Az intézményi hálózatok biztonsága - és ehhez még wireless eszközök?

Követelmények a mobilszolgáltatástól
a vállalati hálózaton át
a végfelhasználó készülékéig

Dr. Szenes Katalin CISA, CISM, CGEIT
szenes.katalin@nik.bmf.hu

Budapesti Műszaki Főiskola
Neumann János Informatikai Kar
Alkalmazott Informatikai Intézet

intézményi (hálózat)biztonság - drótnélküli veszélyek - teeendők

kérdés: mely 2 pont között nincs kábel? (mindenki telefonál)

- mi ez a drótnélküli? kinek engedelmeskedik? testületek, szövetségek
- pro és contra - jó-e, vagy nem jó a wireless?
- támadás - I.
- veszélyek
- specifikus veszélyekhez védelmi lehetőségek

a védekezés KÖZÖS alapelvei - ISACA - ISO, összevetés (+CRM2009)

- ➔ min múlik a védelem a mobilszolgáltatónál
- védekezési stratégia:
  - az előfizető bejelentkezésének védelme
  - ISACA - COBIT, ISO
- a szolgáltató infrastruktúrája
- + milyen érzékeny adatokat kell védeni?
- a szolgáltatásból eredő követelmények

intézményi (hálózat)biztonság - drótnélküli veszélyek - teeendők

mi a baj az elektronikus szolgáltatást nyújtó partnercégeknél? - APACS

➔ védelem a partnercégnél

- védekezési stratégiák
- egyszerűsített példa hálózat, biztonsági elemekkel
  - hagyományos hálózati veszélyek nagyjából kivédve?
  - ha ez bank - használjuk-e az elektronikus csatornáit?
- példa egy szállítói védelmi javaslatra
- tervezett felkészülés - felmérés, feladatok
- indítási stratégia elkészítése
- üzem közbeni felügyelet

- magyarázatok

mi ez a drótnélküli? kinek engedelmeskedik? IEEE, Wi-Fi Alliance

- a 0/1 bitek - jelek - adott rádiófrekvencia csatornákon mennek, a levegőben esetleg pont ott, ahol pl. a mikrohullámú sütő, vagy az orvosi eszközök
- 1999: drótnélküli hálózat szabvány, IEEE 802.11/b Wi-Fi - Wireless Fidelity
- 2003: nagysebességű kiterjesztés: 11/g, most 802.11 b/g
- *hol tartunk most?*
  http://grouper.ieee.org/groups/802/11/index.html
  legfrissebb anyag (2009.05.26-án):
  Wireless LAN Medium Access Control (MAC) and
  Physical Layer (PHY) Specifications - munkaanyag,
  ...rögzített, hordozható és mozgó állomások drótnélküli kapcsolata ...
- szintén 1999: a WLAN termékszállítók, termékeik együttműködése érdekében, megalapítják a Wi-Fi Alliance-t, ez a tagoknak product certification-t ad ki
- www.wi-fi.org tagja "minden" telefontársaság és gyártó, most 20 PageDown-nyi
- 2003: hotspot-ok certification-ja
  hotspot: WLAN hozzáférés közösségi helyekről - szálloda, repülőtér
- *hol tartunk most?*
  2009.05.19.: WiFi Alliance kiterjesztette a WPA2®-t (Wi-Fi Protected Access)

mi ez a drótnélküli? kinek engedelmeskedik? WIMAX, LTE

WIMAX
- nagy sávszélességű internet hozzáférés - a vezetékes, vagy a 3g versenytársa?
- WIMAX szigetszerűen a 3g-ben, vagy együttműködés?
  remélhetőleg együtt, sőt: lesz globális roaming program
- USA WIMAX szolgáltatás: 2.5 gigahertz, Hollandia: 3.5 gigahertz
- *hol tartunk most?*
  2001. WIMAX fórum alapítása www.wimaxforum.org
  több, mint 500 telefonszolgáltató, részegység- és eszközgyártó taggal
  minősítés az IEEE 802.16e termékek együttműködése érdekében
  bázisállomások, PC kártyák, USB modemek, stb.

LTE
- a következő lépés a mobil rádióhullámú kommunikációban
  LTE: 3GPP Long Term Evolution - 3rd Generation Partnership Project
- www.3gpp.org - szélessávú mobil kommunikáció szabványai megalkotására
  1998-ban! ETSI és egyéb szervezetek vannak benne
- remények: a WIMAX fejlesztéseit be lehetne építeni az LTE-be?

pro és contra - jó-e, vagy nem jó, ha drótnélküli eszközöket használunk? - PRO

- *előre* visz, új üzleti lehetőség, presztizs - merthogy tudjuk ezt is kezelni
  - a mobil terjed, képességei bővülnek
- az intézmény folyamatos működését támogathatja
  - kritikus rendszerek elérhetősége pl. i-bank
  - földrajzi függetlenség - mozoghatunk a "terminállal"
    - vevőink
    - szállítóink
    - munkatársaink elérik a vállalati hálózatot + internetet is
  - esetleges tartalék összeköttetési lehetőség
- telepítési rugalmasság
  - nem kell kábelezni

USA-ban gyakori belső WLAN is már, Magyarországon inkább levelezés, de ***okkal!***

pro és contra - jó-e, vagy nem jó, ha drótnélküli eszközöket használunk? - CON

- *bizalmas* adat kikerül az intézményi védelem hatóköréből a levegőbe
  - az adat eddig többnyire belül maradt, csak távolról nyúltak bele
  - a felelősség bent maradt, HA ügyesek voltunk
  - "elég" volt a hozzáférési utat biztonságossá tenni
- adat eddiginél könnyebben kerülhet ki - úgy tűnik, de ez igaz is
  - lehallgatás - ÜZLETI, SZEMÉLYES ADATOK
  - könnyebben kerül kártevő az eszközre, és irányítását átveszi
    - vírus, féreg, trójai
- rendelkezésre állási hiányosságok
  - sávszélesség
  - interferencia
- könnyebben ellopják, mint egy - nagyobb - számítógépet
- követhetetlen, nagy roaming díjak
  - meglepetés - drága használat

támadás - I.

- a támadók - kik?
  - alkalmazott
  - partner
    - szerződő fél: vevő, szállító
  - versenytárs
  - hacker, cracker, diák,
  - bűnöző, kém, ügynök, terrorista

haszon
tudatlanság
rosszindulat
szórakozás

- honnan jön a támadás, és mit támad?
  - a "sávos" "levegőből"
  - vállalati hálózatot
    - kívülről: war driving, war chalking
    - belülről
  - valamelyik mobil szolgáltató hálózatatát
  - magát a mobil eszközt, vagy rajta keresztül

veszélyek

minden, ami a vezetékes hálózatra veszélyes + a speciális architektúrából eredők

általános példák
- lehallgatás
- IP cím spoofing - hamisítás
- smurf
- teardrop
- vírusok, férgek, trójaiak, stb.,

speciális példák
- signaling channel DOS attack
- silent SMS DOS attack
- az eszköz elvesztése, ellopása
- egészségkárosító hatás? számtalan kutatás szerint mégse
- (használata elterelheti a figyelmet)

veszély - signaling channel DOS attack / védelmi lehetőség

- signaling channel DOS attack
  drótnélküli esetben, pl. a jelenlegi 3G szabványoknál
  sokkal több jeladó üzenet / handshake kell, mint vezetékesnél
  CDMA2000 vagy UMTS szabványon alapuló 3G hálózatokra:
  a 3G hálózat "vezérlését" terheli túl, ritka, és kicsi csomagokkal egyre újabb rádiócsatorna létrehozására készteti a hálózatot, így jelentős teljesítményvisszaesés, de még az eszközöknek is árt
  mivel ritkák és kicsik a csomagok, az intrusion detection eszközök nem veszik észre, hiszen azok pont a nagy forgalomra vannak kihegyezve

lehetséges megoldás pl.:
Lee, Bu, Woo: On the Detection of Signaling Wireless Attack on 3G Wireless Networks
kb. 2006., http://www.cse.cuhk.edu.hk/

forgalom monitorozás - az eredmény satatisztikai módszeren alapuló feldolgozása

Dr. Szenes *wireless veszélyek, követelmények* 10

veszély - Smurf attack / védelmi lehetőség

- Smurf attack
  a támadó sok ICMP csomagot küld a megtámadott hálózatba, a csomagok az áldozat gép hamisított címét tartalmazzák. Broadcast az üzenet
  Ha a router rosszul van konfigurálva, vagy gyenge minőségű, kiengedi a válaszokat, amelzeket mind az áldozat számítógép kap meg, és összeomlik a forgalomtól

védelem lehet:
a hálózati elemek monitorozásában adatbányászati módszerek alkalmazása

Shwe, Lee, Lee: DOS Attack Mining in Sensor Node Replacement
2007.
www.springerlink.com

Dr. Szenes *wireless veszélyek, követelmények* 11

veszély - silent SMS DOS attack / védelmi lehetőség

- silent SMS DOS attack

silent SMS: pl. rendőrségicéllal, az eszköz helymeghatározására
a képernyőn nem íródik ki, hangjelzést nem ad, így maga a támadás észrevehetetlen
a GSM architektúra lehetővé teszi, hogy tömeges SMS-t küldjenek a hálózatba az SMS Mobile Switching Centre-n keresztül
silent SMS is küldhető, protokoll manipulálással

védelemről:
Croft, Olivier: A Silent SMS Denial of Service DOS Attack
kb. 2007.,
http://mo.co.za

Dr. Szenes *wireless veszélyek, követelmények* 12

veszély - teardrop / védelmi lehetőség

Teardrop:
Olyan DOS támadás, amikor fragmentált csomagokat úgy hamisítanak, hogy átfedjék egymást akkor, amikor a fogadó host megpróbálja őket összerakni

védelem reménye lehet wireless esetben:
a neurális hálón alapuló IDS:

Liu, Tian, Wei:
A Wireless Intrusion Detection Method based on Neural Network
www.actapress.com
2006.

a védekezés szolgáltatóra és partnerre is KÖZÖS alapelvei - ISACA - ISO
ne csak védjünk, javítsunk is !

kiindulópont az informataikai biztonságban mindig: a stratégiai célok
ebből lesznek a generikus ellenőrzési célok

3(+2) - ISO (emlékszünk a CRAMM-ra?) és ISACA és COBIT:
- ☹ **rendelkezésre állás, bizalmasság, integritás**
- ☺ mi a **plusz 2**? a funkcionaitás és a dokumentáció - és miért?

- !! sérülékenységmentes(ebb) alkalmazások fejlesztése:
  ISO/IEC 12207:1995 nemzetközi szabvány - MSZ ISO/IEC 12207 2000. május

COBIT + ISO egyaránt
- üzletmenetfolytonosság
- infrastruktúrális elem (asset) menedzsment - konfigurációkezelés
- változáskezelés - ∀-re, fejlesztésre, infratsuktúrára is !
- ! stb. !

COBIT + ISO - de COBIT tárgyszerűbb:
- COBIT 4 (4.0, 4.1) ISO 17799 - 27002, 27001

ISO / COBIT - 1.

ISO 27001	COBIT 4.1
A.6.1.4 : Authorization process for information processing facilities	DS5.3 Identity Management, DS5.4 User Account Management
A.6.2.1:Identification of risks related to external parties, A.6.2.3: Addressing security in third party agreement	DS2 Manage Third-party Services (13 detailed ...)
A.8.1.1: Roles and responsibilities A.8.2.1 : Management responsibilities	PO4.6 Establishment of Roles and Responsibilities, PO4.8 Responsibility for Risk, Security and Compliance, ...!

ISO / COBIT - 2. szükség volt a CISA Review Manual-re!

ISO 27001	COBIT 4.1
... 3) Explanation: The term 'owner' identifies an individual or entity that has approved management responsibility ...	PO2.3 Data Classification Scheme: ... criticality and sensitivity, ... include details about data ownership; ... PO4.9 Data and System Ownership
A.10.1.3 : Segregation of duties	PO4.11 Segregation of Duties
A.11.7 Mobile computing and teleworking Objective: To ensure information security when using mobile computing and teleworking facilities.	**CRM** 5.4.3 Wireless Security Threats and Risk Mitigation 5.3.7... Access Issues With Mobile Technology ...

védekezési stratégiák - a mobilszolgáltatónál

- előfizető bejelentkezésének védelme:
  - autentikáció
  - csak regisztrált előfizetők fogadása
    (IMSI - International Mobile Subscriber Identity) tárolás a SIM kártyán
    de a SIM kártya másolható
  - PIN, PUK kódok

infrastruktúrára:
- a szolgáltatói hálózat elemeire
- érzékeny adatbázisokra

egész működésre
betartandóak:
védelmi követelmények: ISO, ISACA - COBIT
➔ a 3 + 2 ellenőrzési cél érdekében,
➔ megakadályozó, vizsgálati, javító ellenőrzési intézkedések

a mobilszolgáltató infrastruktúrája

tipikus 3G infrastruktúra - UMTS (vagy CDMA)
1
UTRAN - UMTS Terrestrial Radio Access Network
az előfizetőt a szolgáltató "forgalmi" hálózatához köti
(energiaellátás, erőforráskezelés, készülék helymeghatározás támogatás ...)
2
"forgalmi" hálózat - összekötés (bázisállomások, stb. segítségével):
- az UTRAN és a szolgáltató belső hálózata
- az internet és a szolgáltató
- távközlési, illetve más mobilszolgáltatók között

itt elérhető érzékeny adat: a kommunikáció és az előfizetők adatai
3
belső hálózat
mint egy vállalat, de speciális **. / .** úgymint

a mobilszolgáltató belső hálózata
+ milyen érzékeny adatokat kell védeni?

3. a belső hálózat
legfontosabb érzékeny elemei:
- o számlázó rendszer
- o CDR (Call Detail Record) feldolgozások
- o vevőszolgálat
- o adattárház
- o csalásfelderítés
- o vállalati működéstámogatás - a szokásos vállalati információs rendszer

érzékeny adatok = **üzleti** titkok + **előfizetői** adatok
- o személyi ill. a szerződő vállalat adatai, szolgáltatásszerződési adatok
- o forgalmi, számlázási
- o hol van éppen az egyén
- o szent : CDR
- o plusz: a dolgozóknak is vannak személyi adatai!

a szolgáltatásból eredő követelmények a mobilszolgáltatóra

a szolgáltatásból eredő követelmények:
- o a legtöbb alkalmazás és szolgáltatás időérzékeny
- o tárolási követelmények - idő, bizalmasság
- o adat**ki**szolgáltatási követelmények
- o Európai Úniós, és
- o hazai követelmények

pech: Személyi adatok védelme ☝ terroristák elleni harcnak ellentmond
(1992. évi LXIII. törvény, 2003. évi XLVIII. törvény)

és mi a baj azoknál a partnercégeknél,
amelyek az elektronikus szolgáltatásokat akarják nyújtani?

Colin Whittaker, biztonsági vezető, APACS
UK Payments Association - bankok és egyéb pénzügyi szervezetek szövetsége
CERT konferencia, 2008.

az elektronikus bűnözés elleni védekezés nehézségei:
- O a támadók, eszközeik, technikájuk, szervezetők, kommunikációjuk nehezen fel- és ismerhetőek
- O a vevőket és a külső környezetet támadják, így a bank erre nehezen reagál
- O mind a vevők, mind a személyzet nehezen ismeri el, ha hibázik (információt ad ki, fertőzés, stb.)
- O a veszélyek, illetve a támadások hatásainak átfogóképét nehéz megalkotni
- O az állami szervekkel elégtelen együttműködés az információgyűjtésben, és megosztásában
- O az ilyen incidensek kezelése időbe (és persze pénzbe) kerül, és speciális szakismeretet igényel

védekezési stratégiák - a partnercégnél

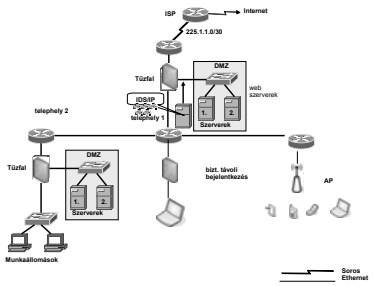
➔ védelem a partnercégnél

- egyszerűsített hálózat, biztonsági elemekkel
  - hagyományos hálózati veszélyek nagyjából kivédve?
  - ha ez bank - használjuk-e az elektronikus csatornáit?
- példa egy szállítói védelmi javaslatra
- tervezett felkészülés
- indítási stratégia elkészítése
- üzem közbeni felügyelet

váltások esetén:

- kivezetés (egyénenként / mobilszolgáltatónként)

védelem a partnercégnél - egyszerűsített példa hálózat, biztonsági elemekkel
hagyományos hálózati veszélyek nagyjából kivédve?
ha ez bank - használjuk-e az elektronikus csatornáit?



Cisco Adaptive Wireless Intrusion Prevention System
védelem a partnervállalatnál - a szállító javaslata ideális védelemre - mi legyen?

http://www.cisco.com/en/US/prod/collateral/wireless/ps9733/ps9817/data_sheet_c78-501388.html
2009.05.26.

Tervezett felkészülés - FEL KELL MÉRNI:
∑ milyen eszköz, milyen hálózati elérés, milyen fontos adat?

eszközfajták	hálózati elérés	milyen fontos adat(rajta/elérh.)
mobiltelefon	Bluetooth (pár m)	személyes adatok, pl.
intelligens telefon	WLAN-ok	telefonjegyzék
pendrive	WAN: 3G, GPRS,...	naptár
zenelejátszó		kódok, jelszavak esetleg
	otthon:	intézményi adatok, pl.
egyéb USB portba	ált. tűzfallal	- vevők adatai
dugható	egybeépített router	- munkatársak adatai
	vezetékes / WIFI	- üzleti titkok, pl. prezi
palmtop	kliensekkel	
laptop	a router-ben kell	intézményi adatokhoz
	állítani a titkosítást	jutás lehetősége

Tervezett felkészülés - informatikai és informatikai biztonsági feladatok

- tervezés & kiválasztás
  - plusz infrastruktúrális elemek megtervezése, kiválasztása, meglévők esetleges átalakítása
  - a technológiai követelmények ÉS következmények figyelembe vételével pl. eszköz operációs rendszerének (Windows, Symbian, Palm,...) kitettsége, kapcsolatok blokkolása (Bluetooth)
- beszerzés (tender, flotta, ...)
- mobil eszköz átadás / átvételi rendjének kialakítása
- jogosultság tervezés
- üzem közbeni felügyelet
- védelmi berendezések, beállítások, módszerek, stb.
  - a cég hálózatában és számítástechnikai berendezésein
  - a mobil eszközökön

  (vírusirtó, patch-elés, bekapcsoláskor aktivizálandó lehetőségek, ...)
- elvesztésre reagálás megtervezése - ne legyen büntetés, jobb, ha rögtön kiderül!

indítási stratégia elkészítése

az indítási stratégia fő elemei:

célmeghatározás - ∀ ebből következik

➔ a felső vezetés céljai: ISACA, ISO
➔ kinek, milyen fajta eszközt akarunk biztosítani?
➔ ez a vállalati hálózatban mely infrastruktúrális elemeket
  - igényli
  - érinti

➔ követelmények meghatározása:
  - üzleti felhasználó
  - informatikai szervezet
  - informatikai biztonság
  - egyéb külső / belső támogató szervezeti egységek

üzem közbeni felügyelet

- mobil eszköz átadás / átvétele
- jogosultság menedzsment
- védelmi berendezések üzemeltetése
- logolás
- incidensekre reagálás
- a mobileszköz menedzselése
  - beállítás átadás előtt
    (vírusirtó, patch-elés, bekapcsoláskor aktivizálandó lehetőségek, ...)
  - karbantartás - karbantartási támogatás
  - visszavonás kilépéskor
- elvesztés kezelése (tartalom titkosítás / törlés, jelszó, ..)

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

ha hazamegy a partnercég alkalmazottja:
ne legyen a titkosítás törhető

WEP 64 vagy 128 bites kódolás

a WEP kulcs hexa számjegyek keveréke: 0,1, ... 9, A, B, ... F
sőt, van gyártó, amely enged decimális kulcsot is!

a 64 bites 5 db 2-jegyű hexadecimális szám, pl. CC AB F6 23 66
a 128 bites 13 db 2-jegyű hexa szám

ezt kell a router-ben megadni, aztán, a hozzáférés konfigurálásakor, az összes kliensben, ami majd a router-hez kapcsolódik
már a Windows is többféle titkosítási algoritmust tud kezelni

a Wi-Fi Alliance a WPA2® -t fogadta el
ez AES Advanced Encryption Standard titkosítást használ, max. 256 bites a kulcs

magyarázatok

hacker - Wikipédia nyomán - guru, varázsló
programozó, aki program kód, vagy erőforrások módosításával próbál valami sérülékenységet kihasználni
lehet olyan informatikai biztonsági szakértő, aki jól ismeri a számítógép, a számítógéphálózatok biztonsági lehetőségeit, és

- felhívja a figyelmet gyengeségeikre, vagy
- megpróbálja ezeket kihasználni

cracker: a "feketekalapos", a rosszindulatú hacker
- néha fordítva van – a cracker a jó, hacker a rossz

magyarázatok

infrastruktúrális elem
- amit sérülékenység szempontjából érdemes megkülönböztetni:
- Az informatikai infrastruktúra komponensei. Maga a számítógép is infrastruktúrális elem, a rajta futó szoftverrel, az adatbázis kezelő rendszerrel, a számítógépes kommunikációt biztosító hálózati elemekkel, az informatikai szolgáltatás megfelelő minőségét, sértetlenségét és bizalmasságát biztosító védelmi elemekkel (azok részeivel - infrastruktűrális elemeivel) és persze az ezek segítségével működő, az üzleti folyamatokat szolgáló alkalmazói programrendszerekkel együtt.