Tanulmány

A mozgásban levő információ védelme a Cisco Secure Wireless megoldással

Bevezetéas

A vezeték nélküli hálózatok terjedése megszüntette a megbízható és megbízhatatlan hálózatok közötti hagyományos határvonalat, és a hálózat peremének védelme helyett az információbiztonságot helyezte a középpontba. A mobil információ biztonságossá tétele és a vezeték nélküli környezetnek a jogosulatlan hozzáférést megakadályozó ellenőrzése egyaránt elsődleges fontosságú a céges adatok és rendszerek sértetlenségének megőrzéséhez.

A vezeték nélküli alkalmazások gyors terjedésének következtében egyre fontosabbá válik a vezeték nélküli biztonság, különösen Wi-Fi alapú vezeték nélküli LAN-hálózatok esetén. Az ilyen hálózatok három olyan jellemzővel rendelkeznek, amelyek miatt még fontosabb a biztonságossá tételük. Először is a vezeték nélküli forgalom értelemszerűen az éteren keresztül kerül továbbításra, így nincsenek olyan fizikai határai, mint például a falak. Ezért a meglévő határvédelmi megoldások, köztük a tűzfalak sem képesek a biztonsági házirendeket a belső és külső határok mentén hatékonyan betartatni. Másodsorban az olyan szabványok, mint amilyen a 802.11 protokoll is, megfelelően dokumentáltak és érthetők, így bárki számára könnyedén hozzáférhetők. Ez az átláthatóság egyszerűbbé teszi a rosszindulatú támadások indítását. Végül, de nem utolsósorban, a Wi-Fi a nem engedélyköteles 2,4GHz-es és 5GHz-es frekvenciákon működik. Az engedély meglétét igénylő mobilfrekvenciákkal ellentétben ezeket a frekvenciákat bárki használhatja. Bár az FCC az agresszív és rosszindulatú használat megakadályozása érdekében kötelezővé teszi bizonyos szabályok betartását, ezek betartatásának nehézsége miatt ezen frekvenciák törvénytelen használata többnyire büntetlen marad.

A mobil információ sértetlensége

A vezeték nélküli biztonsági stratégiák alapja, hogy az informatikának a bizalmas ügyfél-, partner- és pénzügyi adatok védelmére kell összpontosítani. Az információ digitalizálása és az IP-kommunikáció széles körű elterjedése fokozták a munkavégzés hatékonyságát és javították az üzleti folyamatokat, mivel azonnal hozzáférhetővé teszik az információt. Azon erőfeszítésükben, hogy szabályozzák a bizalmas információk elérhetőségét és védelmét, a kormányzatok és egyes iparági testületek olyan szabályokat fogalmaztak meg, amelyek iránymutatást adnak a vállalatok számára a bizalmas adatok védelme tekintetében. Az egyes üzleti szervezetekre érvényes szabályok száma és hatálya a vállalat méretétől és tevékenysége jellegétől függ. Mindazonáltal három olyan fő szabályozó szabvány alakult ki, amelyek a vállalatok jelentős részére érvényesek: az egyik a Sarbanes-Oxley törvény, a második a HIPAA-törvény személyes adatokra vonatkozó előírásai, a harmadik pedig a Personal Cardholder Information (PCI) adatbiztonsági szabvány. Az 1. táblázat további információkat közöl ezekről a fontos szabványokról.

1. táblázat Szabályozói követelmények

Szabályozás	Követelmények
Sarbanes-Oxley törvény	Minden tőzsdén jegyzett vállalatnak: ▪ Megfelelő belső ellenőrzési struktúrát és eljárásokat kell fenntartani a pénzügyi jelentések elkészítésére ▪ Értékelnie kell a belső ellenőrzési struktúráknak a hatékonyságát
HIPAA-törvény	Adminisztratív, műszaki és fizikai védelmet kell fenntartani: ▪ A betegek adatainak sértetlenségének és bizalmasságának megőrzése érdekében ▪ A fenyegetések és kockázatok, illetve a betegek adatainak jogosulatlan felhasználása vagy nyilvánosságra hozása ellen
PCI	Bankkártyás fizetést lehetővé tevő minden kereskedőnek (az elektronikus kereskedőknek is): ▪ Biztonságos hálózatot kell kiépíteniük és fenntartaniuk ▪ Védeniük és titkosítaniuk kell a kártyabirtokosok adatait ▪ Rendszeresen felügyelni és tesztelni kell a hálózatokat (köztük a vezeték nélküli hálózatokat is)

Bár ezen szabályozások egyike sem explicit módon követeli meg a vezeték nélküli biztonságot, az irány egyértelmű. Mindegyik szabály az információk védelmét és ellenőrzését követeli meg, mindegy, hogy pénzügyi adatokról, a betegek bizalmas jellegű feljegyzéseiről vagy bankkártya-tranzakciókról van szó. A vezeték nélküli infrastruktúrával továbbított adatmennyiség egyre nőni fog, és a jogosulatlan hozzáférés megakadályozása érdekében megfelelően titkosítani és ellenőrizni kell. Ezen túlmenően a fizikai vezeték nélküli környezetet állandóan felügyelni és biztosítani kell, hogy kiszűrhetők legyenek a vállalati rendszerekbe „hátsó ajtót” nyitó jogosulatlan hozzáférési pontok.

A biztonsági incidensek költsége

Nem minden szabályozás tartalmaz büntető szankciókat, számos – köztük a PCI is – azonban igen. Ám a vállalatok számára az adott szabályozás által kilátásba helyezett bírságoknál sokkal nagyobb üzleti jelentőséggel bír a biztonsági incidensek által okozott költség. Bár a bírságok által keltett fenyegetés tudatosíthatja a vezetőségben a szigorú biztonsági ellenőrzések fontosságát, vannak kevésbé megfogható, mégis sokkal nyomatékosabb ösztönzők. Egy, a Gartner Group által készített elemzés szerint a biztonsági incidensek sérült ügyfélrekordonként 90-1500 dollár közvetlen költséget okozhatnak.[1] Egy másik, az Information Systems Security által készült kutatás kimutatta, hogy egy nyilvánosságra kerülő biztonsági incidens jelentős hatással lehet az érintett cég piaci értékére. A kutatás becslése szerint az adott cég árfolyama a nyilvánosságra került biztonsági incidens következtében az első nap 2,7 százalékkal, az első három napon pedig mintegy összesen 4,7 százalékkal csökken.[2]

Az alábbiak tartozhatnak az ügyfél- és pénzügyi adatokat érintő biztonsági incidensek költségei közé:

- Szabályozói bírságok
- Külső biztonsági auditálás költsége
- Ügyfeleknek vagy partnereknek fizetett kártérítés
- Az ügyfelek bizalomvesztése, amely a jövőbeli bevételek csökkentését eredményezheti
- A vállalat hírnevén esett csorba
- Befektetői bizalomvesztés
- Piaci értékvesztés

[1] Data Protection Is Less Costly Than Data Breaches (Az adatok védelme kevésbé költséges, mint az adatlopásból származó kár) , Gartner Group, 16 September 2005

[2] The Financial Impact of IT Security Breaches: What Do Investors Think? (Az IT biztonsági incidensek pénzügyi hatása: Mit gondolnak a befektetők?), Information Systems Security, 2003. március/április

A kitettség korlátozása a Cisco Secure Wireless megoldással

A Cisco az Önvédő Hálózat (Self-Defending Network) stratégiával segíti a vállalatokat az adatbiztonsági követelményeknek való megfelelésben. Az Önvédő hálózat a Cisco hosszú távú stratégiája a szervezetek üzleti folyamatainak védelmére, amely a belső és külső forrásból érkező fenyegetések azonosítása, megelőzése, illetve az azokhoz való alkalmazkodás alapján valósul meg. Az ilyen jellegű védelem segít a szervezeteknek, hogy jobban kihasználják a hálózati erőforrásaikban rejlő információk előnyeit, ezáltal javítsák üzleti folyamataikat és csökkentsék költségeiket.

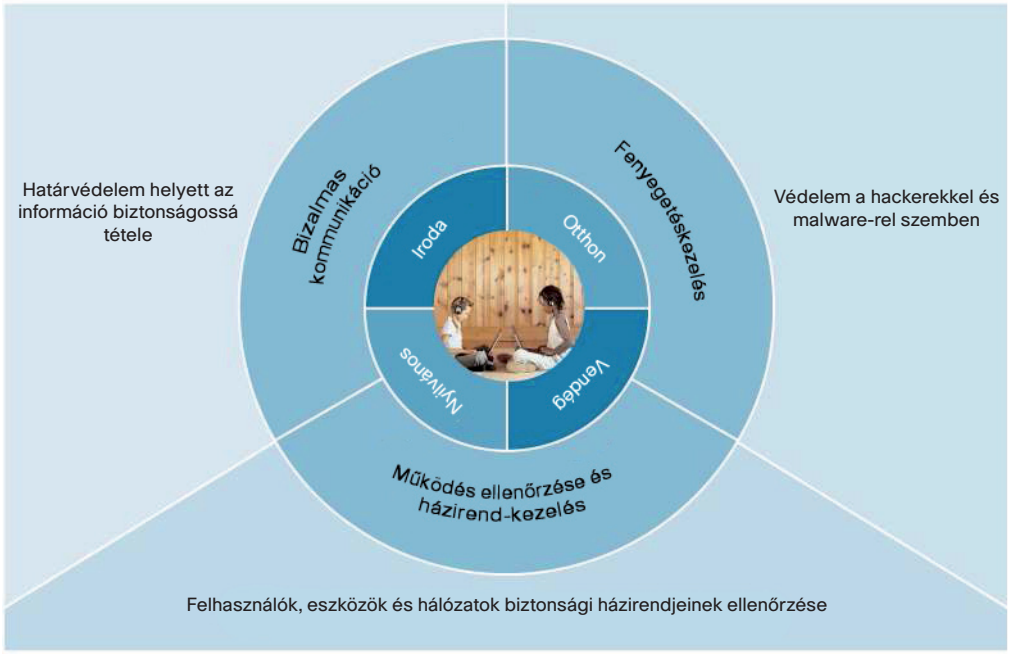
A Cisco Önvédő hálózat biztonsági megoldásokat az alábbiak jellemzik:

- A biztonság érintetlensége a hálózat minden elemében
- Együttműködő folyamatokat a különbözi biztonsági és hálózati elemek között
- A hálózat azon képessége, hogy az új fenyegetésekhez már megjelenésükkor alkalmazkodni tud

Az önvédő metodika iránymutatást ad a vállalatoknak arra, hogyan hozzanak létre biztonságos kommunikációs infrastruktúrát és segít elérni megfelelőségi céljaikat. A vezeték nélküli biztonsági követelmények teljesítése érdekében a Cisco architekturális megközelítést javasol a vállalatoknak a vezeték nélküli hálózatuk megtervezésére és létrehozására.

A Cisco Secure Wireless megoldás átfogó biztonsági keretrendszer, amely a mozgásban lévő információ biztonságos kommunikációját, a különböző felhasználók és alkalmazási lehetőségek biztonsági házirendjeit és robosztus fenyegetés elleni védekezőképességet kombinálva védi az információkat és a rendszereket a vezeték nélküli fenyegetésektől (lásd 1. ábra). Teljes körű architektúrát biztosít, amely a Cisco Unified Wireless Network, vagyis a Cisco egységes vezeték nélküli hálózat meglévő biztonsági funkcióit releváns biztonsági megoldásokkal, így többek között a Cisco hálózati hozzáférés-szabályozási (Network Admission Control – NAC) készülékkel, a Cisco behatolásmegelőző rendszer (Intrusion Protection System – IPS) szoftverrel felszerelt Cisco ASA 5500 sorozatú tűzfalakkal, a Cisco Security Agent szoftverrel, illetve egyéb alkotóelemekkel integrálja.

1. ábra A Cisco Secure Wireless megoldás biztonsági keretrendszere



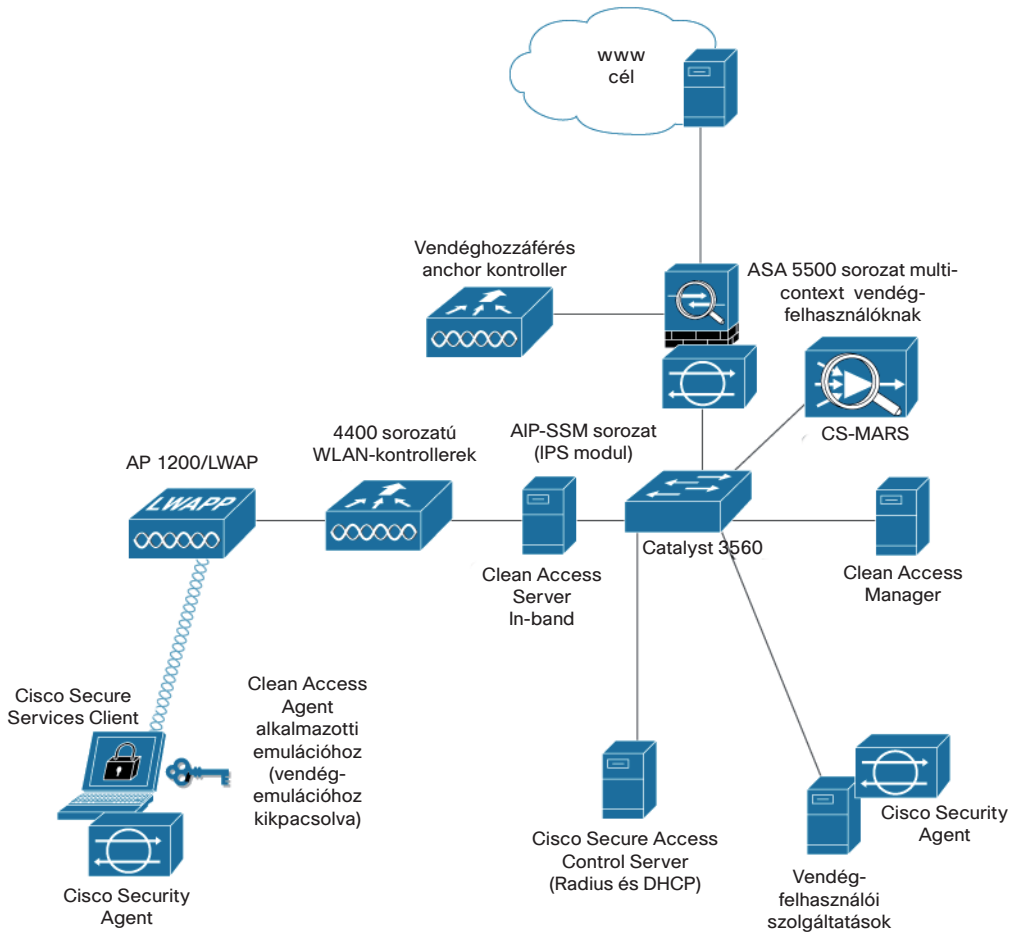
A Secure Wireless megoldás alkotóelemei

A Cisco Secure Wireless megoldás teljes körű architektúra, amely a legfontosabb biztonsági és vezeték nélküli megoldásokat integrálva nyújt szabványalapú, iparágvezető hálózatvédelmet (lásd 2. ábra). Az architektúra vezetékes és vezeték nélküli biztonsági szolgáltatásokat kombinálva biztonsági funkciók egységes csomagját kínálja, amely nem csupán robosztus védelmet jelent a fenyegetések ellen, hanem a biztonságos vezeték nélküli hálózatok megvalósításának és fenntartásának teljes költségét is csökkenti.

A Cisco Secure Wireless megoldás legfontosabb jellemzői:

- Egységes vezetékes és vezeték nélküli behatolásvédelmi / behatolásészlelő rendszer (IPS/IDS)
- Kliensellenőrzés, posture értékelés és javítás
- Vezeték nélküli egyszeri bejelentkezés (single sign-on) és 802.1X integráció
- Biztonságos vendéghozzáférések ellenőrzése
- Host behatolásmegelőzés
- Jogosulatlan eszközök észlelése automatikus RF-felügyelettel
- A vezeték nélküli biztonság kezelése

2. ábra A Cisco Secure Wireless megoldás architekturális áttekintése



Egységes vezetékes és vezeték nélküli behatolásmegelőzés

Közreműködő termékek

- Cisco Intrusion Prevention System modul (AIP-SSM)
- Cisco ASA 5500 tűzfal
- Cisco vezeték nélküli LAN-kontroller

A Cisco Secure Wireless megoldás vezetékes és vezeték nélküli behatolásészlelést és -megelőzést integrálva mérsékli a hackerek és rosszindulatú kódok fenyegetéseit. A hálózati az IP-rétegtől az alkalmazásrétegig (L3-tól L7-ig) vizsgálja a forgalomfolyamot és kutat potenciálisan káros vírusminták (signature) és gyanús alkalmazásviselkedés után. Vírusminta észlelése esetén a vezetékes IPS megoldás riasztja a vezeték nélküli LAN-kontrollert és közli vele, hogy vírusminta jelentkezett a vezeték nélküli hálózaton. A vezeték nélküli LAN-kontroller ekkor fizikailag blokkolja a kliens hozzáférési ponthoz csatlakozását. A vezetékes és vezeték nélküli megoldások ilyetén integrációja megelőző (zero-day) riasztást és válaszlépést biztosít a potenciális vírusok, malware és gyanús vírusminták megjelenésére.

Kliens posture értékelés és javítás

Közreműködő termékek

- Cisco NAC-készülék
- Cisco vezeték nélküli LAN-kontroller

A Cisco Secure Wireless megoldás képes a felhasználók és eszközök azonosságának ellenőrzésére, illetve mindenre kiterjedő biztonsági házirendek betartatásával biztosítja, hogy a felhasználók és eszközök az antivírus és spyware védelmi szoftver legfrissebb verziójával legyenek felszerelve. Amennyiben egy kliens nincs frissítve, a megoldás karanténba helyezi és elkülöníti a hálózat többi részéről mindaddig, amíg a felhasználó (vagy a rendszergazda) meg nem oldja ezt a problémát. A Cisco NAC-készülék és a Cisco egységes vezeték nélküli hálózat közötti szoros együttműködés biztosítja, hogy a vezeték nélküli kliensek betartják az aktuális biztonsági házirendet és nem fertőzik meg a hálózatot külső hálózatokból szerzett malware-rel.

Vezeték nélküli egyszeri bejelentkezés

Közreműködő termékek

- Cisco NAC-készülék
- Cisco vezeték nélküli LAN-kontroller
- Cisco Secure Services Client
- Cisco Secure Access Control Server (ACS)

A megoldás a Cisco Secure Services Client 802.1X ellenőrzési funkcióit is kihasználva egyszerűsíti a vezeték nélküli használatot a vezeték nélküli hálózatba és a NAC-készülékbe (a posture értékeléshez) történő egyszeri bejelentkezés lehetővé tételével. Ez a funkció kényelmesebbé teszi a felhasználói élményt és összevonja a nyilvántartást (accounting) és adminisztrációt, és közben a jelszókezelést is javítja. A 802.1X ellenőrzés és a posture értékelés együttesen a felhasználók számára észrevehetetlenül teszik biztonságossá a kapcsolatot és védik a hálózatot a malware-től.

Biztonságos vendéghozzáférés

Közreműködő termékek

- Cisco vezeték nélküli LAN-kontroller
- Cisco ASA 5500 sorozatú tűzfal
- Cisco NAC-készülék (opcionális)

A vállalatok egyre gyakrabban találkoznak azzal az igénnyel, hogy hálózati kapcsolatot biztosítsanak olyan külső személyek számára, mint amilyenek a látogatók, az alvállalkozók, a tanácsadók vagy a partnerek. A szinte minden laptopban megtalálható Wi-Fi-nek köszönhetően a vezeték nélküli hálózat tökéletes eszköz a vendéghozzáférések biztosítására. A Cisco Secure Wireless megoldás a vendéghozzáférés két szintjét kínálja. Az alapfunkció esetén biztonságos alagút helyezkedik el a hálózaton belüli kontroller és a nem biztonságos hálózati területen levő vendégkontroller között, amely közvetlenül a vállalati hálózaton kívülre irányítja a vendégforgalmat. A vendégkontroller testreszabható webes kezelőfelületet biztosít a felhasználói bejelentkezésre és a felelősségi kikötések közlésére, illetve Lobby Ambassador funkciójával akár felhasználónként eltérő bejelentkezési jogosultságokat is képes támogatni.

A Cisco Secure Wireless megoldás a Cisco NAC-készüléket használja az ennél magasabb szintű vendégszolgáltatásokhoz, így többek között a szerepalapú hozzáférés meghatározására és kliens posture értékelések és javítások végrehajtására. Ez a készülék a Cisco vezeték nélkül LAN-kontrollerek funkcióit egészíti ki. A Cisco ASA tűzfalcsalád termékeivel a megoldás mindenre kiterjedő hálózatforgalmi házirendek létrehozására és betartatására lesz alkalmas, így biztosítva páratlan tartalom-ellenőrzést.

Végponti vezeték nélküli használat ellenőrzése

Közreműködő termékek
▪ Cisco Security Agent

Egy mobilkliens jellegéből adódóan gyakran csatlakozik megbízható és nem megbízható hálózatokhoz is. Bár a jelenlegi IT-feladatok nagy része a belső hálózat ilyen mobil kliensek által behozott támadások elleni védelmére irányul, a klienst magát is védeni kell. A Cisco Secure Wireless megoldás elfogadott vezeték nélküli használati szabályokat tartalmaz, amelyek a klienscsatlakozási házirend betartatásával védi a megbízható hálózaton kívül kapcsolatot létesítő vállalati eszközöket. A Cisco Security Agent Day Zero támadás elleni védelmet is tartalmaz, és képes konkrét vezeték nélküli házirendek, köztük az alábbi szabályok betartatására:

- A vezeték nélküli hálózati csatolókártya (NIC) kikapcsolása vezetékes hálózathoz csatlakozáskor
- A vezeték nélküli ad hoc csatlakozások kikapcsolása
- Service Set Identifier (SSID) egyeztetési szabályok betartatása
- Nem megbízható hálózati csatlakozások alatt VPN engedélyezése

Jogosulatlan eszközök észlelése és elszigetelése

Közreműködő termékek
▪ Cisco egységes vezeték nélküli hálózat ▪ Cisco Location Appliance

A vezeték nélküli biztonsági stratégia meghatározó eleme a vezeték nélküli környezet RF-felügyeleti funkciók használatával történő ellenőrzése a jogosulatlan használat megelőzése érdekében. Mivel sok alkalmazottat vonz a vezeték nélküli kapcsolat szabadsága és az otthoni kategóriájú hozzáférési pontok már alacsony áron elérhetők, a jogosulatlan hozzáférési pontok sok vállalat számára jelentenek gyakori problémát. A szervezetek többsége agresszíven közelit a vezeték nélküli kapcsolatok adatforgalmának biztonságos kialakításhoz, és megközelítésüket általában a Wi-Fi Protected Access (WPA) és WPA2 iparági szabványokra alapozzák. Csak kevés vállalat képes teljes mértékben megérteni az átfogó RF-felügyelet szükségességét. Az RF-felügyelet teljes rálátást enged a vezeték nélküli környezetre és biztosítja, hogy jogosulatlan hozzáférési pontok vagy külső (esetleg belső) személyek kártékony viselkedése ne teremtsen hátsó ajtós (backdoor) hozzáférést a hálózathoz, feltárva ezzel a teljes vállalati rendszert.

A Cisco Secure Wireless megoldás közvetlenül a hozzáférési pontokba integrálja az RF-felügyeletet és folyamatosan, napi 24 órában és heti 7 napban azonosítja, behatárolja és szigeteli el a jogosulatlan vezeték nélküli tevékenységet. Ez a lehetőség minden megfelelőségi kezdeményezés szempontjából rendkívül fontos a bizalmas adatok védelméhez.

A vezeték nélküli biztonság kezelése

Közreműködő termékek
▪ Cisco Wireless Control System ▪ Cisco Security Mars

Minden biztonsági megoldás magától értetődően használható kezelőeszközöket igényel a hálózatbiztonság fenntartására. A Cisco Secure Wireless megoldás a Cisco Wireless Control System (WCS) szoftvert használja a vezeték nélküli LAN-hálózat tervezésére, konfigurálására és kezelésére. A Cisco WCS olyan alapot biztosít, amely lehetővé teszi az IT-menedzsereknek, hogy központilag tervezzék, ellenőrizzék és felügyeljék a nagyvállalati vezeték nélküli hálózatokat. Ezáltal egyszerűsödik a működtetés és csökken a teljes élettartamköltség. A WCS riasztja a hálózati rendszergazdákat a biztonsági fenyegetésekről, és a hálózat grafikus nézetét kínálja számukra, amely a jogosulatlan hozzáférési pontok helyét és fenyegetési szintjét is tartalmazza. A WCS szoftverrel együttműködő Cisco Security Monitoring, Analysis, and Response System (Cisco Security MARS) rendszer felismeri és összefüggésbe állítja a valódi hálózati támadásokat, valamint végrehajtható útmutatást ad megállításukra. Ezen kezelőfunkciók kombinációja a legátfogóbb és magától értetődően használható kezelési keretet biztosítja a jelenlegi vezeték nélküli biztonsági architektúrák mindegyikéhez.

A Cisco Secure Wireless megoldás a már bemutatott funkciókon túlmenően is iparágvezető funkciókat foglal magában a magasabb szintű biztonság érdekében. A Cisco vezetésével kifejlesztett Management Frame Protection (MFP) technológia a 802.11 csomagok menedzsment kereteinek titkosításával növeli a továbbított adatok titkosításának szintjét. Ha a kliens és az infrastruktúra között kombinálva alkalmazzák, az MFP

jelentős mértékben csökkenti a protokollalapú, köztük a man-in-the-middle támadások veszélyét.

Mivel a hálózatot elérő klienseszközök száma nagyon gyorsan emelkedik, a Cisco felismerte a klienskezelés és –biztonság fontosságát. A Cisco Compatible Extensions program alapján a Cisco közvetlenül a Wi-Fi eszközök gyártóival együttműködve egységesen ágyazza be a készülékekbe az olyan biztonsági funkciókat, mint az MFP, hogy a termékeket használó vállalatok számára elérhetővé tegye azokat. Az adott biztonsági funkciók támogatása növeli a teljes hálózatbiztonságot és egyszerű, biztonságos kapcsolatot biztosít a kliens és az infrastruktúra között. A Cisco ezzel párhuzamosan folytatja az együttműködést a szabványalkotó testületekkel, hogy nyílt, szabványalapú módon dobja piacra ugyanezeket a biztonsági funkciókat.

Integrált szolgáltatások és támogatás

Napjainkban a vállalatoknak versenyképességük megőrzése érdekében gyorsan kell reagálniuk az útjukba kerülő váratlan változásokra, lehetőségekre és fenyegetésekre. A Cisco Services és annak WLAN-hálózatokra és biztonságra szakosodott partnerei segíthetnek szervezetének, hogy megfeleljenek a jelenlegi szabályozói követelményeknek. Szakértőink a Cisco már bizonyított eszközeit és a bevált legjobb módszereket alkalmazva segítenek teljes körűen biztonságos WLAN-infrastruktúra kialakításában. Az így létrejövő biztonságos és rugalmas megoldással kezelhetők az olyan üzleti kihívások, mint a PCI-megfelelőség, a biztonság- és a kockázatkezelés.

Összefoglalás

A vezeték nélküli hálózatok megváltoztatják a hálózatbiztonság informatikai megközelítését. A vezeték nélküli infrastruktúra fizikai jellemzői és a mobilitás az információ szabadabb, a fizikai határokat kevésbé figyelembe vevő mozgását teszik lehetővé. A vállalatok hatékonyságuk növelése érdekében ráadásul egyre inkább támaszkodnak az információ digitalizálására, és az információ sértetlensége érdekében kidolgozott szabályozói követelmények növekvő számával kénytelenek szembesülni. Az információk, elsősorban az ügyfél- és pénzügyi adatok megfelelő ellenőrzése és biztonsága áll a szabályozó előírások, így az Sarbanes-Oxley törvény, a HIPAA-törvény és a PCI-szabvány középpontjában.

A Cisco a Cisco Secure Wireless megoldást ajánlja az információ és informatikai rendszerek sértetlenségét biztosító architektúraként. A Cisco az egyetlen olyan technológiaszolgáltató, amely az iparágvezető vezeték nélküli biztonsági protokollokat (például WPA és WPA2) olyan a kategóriájában legjobb biztonsági megoldásokkal egyesíti, mint a Cisco NAC-készülék, a Cisco ASA tűzfalak és a Cisco Security Agent. Az eredmény egy olyan biztonsági megoldás, amely nem csupán a pénzügyi, ügyfél-, beteg- és bankkártyaadatok védelmét biztosítja, hanem amely az üzleti megfelelőségi követelmények teljesítését is lehetővé teszi az IT-részleg számára.

További információért kérjük, látogasson el az alábbi weboldalakra:

- Cisco vezeték nélküli biztonsági megoldások: http://www.cisco.com/go/wirelesssecurity
- Cisco egységes vezeték nélküli hálózat: http://www.cisco.com/go/unifiedwireless

Cisco Systems Magyarország Kft.
1123 Budapest, Csörsz u. 45.
Telefon: (1) 225 4600
Fax: (1) 225 4611
www.cisco.hu