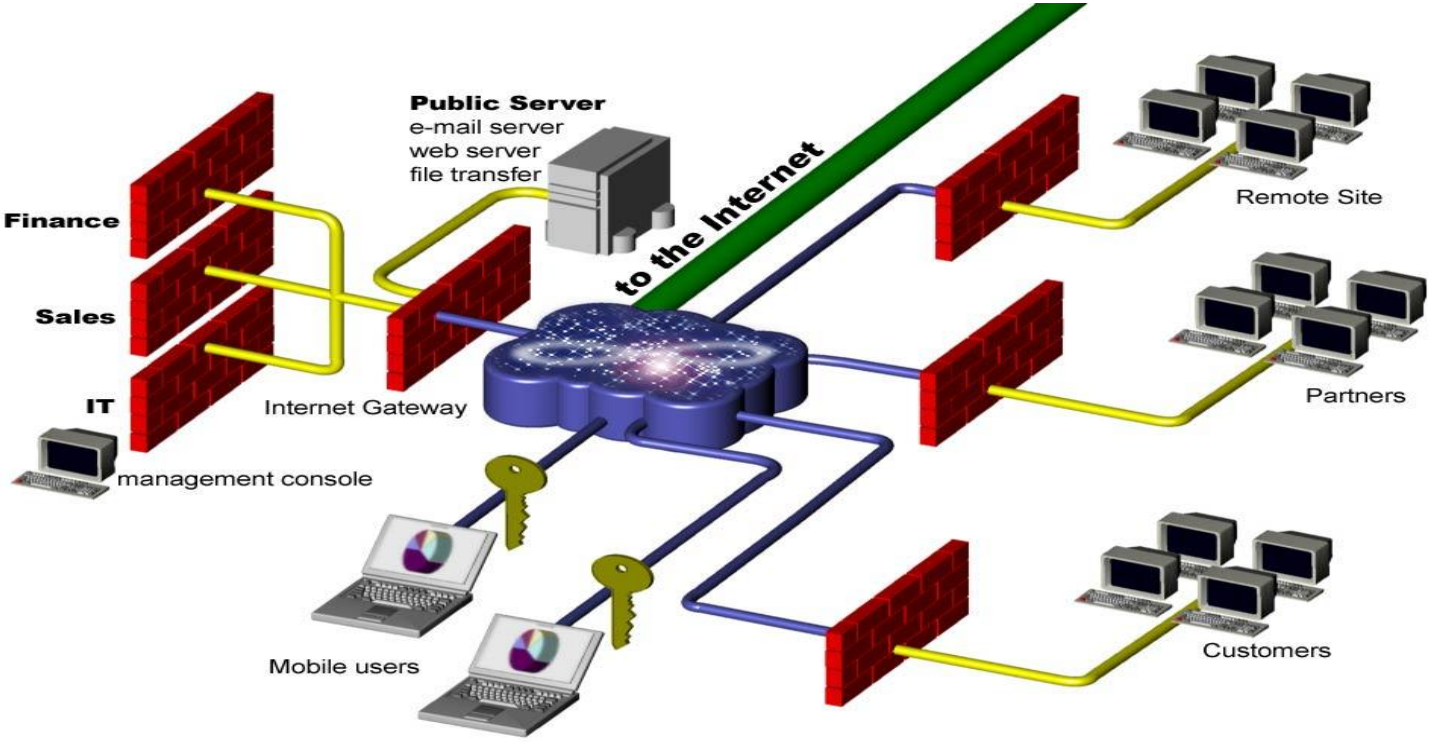
Logikai biztonság

Rendszerelemek

- A nem használt szolgáltatások/programok leállítása
- Authentikáció – Bejelentkező felhasználó azonosítása
- Authorizáció – A bejelentkezett felhasználó hozzáférés kontrollja
- Biztonsági felülvizsgálat – „hardening”
- Titkosítás használata
- Távoli elérés tiltása
- Naplózás és naplóelemzés

Amit tudni kell

Az egyik legáltalánosabb probléma még mindig az adatfolyam megértésének hiánya – az adat keletkezésétől a végpontig milyen rendszereken halad át.



Az auditor feladata

A rendszerek és adatfolyamok megértése
Milyen veszélyek fenyegetnek?
Mit akarok megvédeni?

A hagyományos hozzáférési kontrollok limitjei:
„Lemon dilemma” – hatása a biztonságra
Hiányzó incidens kezelési gyakorlat

Megoldások
Átfogó ismeretek (nem könnyű)
Az IT biztonság elismert alapszabályainak használata
Dolgozók képzése
Minőség

Mobil biztonság

Mobil biztonság

Mobil biztonság – okos telefonok, tabletek, e-könyvolvasók stb. az életünk részévé váltak. Ahogyan IT és biztonsági vezetők már tudják, a mobil technológiák olyan szintre fejlődtek, hogy vállalati dolgozók a mobilitás adta lehetőségeket a legmesszemenőbbekig használják.

A mobilitás 10 legnagyobb veszélye

- A mobil eszközök támadási felülete kicsi, de mélyre ható
- Mobil vírusok fejlődnek
- Alkalmazás boltban nem a biztonság az első
- Mobil eszközöket könnyű elhagyni, így az adatokat is
- Kié az eszköz? Kié az adat?
- Komplex adatcsatorna biztonság
- Mobil biztonsági eszközök még gyerekcipőben járnak
- Az IT-nek nem sok kontrollja van felettük
- A túl sok biztonság visszaüt
- Hiányzó szabályozásnak káosz a vége

Néhány “népszerű” mobil vírus

Vírus	Megjelenés	Platform	Terjedés	Hatás
Cabir	2004	Symbian	Bluetooth	- Lemeríti az eszközt - Megváltoztatja a háttérképet és ikonokat
Skulls	2004	Symbian	Többféle (Email, Web Sites, P2P)	- Alkalmazásokat felülír, használhatatlanná téve ezeket - Lecseréli az ikonokat a saját ikonjára (Halálfejes ikonok)
PbStealer	2005	Symbian	Többféle (Email, Web Sites, P2P)	- Kimásolja a kontaktjainkat egy szövegfájlba és átküldi az első közelben lévő eszközre Bluetoothon keresztül
RedBrowser	2006	Symbian	Többféle (Email, Web Sites, P2P)	- Az első Java-alapú mobil vírus - Számos SMS-t küld ugyanarra a számra
Ikee	2008	iPhone	Jailbreakelt eszközök, melyek SSH szerver alap-értelmezett jelszót használnak	- Az első iPhone féreg - Lecseréli a háttérképet
Zeus	2009	Többféle	Többféle	- Megpróbálja bizonyos bankok 2 faktoros authentikációját megkerülni - Megfigyeli az mTAN tartalmú SMS –eket és ezeket titokban egy távoli szerverre továbbítja
DroidDream	2011	Android	Legit alkalmazás-nak állítja be magát	- Emelt díjas SMS-eket küld - Botnet képességgel rendelkezik - További vírusokat tölt le

* A fenti táblázat csak néhány ismertebb mobil vírust mutat be. Ezekenek több változatuk van, többféle platformmal, terjedési módszerrel és hatással.

1. http://arstechnica.com/apple/news/2009/07/apple-patching-critical-sms-vulnerability-in-iphone-os.ars

Eurograbber

- A Zeus trójai variánsa
- 2012 augusztus
- Bank Info Security jelentése szerint az Eurograbber 47 millió dollárt lopott el
- Több, mint 30 000 kiskereskedelmi és vállalati számlát érint
- Nagyon kifinomult támadási módszer

APT

Történelem

- Spear phishing / Social engineering
- Trójai és malware
- Interaktív
- Állandó kapcsolat

A TeamSpy története

- Első Kaspersky TeamSpy jelentés 2013 március 20.-án
- Rejtett nemzetközi kiber-adatlopás és megfigyelés
- Cirill betűket is tartalmaz
- Cp1251 alap karakterek
- c&c domain nevek Belorusz és Ukrán hivatkozásokkal
- némelyik c&c domaint még 2004-ben regisztrálták!
- Első ismter patchelt Teamviewer 2012 májusban
- valószínűleg 2004 óta aktív, de 2008 biztos

Valóság

- Felhasználók képzése
- Fizikai biztonság ellenőrzése
- APT ellenőrzés és
- Incidens kezelési szaktudás
- Incidens kezelés – gyakorlatozás
- Pentest