**LAN Hálózat Biztonság**

**Fizikai biztonság**

A központban a helyiség, ahol a szerverek és a hálózati eszközök találhatóak, az épület legfelső szintjén van és csak az IT szakember irodáján keresztül lehet bemenni, hogy minél nehezebben elérhető és felfedezhető legyen egy támadó számára. Az épületbe csak a biztonsági őr által beengedett, ott dolgozó személyek mehetnek be munkaidőben. Beléptető rendszer nem üzemel, mivel az alacsony létszámú személyzet miatt feleslegesnek lett ítélve. Kamerák találhatóak az összes szinten. A szerverekhez és a hálózati eszközökhöz, valamint az IT szakember irodájába csak az ott dolgozó IT szakember mehet be arc- és ujjlenyomat azonosítás, és egy hetente változó, 20 karakter hosszú jelszó megadása után.

A többi fiókirodában csak a fiókvezetők irodáján keresztül lehet bemenni a szerverekhez és a hálózati eszközökhöz. Hasonló biztonsági intézkedések vannak, mint a központban. A különbség, hogy nincs biometrikus azonosítás, mivel nincs helyi IT szakember. Csak egyszer használható, 20 karakter hosszú jelszavak vannak, amelyet a központban lévő IT szakember mondhat meg a fiókvezetőnek egyszerű hibák megoldására. Nagyobb hiba esetén az IT szakember személyes megjelenése szükséges. Ezeket egy másik cég (Patent Cégcsoport**)** telepítette és üzemelteti.

**Hitelesítés**

A hálózati eszközök kis száma miatt, valamint azért, mert csak egyetlen ember, az IT szakember férhet hozzá ezekhez, ezért ezeken a helyi adatbázis alapú hitelesítés lett választva egy központi AAA szerver helyett. Mindegyik eszközön jelszó került konfigurálásra a privilegizált EXEC módba való belépéshez. A felhasználónév minden eszköz konzol és VTY vonalán azonos. A jelszavak és a felhasználónevek minden eszközön megegyeznek, és a jelszavak mindegyiken titkosítva vannak tárolva. A jelszó és a felhasználónév a *x. táblázatban* látható.

x. táblázat Jelszavak

|  |  |  |
| --- | --- | --- |
| **Jelszavak** | | |
| **Típus** | **Felhasználónév** | **Jelszó** |
| enable | **-** | 9@PqZ$7sRfT!1a |
| konzol | admin |  |
| VTY |

**Belépés próbálkozások száma**

A brute force támadások elleni védelem érdekében korlátozva lett egy megadott időn belüli belépés próbálkozások száma. A konfigurálás alapján 1 percen belüli 3 helytelen bejelentkezés után 10 percig nem lehet bejelentkezni.

**Inaktív időkorlát**

Ha a hitelesített felhasználók inaktívak, akkor egy idő után automatikusan ki lesznek jelentkeztetve. Erre azért van szükség, hogy illetéktelen felhasználók ne tudják használni ezeket a nyitva maradt bejelentkezéseket. A beállítások szerint egy bejelentkezés nyolc percig lehet inaktív.

**Webes felület**

Az ip http server és az ip http secure-server szolgáltatások kikapcsolásával megszűnt a forgalomirányítók és kapcsolók web-alapú kezelésének lehetősége. Mivel a parancssori kezelés kerül alkalmazásra a hálózati eszközök konfigurálásához, ezek a szolgáltatások feleslegessé váltak. A web-alapú kezelés növelné a hálózati eszközökhöz való jogosulatlan hozzáférés kockázatát, és a támadási felületet. Ez a beállítás minden forgalomirányítón és kapcsolón konfigurálásra került.

**SSH**

A biztonság növelése érdekében a hálózati eszközöket Telnet helyett a forgalmat titkosító SSH-n keresztül lehet VTY vonalon elérni. A nagyobb biztonság érdekében az SSH 2-es verziója került beállításra, és 4096 bit hosszú RSA kulcsokat használ. A felhasználó hitelesítése az IT szakember számítógépén generált, 2048 bit hosszú aszimmetrikus kulcspár használatával történik. A publikus kulcs minden forgalomirányitón manuálisan lett eltárolva, a privát kulcs és a felhasználónév pedig az IT szakember gépén található PuTTy nevű szoftverben el lett mentve egy új, Network\_devices nevű session-be. Így az IT szakembernek csak a konfigurálni kívánt eszköz IP címét kell beírnia. A publikus és a privát kulcs pedig a C:\ssh\keys mappában van elmentve az IT szakember számítógépén public\_key.pub és private\_key.ppk néven.

**Management VLAN**

A kapcsolókon nem az alapértelmezett, 1-es VLAN lett konfigurálva management VLAN-ként, hanem a 37-es. Ezáltal megszűnt annak a veszélye, hogy a kapcsoló konfigurálása során valamelyik 1-es VLAN-ban maradt vagy került interfészhez csatlakozva valaki könnyedén, forgalomirányitó nélkül elérje a kapcsolók üzemeltetési síkját. Emellett meg lett nehezítve a hálózat felderítése a támadó számára, illetve csökkentve lett a VLAN ugrásos támadás sikeressége.

**VLAN**

Az alapértelmezett, 1-es VLAN nem lett alkalmazva a hálózat szegmentálása során. Ezzel meg lett nehezítve a hálózat felderítése a támadó számára, illetve csökkentve lett a VLAN ugrásos támadás sikeressége. Emellett megszűnt annak a veszélye, hogy a kapcsoló konfigurálása során valamelyik 1-es VLAN-ban maradt vagy került interfészhez csatlakozva valaki könnyedén, forgalomirányitó nélkül elérjen egy használatban lévő VLAN-ban található eszközöket.

**Nem használt portok**

Minden nem használt port le lett kapcsolva, access módba lett állítva, és a nem használt (black hole) 29-es VLAN-ba került. Így csak a használt portokon történhet forgalom. Ezzel csökkentve lett a különféle támadások, például a VLAN ugrás, a MAC-cím elárasztás, az ARP hamisítás, valamint a DHCP-hamisítás, vagy a DHCP-kiéheztetés esélye. Azonban ezek a veszélyek továbbra is fennállnak az aktív portokon, ezért ezeken további konfigurációkra van szükség.

**Portbiztonság**

A MAC-cím elárasztás és a DHCP-kiéheztetés ellen portbiztonság lett beállítva a kapcsolók access típusú interfészein, amikhez a végpontok csatlakoznak. A portbiztonság maximum 1 MAC-címet tanul meg sticky módszerrel, ami biztosítja, hogy egy megadott eszközöktől származó forgalomra korlátozódjon a hozzáférés a portokon. A legerősebb biztonságot nyújtó, alapértelmezett megsértési mód, a shutdown beállításával a kapcsolók leállítják a portot, ha eltérést talál az üzenet forrás MAC-címe és a megtanult cím között. A hálózat üzembe helyezése után minden switch futó konfigurációja el lett mentve az indító konfigurációba. Ezáltal biztosítva lett, hogy a kapcsolók csak az előre telepített végpontok MAC-címeit fogadják el újraindításuk után is.

**Trunk portok**

A kapcsolók trunk portjain ki lett kapcsolva a Dynamic Trunking Protocol (DTP) funkció, és be lett állítva, hogy csak az előre létrehozott VLAN-ok forgalmait engedjék át. Ezen kívül meg lett változtatva a native VLAN az alapértelmezett, 1-es VLAN-ról a nem használt 11-es VLAN-ra. Ezzel jelentősen csökkentve lett a VLAN ugrásos támadás kockázata.

**DHCP Snooping**

A DHCP Snooping kapcsolókon való beállításával lett megoldva a védekezés a DHCP-támadások ellen. A DHCP-hamisítás elleni védekezés érdekében a DHCP Snooping funkcióban a kapcsolók trönk portjait, valamint a DHCP-szerverhez csatlakozó portot megbízható (trusted) portként lettek beállítva. Ezzel biztosítva lett, hogy csak az előre telepített DHCP-szerver küldhessen DHCP válaszüzeneteket (DHCPOFFER, DHCPACK, DHCPNAK). A DHCP-kiéheztetés veszélye a nem megbízható (untrusted) portokon a DHCP-üzenetek korlátozásával lett csökkentve. A fogadható üzenetek száma négyre lett korlátozva. A DHCP-snooping minden használt VLAN-ban konfigurálva lett.

**Dinamikus ARP-ellenőrzés**

Az ARP-mérgezés és az ARP-hamisítás ellen a dinamikus ARP-ellenőrzés (DAI) lett konfigurálva a kapcsolókon. A DHCP Snoopinghoz hasonlóan lett beállítva, vagyis csak a szerverekhez csatlakozó és a trönk portok lettek megbízhatók. A nem megbízható portokon a forrás- és cél MAC- és IP-címeket a DHCP Snooping táblája alapján ellenőrzi, és eltérés esetén eldobja az ARP-üzenetet. A DAI minden használt VLAN-ban konfigurálva lett.

**BPDU Guard**

A feszítőfa elleni támadás különféle veszélyeket rejt magában, mint például közbeékelődést vagy szórási vihar keletkezését, ami az egész kapcsolt hálózat leállásához vezethet. Ez a BPDU Guard konfigurálásával lett kiküszöbölve, amely minden access módban és PortFast-tal konfigurált porton be lett állítva. Így, ha ezen portok valamelyikén egy BPDU érkezik, az a port letiltott állapotba kerül.

**Root guard**

A hálózat stabilitása és a feszítőfa protokoll megfelelő működésének érdekében a root guard funkció lett alkalmazva a multilayer switcheken. Bár a hálózatban jelenleg nincsen második rétegben hurok, viszont az esetleges jövőbeli bővítések során keletkezhet. Biztonsági szempontból a root guard használata azért fontos, mert megakadályozza, hogy egy rosszindulatú vagy hibás konfigurációjú eszköz gyökérponti hídként vegye át az irányítást a Spanning Tree protokoll felett. A másodi rétegben levő kapcsolóknál ez a beállítás nem lett alkalmazva, mivel az access típusú portjait a BPDU guard védi. Az egymást összekötő trunk portjain lehetne alkalmazni, de ha hurok keletkezik a hálózatban a későbbi bővítések miatt, akkor a kapcsolók ezen portjain is érkezhet BPDU a gyökérponti hídtól. Ekkor ezen a porton megszűnne a bejövő keretek továbbítása, illetve folyamatosan Syslog üzenetet kapnánk. Mindkét harmadik rétegbeli kapcsoló összes használt és nem használt portján be lett állítva a root guard, hogy a jövőben is biztosítva legyen, hogy minden VLAN-ban az adott harmadik rétegbeli kapcsoló maradjon a gyökérponti híd.

**CDP letiltása**

A Cisco Felderítő Protokoll hasznos hálózati eszközök konfigurálásánál és hibaelhárításánál, viszont CDP-üzenetek elfogásával a támadó fontos információkat tudhat meg a hálózatról. A CDP előnyös a hálózati hibák elhárításához, ezért egy köztes megoldásként CDP-üzenetek küldése csak a hálózati eszközök között engedélyezett, és a végpontok fele pedig tiltott.

**ACL-ek**

A hálózati eszközöket távolról, VTY vonalon csak az IT szakember alhálózatából lehet elérni. Ezért minden hálózati eszközön létre lett hozva egy VTYv4 nevű normál, nevesített és egy VTYv6 nevű kiterjesztett, nevesített ACL, amely a VTY vonalakon csak az IT szakember alhálózatából származó, bemenő forgalmat engedélyezi, és minden mást tilt. Mindegyik telepen mindegyik IPv4-es IT alhálózatból származó forgalmat engedélyezi, így a 10.11.169.0/28, a 10.23.169.0/29 és a 10.37.169.0/29 alhálózatból lehet elérni a hálózati eszközöket távolról. Azért van szükség az összes privát IPv4-es alhálózat engedélyezésére, mivel az interneten keresztül is el tudja érni az IT szakember a más telephelyen lévő hálózati eszközöket a tunneling-nek köszönhetően. Az IPv6 esetében is mindegyik IT alhálózatból (2001:db8:c1c1:abb5::/64, 2001:db8:c1c1:bab3::/64, 2001:db8:c1c1:c1b5::/64) mindegyik épületben lévő mindegyik hálózati eszközt el lehet érni. Az IPv6-os ACE-k célja any.

A management VLAN-okba csak az IT szakember alhálózatából származó forgalom engedélyezett. Ez a feltétel a MANAGEMENTv4 nevű normál, nevesített és MANAGEMENTv6 nevű kiterjesztett, nevesített ACL-ekben lett megfogalmazva, ami a

* KKK-MLS1 VLAN 11
* KKK-MLS2 VLAN 11

interfészén, és a

* DEB-KKK-BR1 G0/0/0.11
* DEB-KKK-BR2 G0/0/0.11
* SZE-KKK-BR1 G0/0/0.11
* SZE-KKK-BR2 G0/0/0.11

alinterfészén a kimenő forgalmat szűri. A forrás alhálózatok ugyanúgy lettek megadva, mint a távoli elérést korlátozó ACL-eknél. Az IPv6-os ACE-k célja any.

Az IT szakember alhálózatát semelyik másik, a cégben dolgozók számára létrehozott alhálózatokból semmilyen protokollon keresztül nem lehet elérni. Minden más forgalom engedélyezett az IT szakember alhálózata felé. Ezt a ITv4 nevű kiterjesztett, nevesített ACL-ek biztosítják, ami a

* KKK-MLS1 VLAN 69
* KKK-MLS2 VLAN 69

interfészén, és a

* DEB-KKK-BR1 G0/0/0.69
* DEB-KKK-BR2 G0/0/0.69
* SZE-KKK-BR1 G0/0/0.69
* SZE-KKK-BR2 G0/0/0.69

alinterfészén a kimenő forgalmat szűri. Az ACE-k célja any. Az ACL-ek csak IPv4-es címeket szűrnek, mivel IPv6-os címmel bárhonnan el lehet érni az alhálózatot és mindent nem lehet tiltani. Azonban az IT szakembernek el kell érnie a többi VLAN-ban lévő számitógépet SSH, RDP vagy ICMP protokollon keresztül. Ezek válasz üzeneteit viszont tiltja az ACL, de ezen protokollok átengedése biztonsági kockázat. Ezért a probléma a következő ACE használatával lett megoldva, ami az ACL elején található és ami engedélyezi a TCP válaszforgalmat:

permit tcp any any established

A vezetéknélküli routerek alhálózatából származó forgalom nem érheti el a többi alhálózatot semmilyen protokollon keresztül, de minden más forgalom engedélyezett. Mivel egyik alhálózatot sem érhetik el, ezért az ACL rövidítése érdekében az egész 10.0.0.0/8 és 2001:db8:c1c1::/48 hálózat elérése lett tiltva. Ezt a WIFIv4 és WIFIv6 nevű kiterjesztett, nevesített ACL-ek biztosítják, ami a

* KKK-MLS1 VLAN 41
* KKK-MLS2 VLAN 41

interfészén, és a

* DEB-KKK-BR1 G0/0/0.41
* DEB-KKK-BR2 G0/0/0.41
* SZE-KKK-BR1 G0/0/0.41
* SZE-KKK-BR2 G0/0/0.41

alinterfészén a bemenő forgalmat szűri. Az összes ACE forrása any. Azonban a Wi-Fi hozzáférés hitelesítése a központi RADIUS szerver biztosítja, illetve a vezetéknélküli forgalomirányítóhoz csatlakozó eszközök a központi DHCP szervertől kapnak IP címet. Ezért a tiltások előtt engedélyezve lett, hogy a szerverek alhálózatát el lehet érni DHCP (67-es UDP port) és RADIUS (1812-es és 1813-as UDP port) protokollal.

**unicast Reverse Path Forwarding (uRPF)**

Minden telephelyen a kapcsolókhoz csatlakozó forgalomirányítók, valamint a harmadik rétegbeli kapcsolók esetében uRPF került konfigurálásra. Ez a beállítás a bemenő forgalmat szűri a forgalomirányítók alinterfészein, illetve a harmadik rétegbeli kapcsolók virtuális interfészein. A csomagok forrás IP-címének érvényességét azért kell ellenőrizni, hogy megakadályozzuk a hamis IP-címekkel végrehajtott túlterheléses támadásokat. Az IP-címhamisítás problémája egyrészt az az, hogy az ilyen forgalom valódi forrása nem követhető vissza, ami megnehezíti a támadások kivédését. Ezenfelül az IP-címhamisítás lehetővé teheti ACL szabályok megkerülését is. Például, ha az IT-szakember VLAN-ját egyik belső alhálózatból sem lehet elérni, viszont egy támadó mégis hozzáférhet, ha egy hamis forrás IP-címet használ. Ezek a biztonsági kockázatok indokolták a strict módú uRPF konfigurálását. Az uRPF beállítások azért a szélső forgalomirányítókra, illetve a harmadik rétegbeli kapcsolókra kerültek, hogy a hamisított csomagok feleslegesen ne jussanak tovább a hálózat belső részeire. Az IPv4-es és az IPv6-os csomagok is szűrve vannak.

**WLAN**

A cégben található vezeték nélküli routereken a cég dolgozói számára létrehozott Wi-Fi SSID szórása le van tiltva, így azt az ott dolgozóknak manuálisan kell beállítaniuk, ha kapcsolódni szeretnének a hálózathoz a vezeték nélküli eszközeikkel. A legmodernebb biztonsági módszer, a WPA3-Enterprise lett engedélyezve. Az AD DS és a RADIUS (  
FreeRADIUS) szerver integrációja lett megvalósítva a Wi-Fi hozzáférés központi hitelesítésére. A felhasználók csatlakozhatnak a hálózathoz a tartomány-hitelesítő adataik használatával. A vezeték nélküli routerek külön VLAN-ban vannak, így a vezeték nélküli eszközöktől származó forgalom jól elkülönül a hálózat többi forgalmától.

A vendégek számára vendég Wi-Fi lett létrehozva, ahol szintén a WPA3-as biztonsági módszer van alkalmazva. A vendégek a tárgyalóban és a konferenciateremben lehelyezett papíron olvashatják a szükséges jelszót a vendég Wi-Fi-hez való csatlakozáshoz.

**OSPFv2 és OSPFv3 hitelesítés**

Az OSPF dinamikus útválasztásának védelmére mindkét verzióban hitelesítés lett beállítva, hogy a támadó az OSPF csomagok megváltoztatásával, vagy hamisak küldésével ne tudja megváltoztatni a forgalomirányítást és ezáltal ne téríthesse el a hálózat forgalmát. Az OSPFv2-nél az egyszerű, szöveges, titkosítatlan jelszó helyett az MD5 kriptográfia hash algoritmus van használva a biztonságosabb hitelesítésre és a csomag sértetlenségének ellenőrzésére. Mindegyik telephelyen minden terület egyedi kulcs és kulcs azonosító párost kapott. Ezek a párosok az *x. táblázatban* láthatóak.

x. táblázat OSPFv2 hitelesítés

|  |  |  |  |
| --- | --- | --- | --- |
| **OSPFv2 hitelesítés** | | | |
| **Telephely** | **Terület** | **Kulcs azonosító** | **Kulcs** |
| Budapest | 0 | 84 | G7pL2qR4sW5kX9zB |
| 5 | 138 | hT8sR0vJ3pW4nY6x |
| 10 | 196 | Q9tM1aE5fV6kL2zY |
| Debrecen | 0 | 121 | A9hbL3kmX457qZ1p |
| Szeged | 0 | 92 | Z8ggJ2evK053dQ9m |

A hálózatban az OSPFv3 hitelesítés IPsec alapú, mely minden OSPFv3 területen egyedi SPI és megosztott kulcs használatával biztosítja a kapcsolatok biztonságát. A nagyobb biztonság érdekében mindegyik telephely mindegyik területéhez egyedi SPI és kulcs páros lett konfigurálva. Így, ha egy terület hitelesítését feltörik, akkor a támadás csak az adott területre tud koncentrálódni. Az SHA-1 hash algoritmus lett alkalmazva. Az SPI és kulcs párosok az *x. táblázatban* találhatóak.

x. táblázat OSPFv3 hitelesítés

|  |  |  |  |
| --- | --- | --- | --- |
| **OSPFv3 hitelesítés** | | | |
| **Telephely** | **Terület** | **SPI** | **Kulcs** |
| Budapest | 0 | 2008 | 3F2A1B8C9D1E4F6A7B8C9D0E1F2A3B4C5D6E7F8A |
| 5 | 12075 | 7A4B1C8D9E2F6A1B8D9E4C5F1A2B3C4D5E6F7A8B |
| 10 | 21478 | 1E2A3B4C5D6E7F8A9B0C1D2E3F4A5B6C7D8E9F0A |
| Debrecen | 0 | 905 | 0A1B2C3D4E5F6A7B8C9D0E1F2A3B4C5D6E7F8A9B |
| Szeged | 0 | 5641 | 9F8E7D6C5B4A3C2D1E0F9A8B7C6D5E4F3A2B1C0D |

**EIGRP hitelesítés**

Az EIGRP által küldött forgalomirányítási információk védelmére hitelesítés lett beállítva. Az egyszerű, szöveges, titkosítatlan jelszó helyett MD5 kriptográfia hash algoritmus van használva a biztonság erősítésére és a csomag sértetlenségének ellenőrzésére. Mivel az EIGRP-nél kötelező a key-chain használata, ezért létre lett hozva egy KEYEIGRP néven. A kulcs a huszonötös azonosítót kapta és végtelen ideig érvényes A kulcs, ami konfigurálásra került a következő: F7#h8m$Q2!xK4pL

**BGP hitelesítés**

A BGP hitelesítés a forgalomirányítási információk védelmére szolgál. Az egyszerű, szöveges, titkosítatlan jelszó helyett az MD5 hash algoritmus van használva a biztonság erősítésére és a csomag sértetlenségének ellenőrzésére. IPv4-nél és IPv6-nál ugyanazok a kulcsok lettek alkalmazva, viszont a kulcsok eltérnek telephelyenként. A kulcsok a *x. táblázatban* találhatóak.

x. táblázat BGP hitelesítés

|  |  |
| --- | --- |
| **BGP hitelesítés** | |
| **Telephely** | **Kulcs** |
| Budapest | D3s6!aP9v#4@bQ8R |
| Szeged | R#7qT!m4L0s3^N2x |
| Debrecen | 8Y%jLz9!F@1r2Vp# |

**Passzív interfész**

Az OSPF konfigurálásánál a végpontok felé néző interfészek passzívok lettek. Ez a beállítás növeli a biztonságot az útválasztási információk terjesztésének korlátozásával, csökkentve a potenciális támadási felületet. Nagyon sok passzív interfészt kellett volna beállítani, ezért az egyszerű konfigurálás érdekében a ”passive-interface default” parancs lett alkalmazva és a ”no passive-interface” paranccsal lettek beállítva a nem passzív interfészek.

**HSRP hitelesítés**

A HSRP-vel konfigurált forgalomirányítók közötti üzenetváltások biztonságának érdekében hitelesítés lett beállítva. A nagyobb biztonság elérése és az üzenetek sértetlenségének ellenőrzése érdekében a hitelesítés az MD5 hash algoritmust használja az egyszerű, szöveges, titkosítatlan jelszó helyett. Minden telephelyen más kulcs van használva, de telephelyenként az IPv6-os és IPv4-es csoport ugyanazt a kulcsot használja. Ezek a *x. táblázatban* találhatóak.

x. táblázat HSRP hitelesítés

|  |  |
| --- | --- |
| **HSRP hitelesítés** | |
| **Telephely** | **Kulcs** |
| Budapest | T7v@2u$M!qW9bZ3^ |
| Szeged | eR5&hX4!jN8p$W1m |
| Debrecen | Y8^fS3\*zZ2@qJ7!k |

**Direkt kulcsok**

A dinamikus forgalomirányító protokollok és a HSRP hitelesítésére direkt kulcsok lettek konfigurálva. Ennek okai a következők:

* Egyszerűbb konfigurálni a hálózati eszközöket direkt kulccsal, így gyorsabb a hálózat telepítése. Emellett nagy mértékben csökken a hibázás esélye a telepítés során.
* Könnyebb nyilvántartani a hitelesítéshez használt kulcsokat. Ez segíti a hálózat karbantartását
* Nagyon sokféle hitelesítés és azokon belül is sokféle kulcs van alkalmazva, ezáltal sok key-chain kellett volna létrehozni a hálózati eszközökön. Ez rossz hatással lett volna a hálózat teljesítményére

**ASA**