Beengedjük-e a drótnélküli eszközöket a vállalati, banki környezetbe?

Dr. Szenes Katalin CISA, CISM, CGEIT, CISSP
szenes.katalin@nik.uni-obuda.hu

Óbudai Egyetem ← BMF ← Kandó
Neumann János Informatikai Kar
Alkalmazott Informatikai Intézet

kérdések

- mi az a drótnélküli átvitel?
  - az info átvitele,
  - és az átvitel jellemzői
  - az Access Point és az autentikálás
  - WEP: 💣 egyre gyorsabban megy a titkosítás feltörése
- tulajdonképpen: hány a G?
- WIMAX is dead - long? live LTE
- támadjunk bluetooth-ot:
  bluejack - how to? - eszközönként is van útmutatás
  részletes utasítás Nokia 6310-re - utcai támadás

és jöjjenek az eszközök !

kérdések

a védekező oldal lehetőségei

- drótnélküli kém eszközök - shopping indul, aztán: a védekező oldal lehetőségei
- támadás / vagy védelem - frekvencia alapon vagy lézerrel - pénzkérdés

nem fogsz mobilozni a környékemen ← fekvenciás
és a kamerákat is megtalálom ← lézeres

- de, ha bármit akarsz - frequency scanning bő választékban
  támadásra + védekezésre
  ☞ vannak hasznos szkenner kódok is

lásd:

- a rendőrségi pozitív példát
  a színek és a számok haszna,
  a fontos, és a triviális információ röviden közölhető

kérdések

- drótnélküli eszköz a munkatársainknál - veszélyes ez?
- a mobilszolgáltatók
- felhasználó vállalat: bőven vannak teendőink!
  - mégegyszer az autentikációról - kölcsönös? sőt: tanusítvány?
  - (EAP, LEAP, EAP-TLS tanusítvány - és vele a feladatok, PEAP)
- és még + teendők a vállalatnál:
  - deploy wireless - hogyan telepítünk drótnélküli hálózatot?
  - - a védelem technikai részletei

kérdések

- az intézményi "teljes" megoldás lényege ***helyi:***

  előszöris menedzsment az életciklus alatt

  - a helyi megoldáshoz szükséges információk - szervezeti pillérre
  - a számítástechnikai megoldások sikertényezői

    konfiguráció menedzsment **+** változáskezelés
  - a leltár
  - a szerepkörök és a menedzsment (≠ főnöki) feladatok

  mit kell előkészíteni? - kis szemezgetp felsorolás: 3 fólia

  ki, mit / mit, ki csináljon? no, és az auditor?

- magyarázatok
- rövidítések
- törvények
- irodalom - a kedvenc
- web címek

az információ átvitel, és ennek specifikumai

információátvitel drót nélkül: 100 ezer éve használjuk: beszélünk egymáshoz
ma:

- 0/1 bitek - jelek - adott rádiófrekvencia csatornákon mennek, a levegőben esetleg pont ott, ahol pl.
  - a mikrohullámú sütő,
  - az orvosi eszközök - ezekkel vigyázni is kell!
  - rádió, TV
  - radar, műhold
  - épületbiztonsági berendezések, vagy a garázsajtó

és persze a mobiltelefon

a jelek jellemzője: fekvencia, amplitudo
nagyobb frekvencia ➔ több adat, de rövidebb távolságra
minőség: interferencia csökkentése

de vannak korlátok: mindenki ugyanabból a rádió frekvencia készletből kaphat
mindenki ezt a spektrumot használhatja

az információ átvitel, és ennek specifikumai

a rádióhullámok 3 Hz - 300 GHz-n mennek
technológiák arra, hogy ne zavarjuk egymást: *csak vázolva!*

- CA - Collision Avoidance

adás előtt az adó belehallgat a csatorába, és akkor ad, ha az üres,vagy
egy broadcast-ot küld a drótnélküli eszköz, ezzel jelzi, hogy adni fog
erre a többi eszköz elhallgat, vagy

- CD - Collision Detection

ha két állomás úgy érzékeli, a csatornán senki nem ad, és egyszerre elkezdenek adni,
érzékelik az ütközést, felfüggesztik az adásukat

- Spread Spectrum

a rendelkezésre álló frekvenciák tovább osztása:
- az üzenet darabjai különböző frekvenciákon mennek
- különféle módokon

az Access Point és az autentikálás

AP Access Point feladata: csatlakozás

- drótos hálózathoz - LAN Ethernet
- drótnélküli hub, egy adott frekvencián, és
  ehhez csatlakoznak a drótnélküli NIC-es eszközök

távolság, frekvenciák kihasználásának módja szerint vannak:
802.11 b, a, e, f, g, h, i

- 802.11x: a hitelesítés!
  lehet EAP - Extensible Authentication Protocol, AES titkosítás

és a *kölcsönös* autentikálás!

- WEP ugyanis:

eszköz autentikál az access point-nál, de fordítva nem ➔ phreaker támogatás
mit lop? - hitelesítő infot, forgalmat

+ egyéb WEP bajok

WEP: egyre gyorsabb törés

http://www.computerworld.com/s/article/9137177/New_attack_cracks_common_Wi_Fi_encryption_in_a_minute
(és ezt 2009. 08. 27-án írták)

- az 1997-ben bevezetett WEP-et már pár év múlva meg tudták törni (statikus kulcs, nem random IV = inicializáló vektor)
- a kérdés csak az volt, hány perc kell? - eddig 12-15 perc
- de most már 1 perc is elég a japán kutatóknak

és persze a távoli bejelentkezéseknél - a titkosítás
beállítandó az összes eszközben

- WEP 64 vagy 128 bites kódolása tehát elég gyenge
- Wi-Fi Alliance a WPA2® -t fogadta el

- AES Advanced Encryption Standard titkosítás, max. 256 bites kulccsal

www.wi-fi.org

tulajdonképpen: hány a G?

a zavar egyik oka az ilyen nevek: 2G, 3G, ..., nG
(n nem feltétlenül egész szám)
1G - többnyire analógot jelöl
2G-től többnyire digitális

az érdeklődés oka: nem csak hangot viszünk át, adatot is
- de milyen gyorsan, mennyit?

jelen: mobil internetezők 3G HSPA hálózaton interneteznek
HSPA: rádiótechnikai módszerekkel átvitel növelés, latencia csökkentés
http://www.3gpp.org/HSPA

- HSDPA - High-Speed Downlink Packet Access,

új adatátviteli protokoll, már *ún*. 3.5 G, a letöltés már ADSL gyorsaságú
☎ video, zene

WIMAX is dead - long? live LTE

tavalyi WIMAX kérdések:

- nagy sávszélességű internet hozzáférés - a vezetékes, vagy a 3G versenytársa?
- WIMAX szigetszerűen a 3G-ben, vagy együttműködés?
  remélhetőleg együtt, sőt: lesz globális roaming program

remény volt: egész városra kiterjedő szélessávú összeköttetés

tavalyi helyzetjelentés:

- WIMAX szolgáltatások USA-ban, Európában
- 2001. WIMAX fórum alapítása www.wimaxforum.org
  többszáz telefonszolgáltató, részegység- és eszközgyártó taggal
  minősítés az IEEE 802.16e termékek együttműködése érdekében
  remények: a WIMAX fejlesztéseit be lehetne építeni az LTE-be?

és most: Cisco kihátrált

(de várják is még - itthon is)

WIMAX is dead -long? live LTE

google.co.uk-ba beütöm: Cisco WIMAX 2020
1.610.000 találat 0.23 mp alatt

www.wimaxforum.org: 568 telepítés,148 országban - 2010. májusi nyitás

2010. márciusban még invesztál WIMAX technológiai megoldásba
http://www.dailywireless.org/2010/03/25/cisco-invests-in-wimax-smartgrid/
de:

http://www.wimax.com/commentary/blog/blog-2010/march-2010/cisco-exits-wimax-access-business-to-focus-on-network-core-edge-0308

"Cisco Exits"
azaz:

WIMAX is dead -long? live LTE

"Cisco Exits"

- "Company confirms that it will discontinue designing and building new WiMAX base stations and will instead focus its mobility efforts on the IP core and network edge."

A vállalat megerősíti, hogy
már nem tervez új WIMAX bázisállomásokat,
nem épít,
hanem ehelyett mobilban az IP-t támogató belső, és
a hálózatok határán működő eszközökre összpontosít.

- de tovább árusítják a meglévő eszközöket, és
- támogatják vevőik meglévő hálózatát is

"but will continue shipping existing equipment and supporting existing customer networks."

WIMAX is dead -long? live **LTE**

LTE - L.T.E. of the 3rd generation radio access technology

mi is ez? májusi "szak"lapban már 4. generáció?

- indulás: 2004., elfogadott technikai specifikáció: 2007.

http://www.3gpp.org/LTE

- csomagkapcsolt kommunikációra optimalizált
  ügyes spektrumkihasználással

és most?

- T-Mobile - Ericsson mobil adatátvitelre LTE-t tesztel 2009-től
- Vodafone teszteli
- Pannon is fogja tesztelni

de drága beruházások kellenek még az LTE-hez

bluejack how to - eszközönként is van útmutatás

google.co.uk-ba beírtam: bluejacking how to - 42.700 találat, 0.59 mp alatt

http://www.bluejackq.com/how-to-bluejack.shtml

bluejack-elésre ez a legesleg weboldal:

"The world's first and most authoritative website dedicated to bluejacking"

Detailed Instructions on How to Bluejack - részletes utasítások, hogyan csináld

Please choose your phone/PDA model below for a more detailed and exact guide showing you how to bluejack with your specific device:

csak írd be, mid van:

Phones PDAs, Smartphones & Computers

Motorola A835 Palm Tungsten T / T2 Motorola E550 Sony Ericsson P800 / P900
Motorola V500/V600/v551/v547/v555 XDAII & iMate Nokia 6310 & 6310i
Any Bluetooth PC
Nokia 6600 Orange SPV C500/iMate Sony Ericsson T610/T630, Z600

bluejack how to - részletes utasítás Nokia 6310-re utcai támadás

legyen Nokia:.

Nokia 6310 / 6310i Bluejacking Guide - written by: carlidude

1. Go to Names - válaszd a Neveket
2. Select Add name - új név bevitele
3. Type your message and press OK - üzenet, és OK
4. Press OK without entering a phone number (unless you want to send one)
5. Press Done - kész
6. Go to Names- Nevek
7. Select Search- Keresés
8. Find your message - előző üzenetedet keresd ki
9. Select Details- válaszd a Részleteket
10. Select Options - Lehetőségek
11. Select Send bus. card - válaszd: Kártyaküldés
12. Select Via Bluetooth - Bluetooth-on
13. If any devices come up select them - a környék eszközeiből válassz
14. If it says Business card sent, you have just bluejacked someone
- ha elment a kártya, jó is vagy, sikerült

az utcai támadás folytatása

- létrejött egy új bejegyzés az áldozat telefonkönyvében
- ha ez rosszindulatú kód -
- program rátöltés az áldozat készülékére, vagy
- telefonkönyvének letöltése,
  a támadó pl. spoof-ol innen egy számot, és felhív arról, vagy
  az áldozattól telefonál
- vagy: feljelentkezés rosszindulatú web oldalra

- áldozat helyének bemérése GPS-sel, ha az aktív

lehet mást is csinálni: phreaker:a "megbízható" közösségi pont
imitálja a közösségi pontot, és
ezen keresztül támad

kérdés: fel merjünk-e venni idegen telefonszámot?

drótnélküli kém eszközök - shopping indul

rejtett kémeszközök

- mini kamera a gomblyukban
- lehallgatók
- felderítő eszközök

google.co.uk-ba: frequency scanner sweeper

ezt választottam:

http://www.tayx.co.uk/bug-detector/default.html

itt aztán minden van,

jönnek a modellek árral, sokszor kibocsátási dátummal

rádióhullám, vagy lézer alapúak

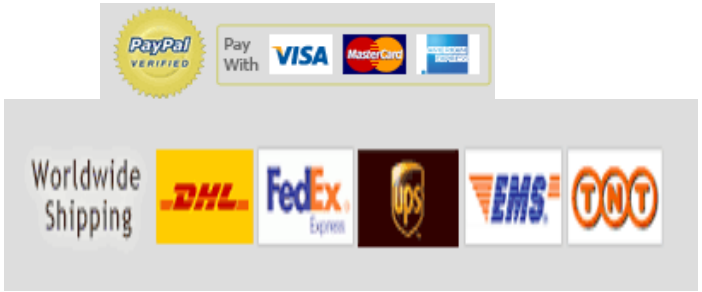
de kémeszköz is kapható

a védekező oldal lehetőségei

és a rejtett kémeszközök felderítése - mivel?
ha rádióval kémkedik - rádióhullámokkal! (de a lézer is jó valamire)
vegyünk felderítő eszközt!

milyen semlegesítő eszközt vegyünk? - ha zavarjuk a sugárzást - semlegesítjük
akár wifi, akár bluetooth - bármilyen drótnélküli jó, hiszen az is hullámmal ad

PÉNZ KÉRDÉSE CSAK



támadás / vagy védelem - frekvencia alapon

fülbe dugható kémkedő

SEH08-Wireless Spy Earpiece
Provide Covert Chat
Price US$81

és, amivel megtaláljuk

ezzel a szkennelővel megtalálhatjuk a poloskát:

- **a kém lehallgatókat**
- **a GPS/GSM alapú nyomkövetőket**
- **gomblyukban viselhető drótnélküli kamerát**

BDS20 - Bug Detector, RF Frequency Scanner

The **Bug Detector** is designed for scan and locate bug devices. The wide scanning range allows you find and sweep spy ear, listening bug, GPS/GSM tracker, wireless pinhole camera, cheat equipments etc.

Launched on Apr 05, 2008

nem fogsz mobilozni a környékemen - fekvenciás és a kamerákat is megtalálom - lézeres

zavarással blokkolja a mobilokat
ez 65$,de 130$-ért már a GPS-t is lehet

JMT-Mobile Phone Blocker
Handheld Mini Cellular Jammer
Price US$65

lézernyalábot bocsát ki,
ez verődik vissza a kamerák lencséjéről

BDS24 - Spy Camera Lens Detector

The **Spy Hidden Camera Lens Detector** uses an array of ultra bright laser lights that create a strong reflection from any kind of camera lens.

Launched on Jul 25, 2009

de, ha bármit akarsz - frequency scanning bő választékban támadásra + védekezésre

google.co.uk-ba beütöm: frequency scan, máris hozza:

frequency scanner
frequency scanners
frequency scanner software
frequency scanner online
frequency scanner interferometry (távolságmérési módszer)
frequency scanner codes - erre van egy pozitív példa, a rendőrséggel
frequency scanning
frequency scanner sweeper
frequency scanner for pc
frequency scanning plan

frequency scanner software:

7.020.000 találatom volt, 0.23 mp alatt 2010. áprilisban

a rendőrségi pozitív példa

- mi az, hogy szkenner kód?
- példa: nézzünk meg rendőrségi kódokat!
  mit tudnak a rendőrség szkennerei a Vadnyugaton?

http://www.policescannercodes.net/
ennek a rendőrségnek a szkennerei

- adókat keresnek UHF-en, VHF-en
- az üzeneteket egyenként fogadják
- egyszerre több üzenetet is tudnak küldeni
- az utasításokat szám- és színkódokkal fejezik ki - így rövid, gyors

életeket menthet!
persze nem életfontosságú üzenetek is vannak
de segít üldözni a bűnözőket

a színek és a számok - haszna

kék kód: busz, vagy taxi bajban van
piros kód: VARDA - Voice Activated Radio Dispatched Alarm
rádiós hangriasztás
bíbor kód: gengszter tevékenység

bűnöző felugrik a villamosra ➔veszélyben az utasok
és ekkor szól a rendőr az autóból: kék kód van

haszon:

- gyors jelentés
- gyors reagálás
- kívülállóknak a tartalom - valamennyire - rejtett

pl. ha lehallgatásról tudnak, jelzik: kívülálló figyeli a rádiót, használj telefont:
11-58, radio monitored, use phone

a színek és a számok - a fontos, és a triviális

- code 2 - sürgős, fény-, hangjelzés nélkül
- code 3 - használj fény-,és hangjelzést
- code 6 - ne gyere be a körzetbe

- code 7 - étkezési szünet
- code 9 - nyári egyenruha
- code 37 - személy / tulajdon körözése

187 öngyilkosság
207 emberrablás
207A emberrablási kísérlet
211 rablás
211A rablási riasztás
211S csendes rablási riasztás

de van még:
ember puskával, késsel, erőszak, erőszak kísérlet, részeg, stb.

drótnélküli eszköz a munkatársainknál - veszélyes?

tavaly már volt:

- milyen drótnélküli eszközökkel
- milyen hálózati eléréssel
- milyen fontos adatok veszélyeztetettek az eszközön + ! rajta keresztül is!

a támadók

kik ● honnan ● miért ● hogyan

- cégből belülről,
- mobilszolgáltatón át,
- magát az eszközt /
- csak az eszközön keresztül
- bárhonnan

lehallgat, spoof-ol, hamisít, ellop, stb.

mi a helyzet a mobilszolgáltatóknál?

náluk tavaly már védekeztünk

mit kell teljesíteniök?

- rendelkezésre állás, bizalmasság, integritás
- funkcionalitás, dokumentáció

a szolgáltató core rendszere

- példa: esetem a számlavezetőjükkel

hogyan támogathatják / támogatják a mobilszolgáltatók a követelmények teljesítését?

autentikáció - persze, az eszközé - SIM kártya, PIN, PUK kódok
működésükre vonatkozó követelmények meghatározása
az infrastruktúrájuk érzékeny pontjainak meghatározása, védelme
érzékeny adatok lelőhelyének meghatározása, védelme
szolgáltatás minőségi követelmények

felhasználó vállalat:
bőven vannak teendőink! - mégegyszer az autentikációról

nem ússzuk meg a helyi intézkedéseket !

a megoldás a felügyelt, menedzselt használat lesz - idén erre összpontosítsunk!

mégegyszer az autentikációról - jön az eszköz, de hogyan?

az autentikálás tehát legyen kölcsönös - EAP

+ amit csak lehet:

jelszó, token, egyszeri jelszó, tanusítvány, smart card, Kerberos

egy Cisco módszer: jelszó alapú autentikáció - LEAP

Lightweight Extensible Authentication Protocol

itt az autentikálás mindenesetre kölcsönös

más: tanusítványos autentikálás EAP - TLS (Transport Layer Security)

de:

felhasználó vállalatnál: és még + teendők!

problémák a tanusítvánnyal:

- ehhez programozni kell az eszközt, rá kell tenni a tanusítványt valahogy
- a tanusítványokat nyilván kell tartani
- CRL (Certification Revocation List) kezelése
- (jöhet kalóz AP vagy autentikációs szerver is jó tanusítvánnyal)
- a szállítók meg kell feleljenek
- mi is bele kell tanuljunk
- csak ezért senki nem fog PKI infrastruktúrát építeni

lehet esetleg PEAP - Protective EAP

- itt csak a szerver használ tanusítványt

és ez még mindig nem elég!

mire figyeljünk drótnélküli hálózat telepítésekor?
a védelem technikai részletei

1. AP: SSID default értékének megváltoztatása
2. broadcast letiltása
3. engedélyezett MAC címek, szűrés beállítása
   bár persze spoof-olható, cleartext-ben közlekedik

4. legalább 802.11i -eszközök legyenek - mármint, ha lehet

5. dönteni az IP címzésről (statikus, és disable DHCP - kis hálózat)
   DHCP - a csatlakozó gép mindjárt kap egy érvényes címet
6. autentikáció kiválasztása - lehetőleg kölcsönös
7. titkosítás kiválasztása - lehetőleg
   ne ugyanazzal a kulccsal, mint a hitelesítés - ahogy a WEP
   és ne mindegyik kliensnek ugyanaz a kulcs (bár ez macera)

de: bármiféle titkosítás, szűrés csökkenti az átviteli sebességet

mire figyeljünk drótnélküli hálózat telepítésekor?
a védelem technikai részletei

8. a hálózat hatókörét korlátozzuk az épületre
   - középre,
   - festék
9. távoli eléréshez
   - 802 11.x RADIUS vagy TACACS
   - legyen titkosított a kommunikáció
10. az AP a támadó kitűnő belépési pontja, ezért:
   - a drótos és a drótnélküli hálózat elválasztása tűzfallal
   - AP és drótos hálózati kommunikáció közé IDS
11. betörési teszt
   - AP azonosítás próba
   - titkosítás feltörése

mindez nem pótolja a szervezettséget!

az intézményi "teljes" megoldás helyi:
először menedzsment az egész életciklus alatt

tervezett, dokumentált, ellenőrzött feladatlista:

ki - mikor - milyen rendszerességgel - miért - mit - részeredmény / bármi kézzel fogható

ellenőrzés: **- " -**

tavaly: tárgyaltuk az indítási stratégiát

miért akarunk drótnélküli eszközöket, mire akarjuk használtatni

kiknek, milyen feladatait akarjuk támogatni

- ➔ *milyen* eszközök,
- ➔ *mi* a helyük a cég infrastruktúrájában
- ➔ *melyik* szervezeti egységnek *mi* lesz ezzel a feladata

érdemes még cizellálni

szükséges:

feladatok - végrehajtók - ellenőrzők 1-1 értelmű egymáshoz rendelése

mit kell tudnunk a feladatokról?

a helyi megoldáshoz szükséges információk

az informatikai biztonság szerevzeti pilléréhez:

feladatokhoz meg kell adni:

- mit
- miért
- mikor - mikorra
- milyen rendszerességgel
- mi a kézzelfogható eredmény, és

- annak milyen - lehetőleg

konkrét,

számszerű,

de mindenesetre mérhető

- jellemzői kell legyenek a teljesítés elbírálhatóságához

a feladatok - végrehajtók - ellenőrzők egymáshoz rendelését ez segíti

számítástechnikai megoldások sikertényezői
konfiguráció menedzsment + változáskezelés

mindenfajta számítástechnikai eszköznél

➔ **drótnélkülieknél is!**

alapvető **siker** tényező:

Dwayne Melancon: Security Controls That Work
IS Control Journal, 2007

felkészülés:
konfiguráció menedzsmentre
változáskezelésre

➔ ehhez leltár kell!

és, ha az infrastruktúráról bármit ki akarunk deríteni - a leltár, az mindig kell

a leltár

mi mindent kell nyilvántartani
modell jelzés

- sorozatszám
- firmware verzió
- operációs rendszer verzió
- kódok - de: adatvédelmi törvényt betartva
- memóriakártyák
- adapterek
- stb.?

és ki fogja ezeket az adatokat feltölteni / karbantartani
felhasználó?
flottamenedzser?
és ki ellenőrzi mindezt?

és minek a nyilvántartásával vigyázzunk? - pl. tudható, hol van a felhasználó
ismét: adatvédelem

a szerepkörök és a menedzsment feladatok / miket készítünk elő

- célok meghatározása
- alapvető szabályok meghatározása
  ne legyen sok szabályzat ➔ nem kell új, de legyen közös fogalomjegyzék
  ne legyen ellentmondás, de tartsa a kapcsolatot a már meglévő szabályzatokkal
- követendő szabványok kiválasztása

és ezután:

- jogosultságkezelésbe illesztés
- legyen-e lehetőség, pl. egy web-es felület, amiről
  a felhasználó adminisztratív feladatokat láthat el? (pl. letöltés, jelszókezelés)
- lesz-e adatmentés? és hova? központi helyre?
- letöltések szabályozása (javítás, továbbfejlesztés, hobby)
- hogyan lesz a felhasználói támogatás?
- mibe lehet beletúrni - pl. megengedjük-e a képernyő átvételét?

és még ez sem elég:

a szerepkörök és a menedzsment feladatok / miket készítünk elő

- titkosítás rendje
- tudjon-e a cég a tárolt üzleti adatokról? és hogyan?
- tudjon-e a cég arról, hol van épp a user?
- mobil eszköz átadás / átvételi rendjének kialakítása
- az eszköz és kapcsolatainak (?) karbantartása
- üzem közbeni felügyelet, úgymint
  - logolás,
  - incidensek kezelése,
  - helpdesk
  - vírusirtás,
  - patch-elés,
  - letöltések,
  - bekapcsoláskor aktivizálandó lehetőségek,
  - . . .

a szerepkörök és a menedzsment feladatok / miket készítünk elő

- visszavonások kilépéskor:
  jogok / lehetőségek felfüggesztése
  / törlése
  visszavételi rend - akár elavulás miatt is
  az eszköz újra felhasználása, átadása más munkatársnak

- elvesztésre reagálás megtervezése - ne legyen büntetés, jobb, ha rögtön kiderül!
  felkészülés: tartalom titkosítás / törlés, jelszó

a szerepkörök és a menedzsment feladatok - ki, mit / mit, ki csináljon?

beszerzés (tender, flotta, ...)	beszerzési részleg vagy: flottamenedzser?
beállítások átadás előtt regisztrálás	flottamenedzser -"-
jogosultságkezelés	helpdesk + informatikai biztonság?
jelszóváltoztatás • kezdetben • később	flottamenedzser? felhasználó?
adat áttöltés - pl. készülékváltáskor	flottamanedzser? helpdesk? felhasználó - és kérjen engedélyt, vagy?

a szerepkörök és a menedzsment feladatok - ki, mit / mit, ki csináljon?

SW csomag letöltés • továbbfejlesztés • hibajavítás	flottamanedzser? helpdesk? felhasználó - és kérjen engedélyt, vagy?
más letöltés - ha szabad	felhasználó - engedéllyel?
szinkronizáció a felhasználó asztali gépével	felhasználó
problémakezelés	helpdesk? flottamenedzser?
elvész, vagy ellopják - távoli adattörlés	helpdesk? flottamenedzser? informatikai biztonság?

és mit csináljon az auditor?

vizsgálja a

- szabályozottságot
- dokumentáltságot !
- sérülékenységi helyzetet

  mint pl.?
  - Access Point beállításai
  - adatáramlások felderíthetősége - titkosítás
- rendelkezésre állás - pl. zajvédelem (interferencia), frekvenciaválasztás
- távmenedzsment kérdések megoldását
  - felhasználók támogatása
  - de: magánéletük tiszteletben tartása - hiszen használati adatokat gyűjtenek róluk
  - adatforgalom / eszközök védelme, és
  - az erre felhasznált eszközök, azok beállításai, stb.

általában:

- mit naplóz, kicsoda, és ki ellenőrzi?

magyarázatok

www.cellular.co.za/technologies/3g/3g.htm nyomán:

3G - 3. generáció

mobil technológiák összefoglaló neve, 2001 végétől, nagysebességű internet, adat, video, CD-minúségű zeneszolgáltatásra, [így] legalább 2 Megabit / sec

hálózat - kézi készülék - bázis állomás -switch - stb. segítségével

CDMA - Code Division Multiple Access - digitális wireless technológia,

amely lehetővé teszi, hogy több user használja ugyanazt a frekvenciát,

interferencia nélkül, a hívás egy egyedi kódot kap, ami a többitől megkülönbözteti

CDMA2000 - CDMA upgrade

UMTS - W-CDMA - Wideband CDMA neve Európában

UMTS: Universal Mobile Telecommunications System

rövidítések

FDDI - Fiber Distributed Data Interface

CSMA - Carrier-Sense Multiple Access

- CSMA/CD CSMA with Collision Detection
- CSMA/CA CSMA with Collision Avoidance

FHSS - Frequency Hopping Spread Spectrum

DSSS - Direct Sequence Spread Spectrum

OFDM - Orthogonal Frequency Division Multiplexing

törvények

Adatvédelmi törvény:

a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról szóló 1992. évi LXIII. törvény.

- pénzügyi szervezetekre 2004-től hatályos kiegészítéssel:

2003. évi XLVIII. törvény

a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról szóló 1992. évi LXIII. törvény módosításáról

irodalom

a kedvenc, mindig idézett

Dwayne Melancon: Security Controls That Work
IS Control Journal, Vol. 4, 2007
pp. 29-32

ITPI - IT Process Institute
http://www.itpi.org/home/default.php

IT Controls Performance Benchmark - the present:
http://www.itpi.org/home/controls_benchmark.php
(12 March, 2010)

web címek

és mikor láttam ezeket?

http://www.computerworld.com/s/article/9137177/New_attack_cracks_common_Wi_Fi_encryption_in_a_minute

ez az info 2009. 08. 27-án keletkezett - 2010.04.08.

a szövetség: www.wi-fi.org - 2010.05.27.

http://www.3gpp.org/HSPA - 2010.04.28

www.wimaxforum.org - 2010.05.27.

http://www.dailywireless.org/2010/03/25/cisco-invests-in-wimax-smartgrid/ -2010.04.08.

http://www.wimax.com/commentary/blog/blog-2010/march-2010/cisco-exits-wimax-access-business-to-focus-on-network-core-edge-0308 - 2010.04.08.

http://www.3gpp.org/LTE - 2010.04.28.

web címek

http://www.bluejackq.com/how-to-bluejack.shtml - 2010.04.02.

http://www.tayx.co.uk/bug-detector/default.html - 2010.04.02.

http://www.policescannercodes.net/ - 2010.04.12.