equicom
az Ön ICT méréstechnikai szakértője

HTE Infokom 2012
Mátraháza

WLAN Biztonság és Megfelelőségi Irányelvek

Kecskeméti Zsolt
Termékmenedzser
Informatikai hálózatok

EXFO EXPERTISE REACHING OUT · FLUKE networks · FITEL FURUKAWA ELECTRIC · AIRMAGNET · cisco Select Partner · ACCEDIAN NETWORKS · SUNRISE TELECOM · VeEX

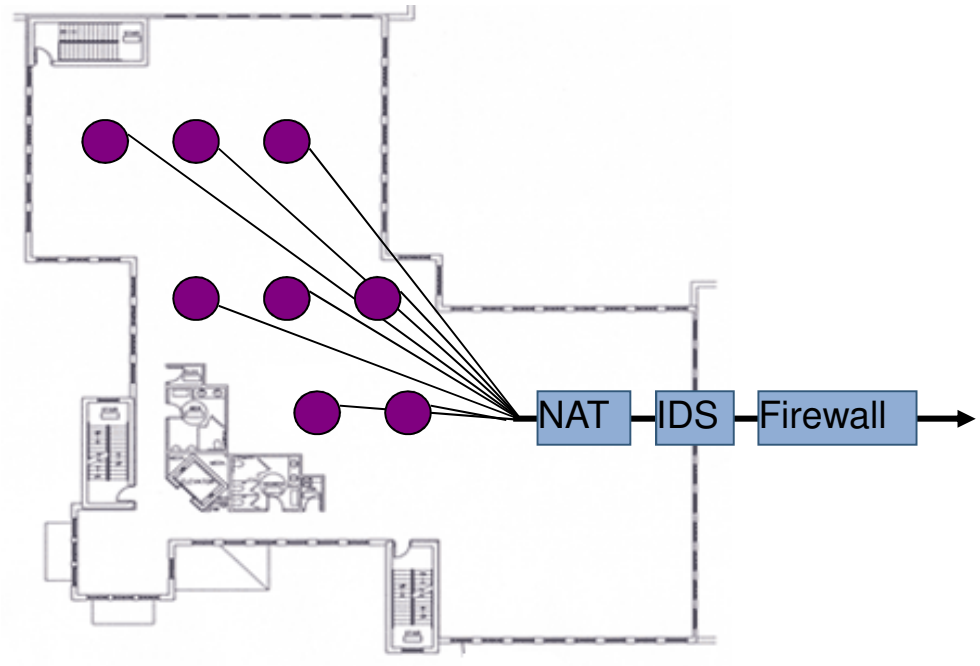
Mivel is foglalkozunk

- Kizárólag ICT méréstechnikai megoldásokra szakosodva
- Több mint 15 éves szakmai múlt
- Világviszonylatban piacvezető beszállítók képviselete
- Közvetlen kapcsolat a felhasználó és gyártó között
- Szakértelem, tanácsadás, támogatás, oktatások

LAN hálózatok – egy kapus

- Szabványkövetés (Cat6, 1000Base-T, 802.3)
- Többszintű fizikai és logikai védelem

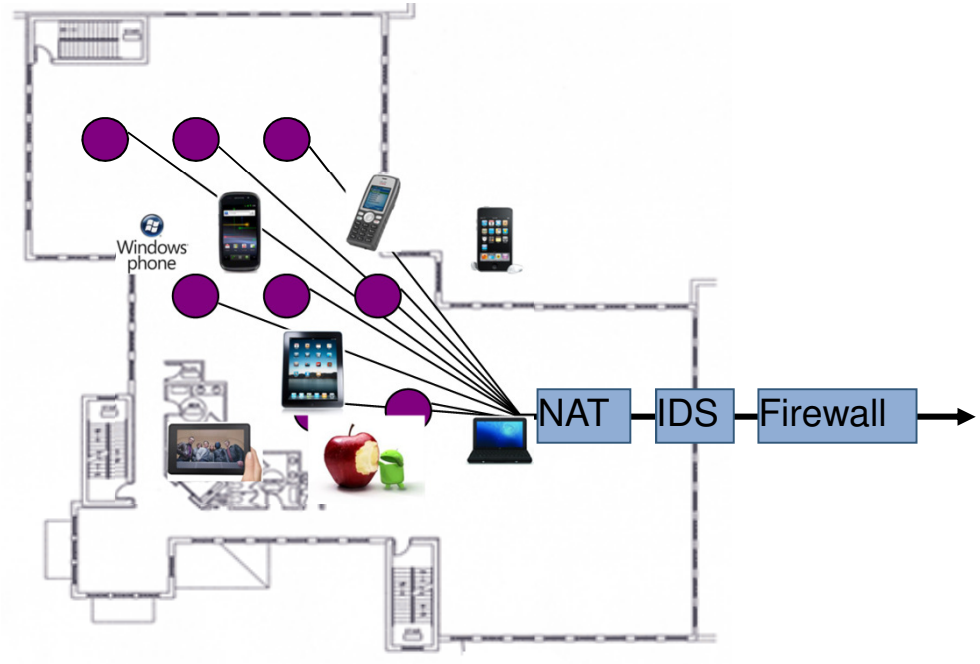
- ✓ Egy (vagy több) kapus
- ✓ Vizsgálat, analízis nélkül se ki- se be nem haladhat forgalom
- ✓ A felhasználók és a helyi infrastruktúra több szintű védelemmel ellátott.



WLAN hálózatok – n kapus

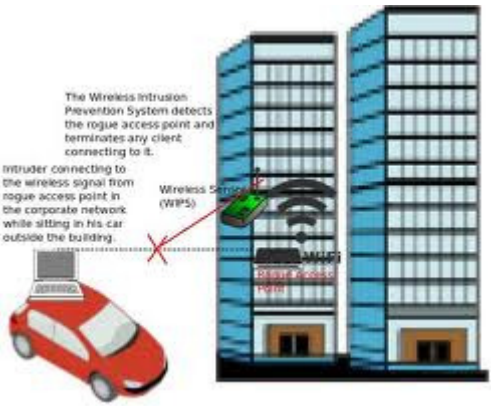
- Osztott rádiós közeg, mindenki hozzáfér
- Ingyenes csatornák, mindenki használhatja

- N kapus rendszer
- 802.11 eszközök és RF egyéb források a „hálózati forgalomban”
- Titkosítva csak az adatkeretek vannak!



Ó ez csak WiFi..

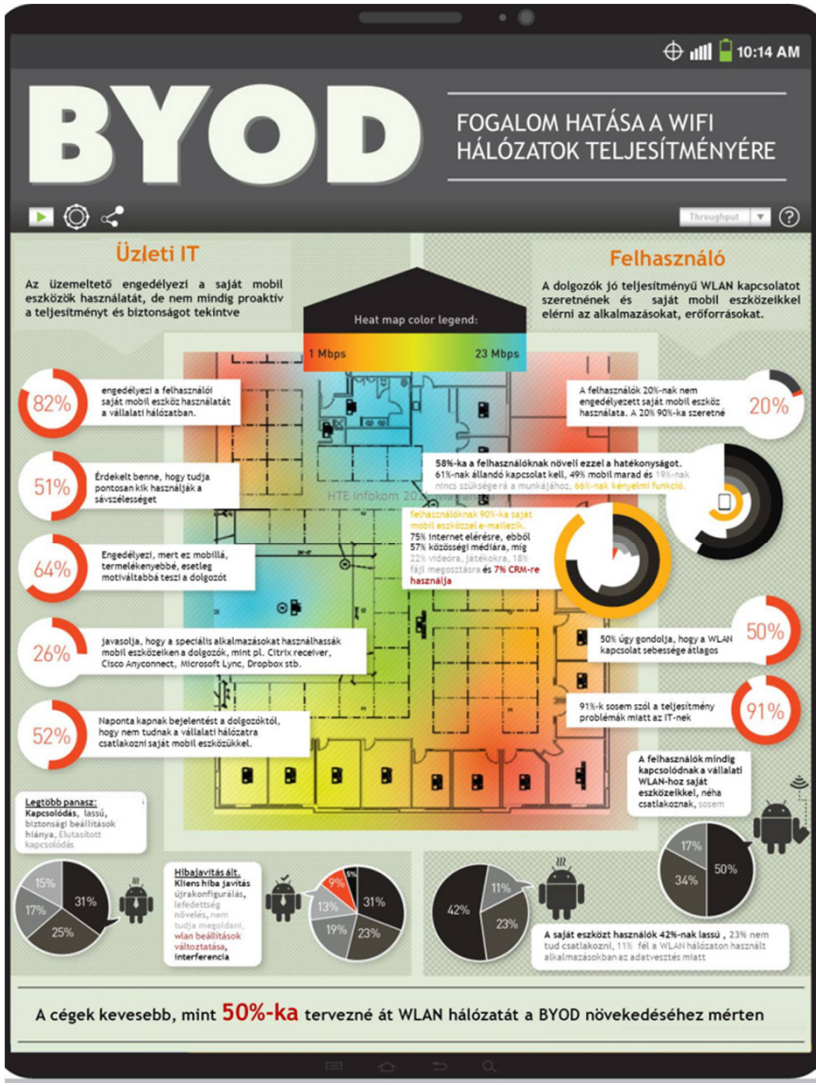
equicom
az Ön ICT méréstechnikai szakértője



Windows phone

WLAN fejlődik - veszély fokozódik?!

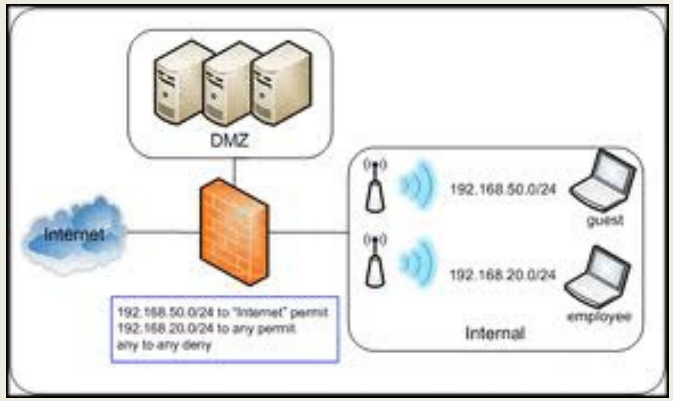
az Ön ICT méréstechnikai szakértője



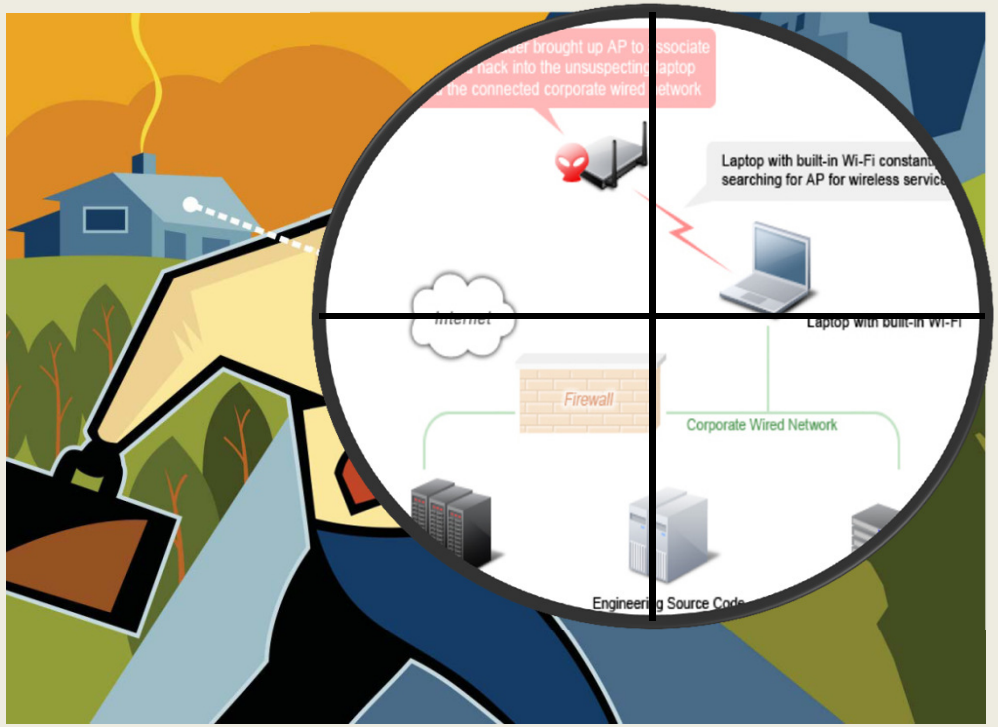
WLAN fejlődik – veszély fokozódik?!

Az én hálózatom biztonságos!

- Szegmensek, VLAN, VSSID, stb.



És ez biztos?



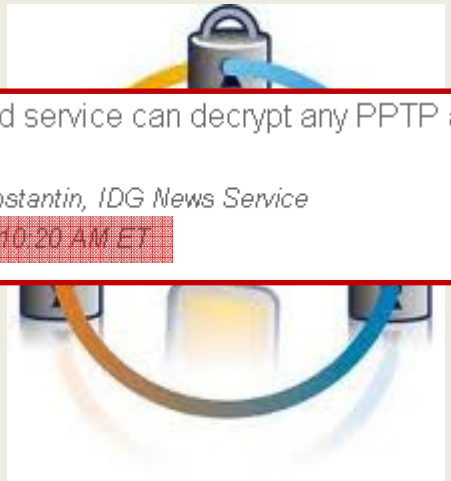
És a kliensek? Az RF osztott média, „bárki láthatja”

WLAN fejlődik - veszély fokozódik?!

az Ön ICT méréstechnikai szakértője

Az én hálózatom biztonságos!

- **Vállalati szintű hitelesítést használok! (AAA, EAP, Radius ++)**



És ez biztos?

Tools released at Defcon can crack widely used PPTP encryption in under a day

New tool and service can decrypt any PPTP and WPA2 wireless sessions using MS-CHAPv2 authentication

By Lucian Constantin, IDG News Service
July 29, 2012 10:20 AM ET

Add a comment Print + Briefcase

Security researchers released two tools at the Defcon security conference that can be used ...l) and WPA2-Enterprise ...entication.

...roduced in Windows NT ...echanism by most

MS-CHAPv2 has been known to be vulnerable to dictionary-based brute force attacks since 1999, when a cryptanalysis of the protocol was published by cryptographer Bruce Schneier and other researchers.

New tool and service can decrypt any PPTP and WPA2 wireless sessions using MS-CHAPv2 authentication

By Lucian Constantin, IDG News Service
July 29, 2012 10:20 AM ET

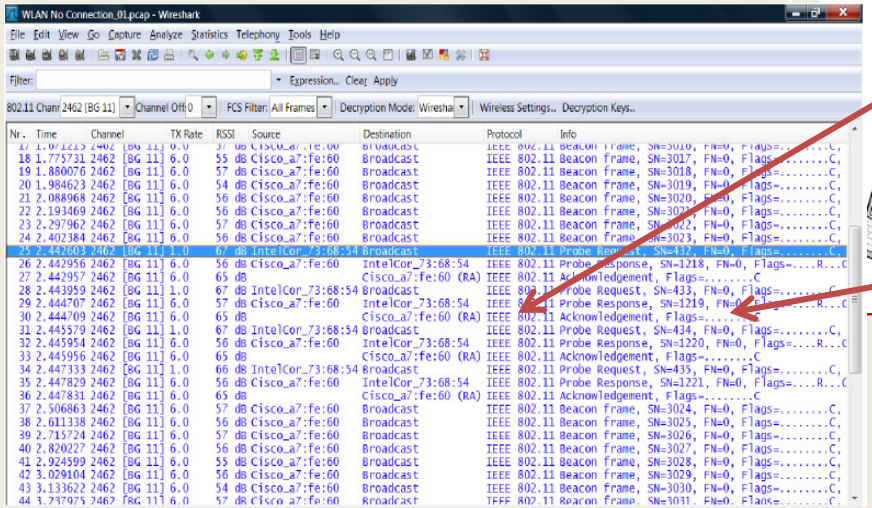
A hitelesítési protokollok sérülékenység vizsgálata?

WLAN fejlődik - veszély fokozódik?!

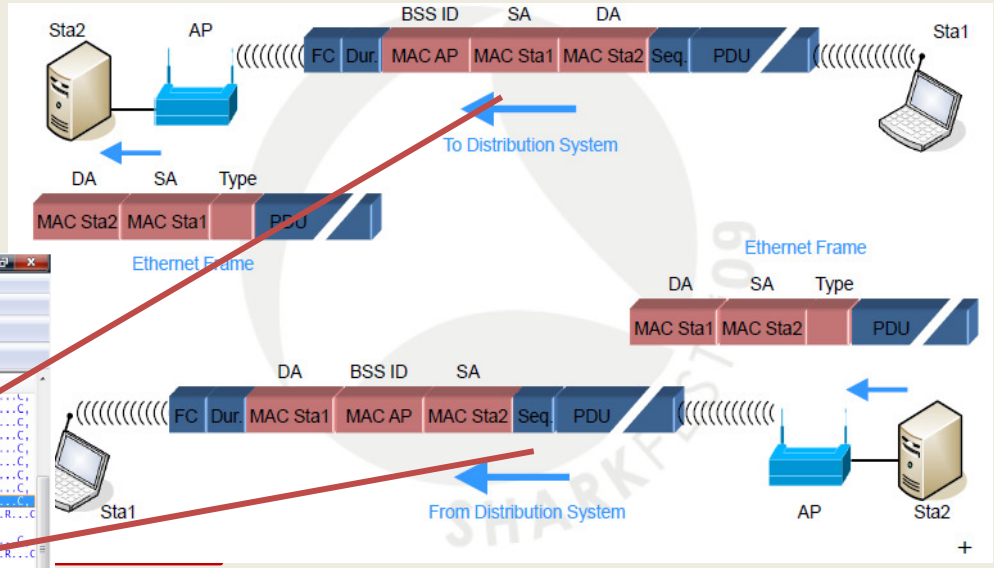
equicom
az Ön ICT méréstechnikai szakértője

Az én hálózatom biztonságos!

- Erős titkosítást alkalmazok (WPA2-E++)



És ez biztos?



Titkosítva csak az adat van a mgmt és ctrl keret nincs!

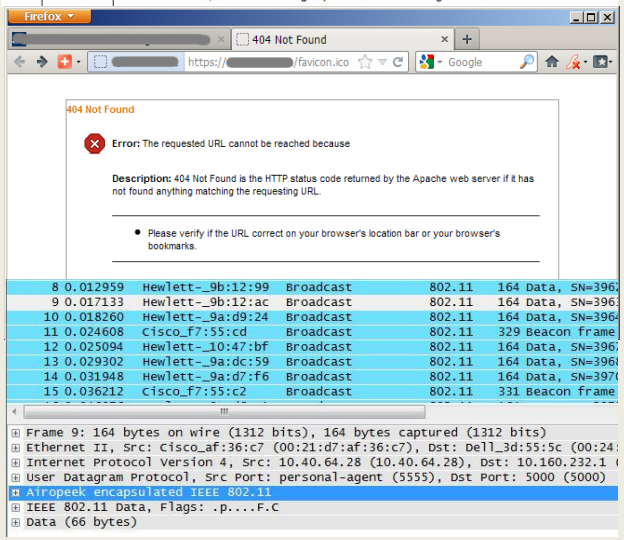
WLAN fejlődik - veszély fokozódik?!

az Ön ICT méréstechnikai szakértője

Az én hálózatom biztonságos!

- A WLC ++ megold mindent

CSCtu24889	AP 'DOT11-2-RADIO_RX_BUF' crashes upon receipt of WPA packet with length 0.
CSCtu28535	APs crash due to unexpected exception to CPUvector.
CSCtu44208	Unable to Telnet/SSH because of maximum number of connections reached, 0 in use.
CSCtu45614	Spectrum Management bit should be set to 1 all the time.
CSCtw56233	Crash on process_one_tx_packet for AP1130.
CSCtw78061	Require option to upgrade image from LDPE to non-LDPE image.
CSCtw78616	APs do not send the ELM flag when reporting wIPS traffic.
CSCtw90269	For RADIUS server, fallback accounting request is sent with missing AcctSessionId.



És ez biztos?

- 802.11abgn
- 1.5GHz Quad-Core
- 1GB RAM + Nvidia Tegra 3
- 134.4 x 69.9 x 8.9 mm
- 130g
- Android x.xx (Linux)
- Multi tasking applications

Display 4.7" 1280 x 720 pixels

android 3G 4G LTE

Bluetooth 4.0 Wi Fi CERTIFIED GPS

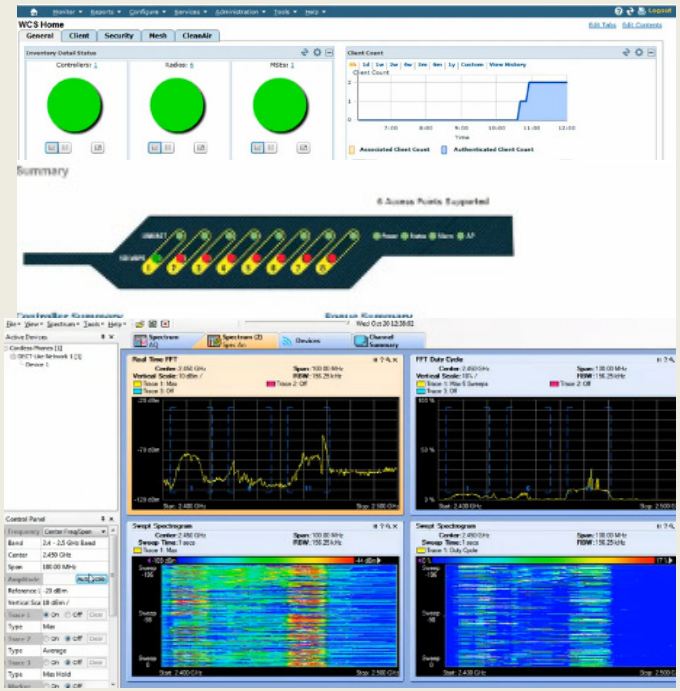
A kliens szűk keresztmetszet!?

WLAN fejlődik - veszély fokozódik?!

az Ön ICT méréstechnikai szakértője

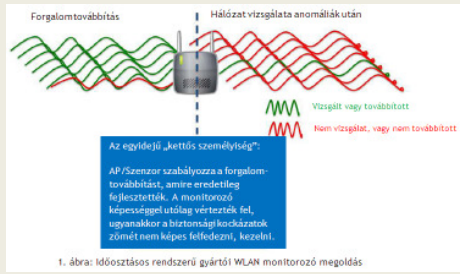
Az én hálózatom biztonságos!

- Az infrastruktúra rendszerem monitorozza is a hálózatom!



És ez biztos?

- Licence szám igény?
- Erőforrás igény?
- Időosztásos vizsgálat
- Konfiguráció időigény?
- Konfigurációs hibák?
- Újraindítás?
- Patch menedzsment?
- Web auth?
- Hamis biztonságérzet..



1. ábra: Időosztásos rendszerű gyártói WLAN monitorozó megoldás

Menedzsment ≠ Monitorozás

Layer1-től, valós időben!

Konfigurációs hibák?

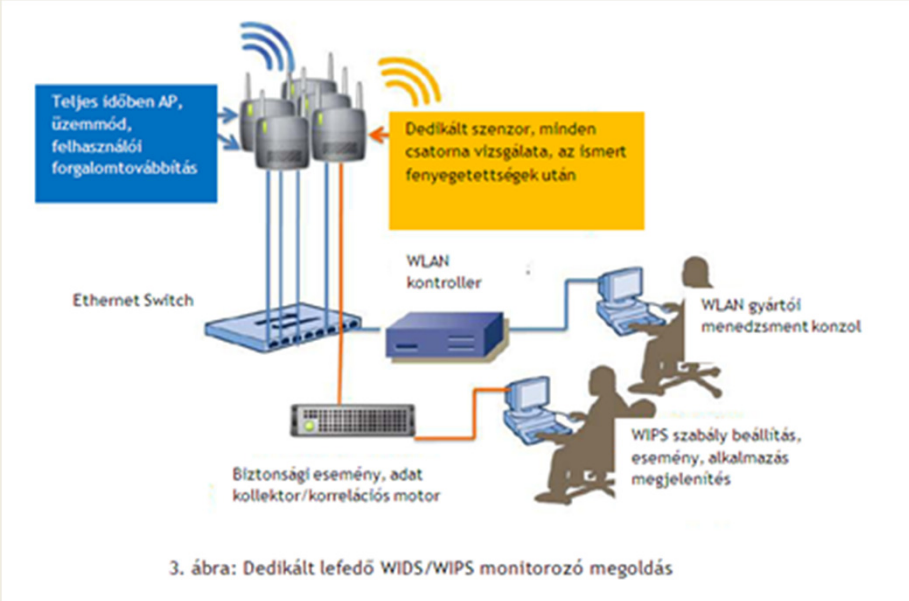
WLAN fejlődik - veszély fokozódik?!

az Ön ICT méréstechnikai szakértője

Az én hálózatom biztonságos!

- Új IT biztonsági törvény a kapuban..
- Megfelelőség, elvárások, auditálás

És ez biztos?



3. ábra: Dedikált lefedő WIDS/WIPS monitorozó megoldás

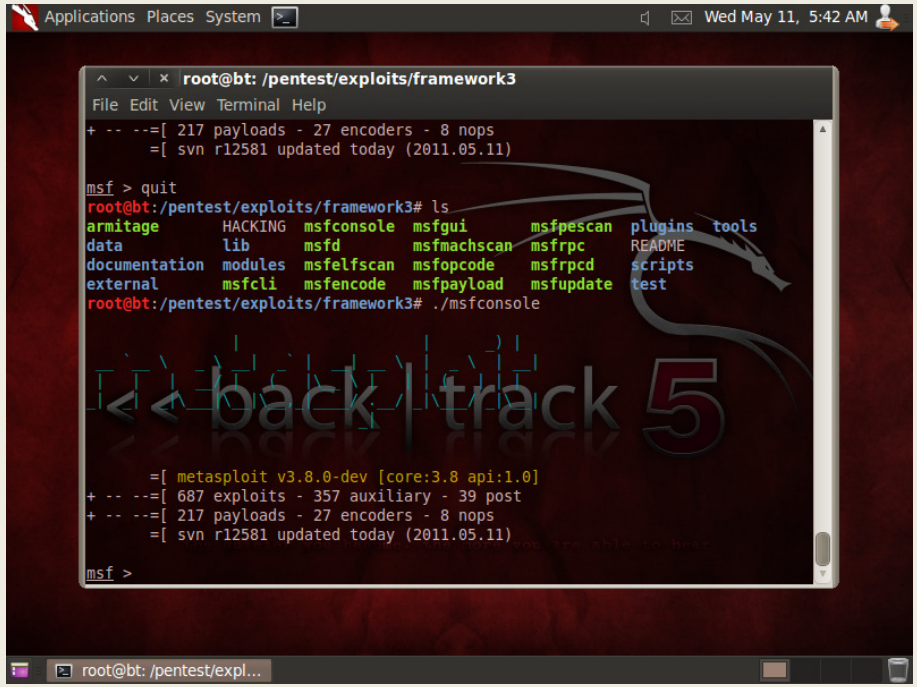
A Megfelelőség?

WLAN fejlődik - veszély fokozódik?!

Az én hálózatom biztonságos!

- Különben is ki törné fel a hálózatom?

És ez biztos?



Mindig van nagyobb cél!

Hamis biztonságérzet?!

PCI DSS és egyéb keretrendszerek

Keretrendszerek, irányelvek, vagy úgy nevezett Template-ek

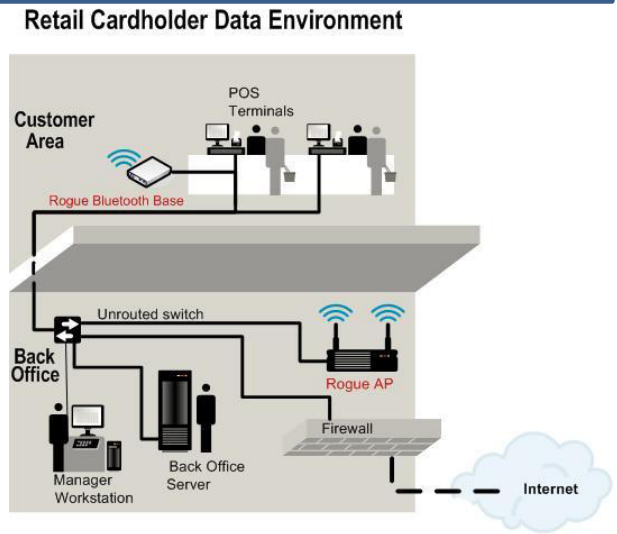
Néhány példa:

- ISO27001
- DoD 8100.2
- HIPAA
- PCIDSS

- GLBA (Gramm-Leach Bliley Act)
- SOX (Sarbanes-Oxley)
- BASEL II (Banking Supervision)
- EU CRD (EU Capital Requirements Directive)

PCI DSS – Payment Card Industry Data Security Standard

PCI Alliance 2011-ben tette hivatalossá a legújabb irányelvét v2.0 verziószámmal.
Ez egyértelműsíti a vezeték nélküli hálózatok (802.11 WLAN, 802.15 Bluetooth) esetén is a hálózat biztonsággal kapcsolatos megfelelőség elvárásokat



A PCIDSS irányelv 4.3.5 kivonat:

Gyakran felülvizsgált, frissített folyamatok és szabályrendszerek implementálása, melyek tartalmazzák és kezelik az IDS/IPS rendszerekből érkező, letárolt adatokat, riasztásokat.

WLAN fejlődik – veszély fokozódik?!

Válaszoljuk meg az alábbi kérdéseket:

- Mik a biztonsági előírások?
- Mivel jár, ha kiesik a WLAN hálózati működés?
- Kompromittálhatnak, intézményi/személyes adatok?
- Felhasználhatnak más, nagyobb cél elérésére?
- Megfelelőségi nyilvántartás, előírások betartása?

Egy-két példa az elmúlt időszakból.

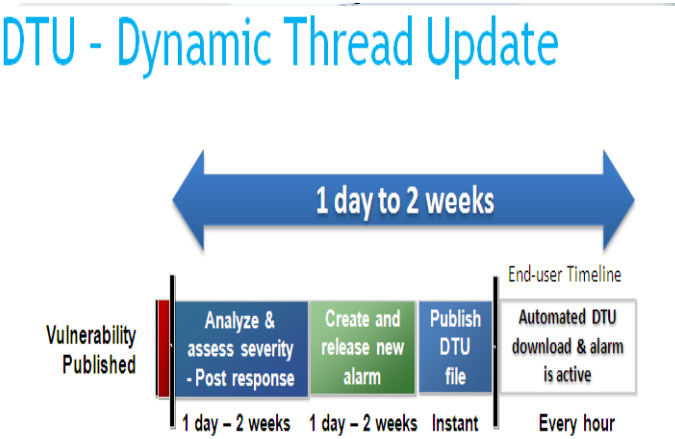
És még nincs vége!

Lefedő architektúrájú monitorozás

- Független kiterjeszthető felügyelet
- Áttekinthető, automatizálható
- RF spektrum analízis valós időben
- 802.11 sérülékenység vizsgálat, beavatkozás valós időben (L1-L2++)
- 24/7/365
- Riasztási és elhárítási rendszer (WIPS/WIDS)
- Gyakori adatbázis frissítés

Miért AirMagnet Enterprise?

- Független kiterjeszthető felügyelet
- Áttekinthető, automatizálható
- RF spektrum analízis valós időben
- 802.11 sérülékenység vizsgálat, beavatkozás valós időben (L1-L2++)
- 24/7/365
- Riasztási és elhárítási rendszer (WIPS/WIDS)
- Gyakori adatbázis frissítés (DTU)



Megjegyzés: SaaS rendszerként alkalmazható

Konklúzió

Emberi oldal

- Belső policy oktatása MINDENKINEK
- Üzemeltetők képzése technológiára (RF, 802.11, Ethernet)
- Üzemeltetők képzése infrastruktúrára (Gyártói)
- Szakértők képzése védelmi mechanizmusokra (Független – CWTS, CWNA min.)
- Külső szakértők bevonása (CEH, ECSA/LPT)

Műszaki oldal

- Infrastruktúra sérülékenység vizsgálat
- Naprakész infó kiszolgálóknál (WLC)
- Szakértők továbbképzése (802.11ac/ad, IPv6, 10G)
- Naprakész információ felhasználók oldaláról (BYOD)
- Rendszerszemlélet (LAN+WLAN)
- Megfelelő megoldást adott feladatra (dedikált WIPS + mobil megoldások)
- Megfelelőségi tanúsítvány (PCI, ISO27001, HIPAA stb.)

Forrásanyagok

Igény esetén kérem jelezzék a kérdőíven, vagy szóban

A, RF spektrum interferenciák tisztázása
B, Lefedő vs. Infrastruktúra alapú monitorozás
C, WLAN hálózatbiztonság és megfelelőségi irányelvek
D, AirMagnet Survey/Planner + Cisco WCS integráció
E, Kipróbálható AirMagnet megoldások
F, Az eszköz(ök) tesztelése saját környezetben

Wi-Fi ismeretek képzés
www.equicom.hu/eok

equicom
az Ön ICT méréstechnikai szakértője

HTE Infokom 2012
Mátraháza

Köszönöm megtisztelő figyelmüket!

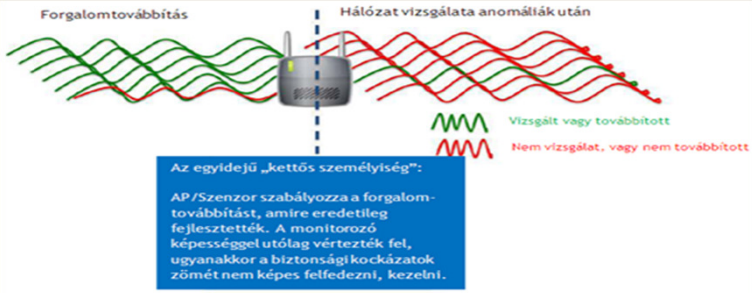
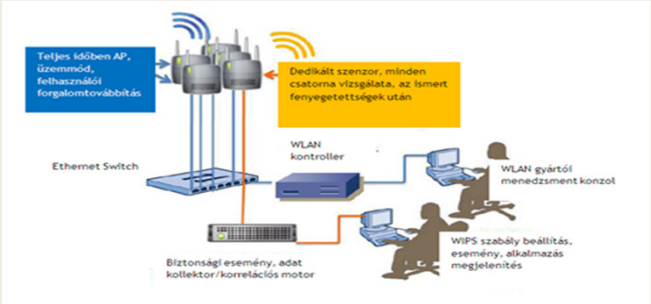
Kecskeméti Zsolt
Termékmenedzser
Informatikai hálózatok

EXFO EXPERTISE REACHING OUT · FLUKE networks · FITEL FURUKAWA ELECTRIC · AIRMAGNET · cisco Select Partner · ACCEDIAN NETWORKS · SUNRISE TELECOM · VeEX

Tartalék diák

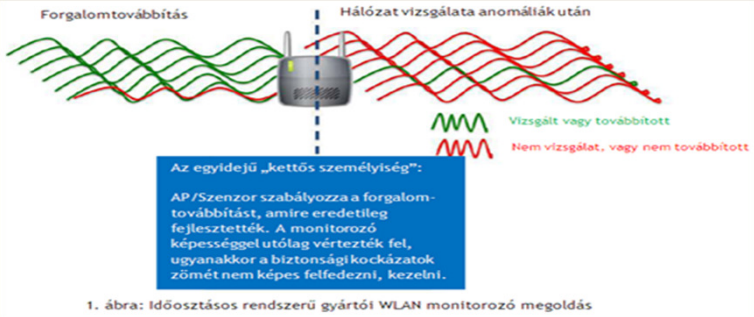
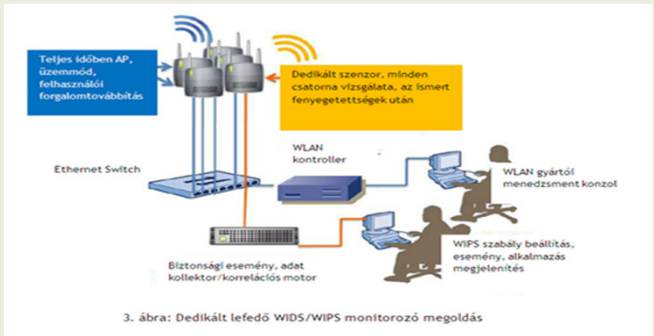
Infrastruktúra vs. Dedikált műszaki

equicom az Ön ICT méréstechnikai szakértője

	Infrastruktúra alapú „monitorozás”	Lefedő architektúrájú monitorozás
	 1. ábra: Időosztásos rendszerű gyártói WLAN monitorozó megoldás	 3. ábra: Dedikált lefedő WIDS/WIPS monitorozó megoldás
RF légtér folyamatos monitorozása	Időszakosan, Limitált csatorna szám	Valós időben 24/7/365 Kiterjesztett csatornák vizsgálata 802.11 és RF monitorozás és beavatkozás
Független felügyeleti rendszer	Hálózati eszköz függő Csak saját gyártmány, WLC-k, MSE-k szükségesek Továbbító és szenzor mód kapcsolás manuális	Infrastruktúra-független felügyeleti rendszer Dedikált szenzor, független az infrastruktúrától
Támadás vizsgálat és elhárítás	Kizárólag DoS technológiára épülő támadások felismerése, teljesítmény és egyéb biztonsági fenyegetettségek, algoritmusok felismerése nincs	Egyedülálló sérülékenység adatbázis, teljesítmény és biztonsági elvű kártékony viselkedés felismerése, konfiguráció elemzés
Adattárolás	Nincs adattárolás, No track record	Visszamenőleg minden vezetékes és wlan visszakereshető, trending infók
Teljesítmény monitorozás	Nincs, csak biztonsági monitorozás érhető el	Automatizált teljesítmény tesztek, hw és sw szenzorral, AP-k és kontroller felhasználásával

Infrastruktúra vs. Dedikált gazdasági

equicom
az Ön ICT méréstechnikai szakértője

	Infrastruktúra alapú „monitorozás”		Lefedő architektúrájú monitorozás
	 1. ábra: Időosztásos rendszerű gyártói WLAN monitorozó megoldás		 3. ábra: Dedikált lefedő WIDS/WIPS monitorozó megoldás
Tipikus elvárások	Idegen eszköz keresés, vezetékes vizsgálat, megfelelőségi jelentések	Idegen eszköz keresés, vezetékes vizsgálat, megfelelőségi jelentések RF és vezetékes blokk Támadó IDS	Idegen eszköz keresés, vezetékes vizsgálat, megfelelőségi jelentések RF és vezetékes blokk, Támadó IDS Dinamikus frissítés NMS, SIEM integráció Valós idejű távoli GUI és RF spektrum an. Valós idejű teljesítmény vizsgálat
Egyedi igények	Pipa be és megfelelt.. (PCI, stb.)	Megfelelőségi riportok, adatvédelmi szabályozás	Tényleges megfelelőség bizonyítás, földrajzilag bárhol dedikált eszközzel, adat,- és információ védelmi szabályozás
CAPEX	€	€- €€	
OPEX			

Software Szenzor

AirMagnet Enterprise / HW Szenzor