Kapcsolási, forgalomirányítási és vezeték nélküli kommunikációs alapok

LAN biztonsági alapfogalmak

Biztonsági fenyegetések és sebezhetőségek

Fenyegetések típusai

- **Információlopás** - számítógép feltörése bizalmas információk megszerzése céljából. Az információ felhasználható vagy értékesíthető különböző célokra. Például: egy szervezet tulajdonát képező kutatási és fejlesztési információk eltulajdonítása.
- **adatvesztés és manipuláció** - számítógép feltörése adatrekordok megsemmisítése vagy módosítása céljából. Példa az adatvesztésre: vírus küldése, amely leformázza a számítógép merevlemezét. Példa az adatmanipulációra: nyilvántartó rendszer feltörése egy tétel egységárának megváltoztatása céljából.
- **Azonosító lopás** - az információlopás egy formája, amikor személyes adatokat tulajdonítanak el valaki személyazonosságának átvétele céljából. Ezt az információt felhasználva egy támadó hozzájuthat hivatalos dokumentumokhoz, hitelt igényelhet és jogosulatlan Internetes vásárlásokat végezhet. Az azonosító lopás egyre növekvő probléma, amely évente több milliárd dollár kárt okoz.
- **Szolgáltatás megszakítás** - a jogosult felhasználók megakadályozása a szolgáltatásokhoz való hozzáférésben. Példa: szolgáltatásmegtagadás (DoS) típusú támadás a kiszolgálók, hálózati eszközök vagy hálózati kommunikációs kapcsolatok ellen.

Sebezhetőségek típusai

A sebezhetőség a hálózat és az eszköz gyengeségének fokmérője.

- **Technológiai sebezhetőségek** (TCP/IP protokoll gyengeség, operációs rendszer gyengeség, hálózati eszköz gyengeség).
- **Konfigurációs biztonsági rések** (nem biztonságos felhasználói fiókok, rendszerfiókok könnyen kitalálható jelszavakkal, rosszul konfigurált internetes szolgáltatások, nem biztonságos alapértelmezett beállítások, rosszul konfigurált hálózati berendezések).
- **Házirend biztonsági rései** (írásbeli biztonsági szabályzat hiánya, politika, a hitelesítés szabályozásának hiánya, a hozzáférés-vezérlés nem kielégítő, a szoftver- és hardvertelepítés és a módosítások nem követik a házirendet, nincs katasztrófa utáni helyreállítási terv).

Fizikai fenyegetések

- **Hardver fenyegetések** - A szerverek, a munkaállomások, a routerek, a switchek vagy a kábelezés fizikai megrongálása.
- **Környezeti fenyegetések** - Szélsőséges hőmérséklet (túl meleg vagy hideg) vagy szélsőséges

páratartalom (túl nedves vagy száraz).

- **Elektromos veszélyek** - Feszültség-tüskék, alacsony feszültségszint (feszültségesés), szűrés nélküli tápellátás (zaj), áramszünet.
- **Karbantartási veszélyek** - Az elektromos összetevők hanyag kezelése (elektrosztatikus feltöltődés), kritikus alkatrészek hiánya, hibás kábelezés és hiányos feliratozás.

E problémák megoldása érdekében szabályzatot kell létrehozni és végrehajtani a fizikai biztonságra is.

Hálózati támadások

Kártevőtípusok

A „malware” a rosszindulatú szoftverek rövid neve (malicious software). Ez a kód vagy szoftver kifejezetten az adatok, számítógépek és hálózatok károsítására, megzavarására, adatok ellopására, vagy törvénytelen műveletek végrehajtására készült.

- **Vírusok** - A számítógépes vírus egy olyan típusú malware, amely a terjedéshez beilleszti saját másolatát egy másik programba, ezáltal annak szerves része lesz. Egyik számítógépről a másikra terjed, fertőzéseket hagyva hátra. A vírusok súlyossága az enyhén bosszantó hatásúaktól kezdve az adatokat vagy szoftvereket károsító és szolgáltatás-megtagadást (DoS) okozókig terjed. Szinte az összes vírus egy futtatható fájlhoz kapcsolódik, ami azt jelenti, hogy a vírus benne van a rendszerben, de addig nem lesz aktív és nem képes terjedni, amíg a felhasználó le nem futtatja vagy meg nem nyitja a fertőzött állományt. A gazdakód végrehajtásakor a víruskód is végrehajtásra kerül. Normális esetben a gazdaprogram a vírusfertőzés után is működőképes marad. Egyes vírusok azonban felülírják a másik programot saját másolatukkal, ami teljesen elpusztítja a gazdaprogramot. A vírusok akkor terjednek, amikor a szoftver vagy dokumentum, amelyhez csatolva vannak, a hálózat, egy lemez, egy fájlmegosztás vagy egy email melléklet használatával átkerül az egyik számítógépről a másikra.
- **Férgek** - hasonlóak a vírusokhoz, mivel működőképes másolatokat készítenek önmagukról, és ugyanolyan típusú károkat okozhatnak. A fertőzött gazdafájlt igénylő vírusokkal ellentétben a férgek önálló szoftverek, és nem igényelnek gazdaprogramot vagy emberi segítséget a terjedéshez. Egy féregnek nem kell kapcsolódnia egy programhoz, hogy megfertőzze a gazdagépet, és belépjen a számítógépbe a rendszer biztonsági résén keresztül. A férgek a rendszer funkcióit használják ki, hogy segítség nélkül terjedhessenek a hálózaton.
- **Trójai programok** - A trójai egy másik típusú rosszindulatú program, nevét a görögök által használt falóról kapta, amelyet Trója bevételére alkalmaztak. Ez egy valódinak látszó káros szoftver. Becsapja a felhasználókat, hogy azok letöltések és végrehajtsák a saját rendszerükben. Az aktiválódásuk után különféle támadásokat indítanak a gazdagép ellen, kezdve azzal, hogy irritálják a felhasználót (állandóan felugró ablakokkal vagy az asztal megváltoztatásával), egészen a károkozásig (fájlok törlése, adatok lopása, vagy vírusok aktiválása és terjesztése). A trójaiak képesek kiskapukat (back doors) is létrehozni, hogy a rosszindulatú támadók hozzáférhessenek a rendszerhez.

Megjegyzés: A vírusokkal ellentétben a trójai programok nem más fájlok megfertőzésével

reprodukálódnak, önmagukat másolják. A trójaiak terjedéséhez felhasználói beavatkozás szükséges, például egy email csatolmány megnyitása vagy egy fájl internetről történő letöltése és futtatása.

Hálózati támadások

- **Felderítéses támadások** - Rendszerek, szolgáltatások és sebezhetőségi pontok felkutatása (nslookup, whois, ping, port pásztázás).
- **Hozzáférési támadások** - Adatok, rendszerhozzáférések és felhasználói jogok illetéktelen kezelése (jelszó elleni támadások, bizalom kihasználás, portátirányítás és közbeékelődés (man-in-the middle)).
- **Szolgáltatásmegtagadási támadások** - Hálózatok, rendszerek és szolgáltatások megbénítása vagy elrontása (DoS. DDoS).

Hálózati támadás elkerülése

Mélységi védelem

A hálózati támadások elkerülése érdekében elsősorban az eszközöket kell megvédeni: a routereket, a switch-eket, a kiszolgálókat és a munkaállomásokat. Sok szervezet alkalmaz mélységi védelmet (defense-in-depth), más néven a védelem rétegzésének stratégiáját. Ez a hálózati eszközök és szolgáltatások kötelékben való működését követeli meg.

Számos biztonsági eszköz és szolgáltatás működik a felhasználók és a berendezések védelme érdekében:

- **VPN** - A router feladata, hogy biztonságos VPN-szolgáltatásokat nyújtson a vállalati telephelyek között, valamint titkosított alagutak segítségével biztosítsa a távoli felhasználók hozzáférését.
- **ASA tűzfal** - Ez a dedikált eszköz állapottartó tűzfalszolgáltatásokat biztosít. Garantálja a belülről induló adatforgalom kijutását és visszatérését, viszont megakadályozza a kívülről érkező kapcsolati kezdeményezéseket a belső számítógépek irányába.
- **IPS** - A behatolásmegelőző rendszer (Intrusion Prevention System, IPS) kártevőket, hálózati támadások mintáit és egyebeket keresve monitorozza a bejövő és kimenő adatforgalmat. Ha támadást észlel, azonnal megállítja.
- **ESA/WSA** - Az e-mail biztonsági célberendezés (Email Security Appliance, ESA) kiszűri a kéretlen és gyanús leveleket. A webes biztonsági célberendezés (Web Security Appliance, WSA) kiszűri a kártevőket terjesztő, ismert vagy gyanús weboldalakat.
- **AAA Server** - Ez a szerver egy biztonságos adatbázisban tárolja a hálózati eszközök elérésére és kezelésére jogosult személyeket. A hálózati eszközök ezen adatbázis segítségével hitelesítik a rendszergazda felhasználókat.

Biztonsági mentések

A konfigurációk és az adatok biztonsági mentése az adatvesztés elleni védelem egyik leghatékonyabb

módja. Az adatmentés a számítógépen lévő információk egy példányát olyan cserélhető adathordozón tárolja, amelyet biztonságos helyen lehet tartani. Az infrastruktúra eszközök konfigurációs beállításairól és IOS-képfájljairól is mentést kell készíteni FTP- vagy hasonló jellegű fájlkiszolgálóra. Ha a számítógép vagy a router hardvere meghibásodik, az adatok és a konfiguráció visszaállítható a biztonsági másolatból.

Az adatok biztonsági mentését a házirendben meghatározott rendszeres időközönként el kell végezni. Az adatmentéseket általában külső helyszínen (offsite) tárolják, hogy megvédjék a biztonsági másolatot, ha bármi történne a fő létesítménnyel. A Windows operációs rendszert futtató számítógépek rendelkeznek biztonsági mentés és visszaállítás segédprogrammal. Ez fontos, mivel a felhasználók másolatot készíthetnek adataikról egy másik meghajtóra vagy egy felhőalapú tárhelyre.

Frissítés és hibajavítás

A legutóbbi fejlesztések eredményeinek folyamatos alkalmazása eredményesebb védekezést tesz lehetővé a támadások ellen. Amint egy új kártevő megjelenik, a vállalkozásoknak frissíteniük kell víruskereső szoftvereik adatbázisát.

A féregtámadások elkerülésének leghatékonyabb módja az operációs rendszer biztonsági frissítéseinek telepítése és a sebezhető rendszerek hibajavítása (patch). A nagy számosságú rendszerek felügyelete maga után vonja egy általános szoftvercsomag (operációs rendszer és kliens alkalmazások) létrehozásának szükségességét, amely telepítéskor vagy frissítéskor használható. Amennyiben a biztonsági követelmények változnak, a már üzemelő rendszereken is szükség van a biztonsági frissítések telepítésére.

Hitelesítés, jogosultság kezelés és naplózás

Minden hálózati eszközt úgy kell konfigurálni, hogy csak az engedélyezett személyek férhessenek hozzá. A hitelesítés, jogosultság kezelés és naplózás (Authentication, Authorization, and Accounting, AAA vagy tripla A) olyan biztonsági szolgáltatások, amelyek a hálózati eszközök hozzáférésszabályozásának alapját alkotják.

Az AAA vezérli, hogy ki férhet hozzá a hálózathoz (hitelesítés), mit csinálhat belépés után (jogosultság) és nyomon követi a használat során végrehajtott műveleteket (naplózás).

Tűzfalak

A tűzfal az egyik leghatékonyabb biztonsági eszköz, amely a belső hálózati felhasználók külső veszélyektől való megvédésére szolgál. A tűzfal úgy védi a számítógépeket és hálózatokat, hogy megakadályozza a belső hálózatba irányuló nem kívánt adatforgalmat.

A tűzfal két vagy több hálózat között helyezkedik el, ellenőrzi a köztes forgalmat, és véd a jogosulatlan hozzáféréstől is. A felső ábra azt mutatja be, hogy a tűzfal engedélyezi a belső hálózatból induló forgalom kilépését, majd visszatérését. Az alsó topológia pedig azt szemlélteti, hogy miként blokkolja a külső hálózatból (pl.: az internetről) a belső hálózat felé indított adatforgalmat.

A tűzfal bizonyos szolgáltatásokhoz ellenőrzött hozzáférést biztosíthat külső felhasználók számára. A külső felhasználók számára elérhető szerverek egy speciális hálózatban kapnak helyet, amelyet demilitarizált zónának (DMZ, demilitarized zone) neveznek. A hálózati rendszergazdák speciális irányelveket alkalmazhatnak a DMZ-hálózathoz kapcsolódó állomásokra.

Tűzfalak típusai

A tűzfalaknak számos formája létezik. Ezek különféle technikákat használnak annak meghatározására, hogy mi számít engedélyezett és mi tiltott hálózati hozzáférésnek. Az alkalmazott módszerek a következők:

- **Csomagszűrés** - IP- vagy MAC-cím alapján akadályozza meg vagy engedélyezi a hozzáférést.
- **Alkalmazás szűrés** - Tiltja vagy engedélyezi a hozzáférést bizonyos alkalmazások számára portszámuk alapján.
- **URL-szűrés** - Tiltja vagy engedélyezi weboldalak elérését adott URL vagy kulcsszó alapján.
- **Állapotalapú csomagvizsgálat (Stateful Packet Inspection, SPI)** - A bejövő csomagok csak a belső hálózat állomásairól kezdeményezett kérések válaszcsomagjai lehetnek. A nemkívánatos csomagok külön engedély hiányában kiszűrésre kerülnek. Az SPI képes arra is, hogy felismerjen és kiszűrjön bizonyos támadástípusokat, például a szolgáltatás megtagadást (DoS).

Végpontok biztonsága

A végpont vagy állomás olyan egyedi számítógépes rendszer vagy eszköz, amely hálózati ügyfélként működik. Gyakori végpont típusok a laptopok, az asztali számítógépek, a szerverek, az okostelefonok és a tabletek. Az állomások biztonsága az egyik legnagyobb kihívás a hálózati rendszergazda munkájában, mivel itt az emberi tényezőt is számításba kell venni. A vállalatnak rendelkezni kell jól dokumentált szabályzattal és a munkavállalóknak be kell tartaniuk az abban leírtakat. Ezenkívül az alkalmazottakat fel kell készíteni a hálózat megfelelő használatára is. A házirend szabályok tartalmazzák a víruskereső és behatolás megelőző szoftverek használatának módját. A minden részletre kiterjedő állomásbiztonsági megoldások a hálózati hozzáférés vezérlésén alapulnak.

Eszközbiztonság

Cisco AutoSecure

A hálózati területen működő eszközök biztonságának fenntartása kiemelt figyelmet kíván. Egy új rendszer telepítése után az eszköz biztonsági beállításai az alapértelmezett értéket kapják. A legtöbb esetben ez a biztonsági szint nem elegendő. Cisco routerek esetében az AutoSecure szolgáltatás segít a rendszer biztonságossá tételében.

```
Router# auto secure
                --- AutoSecure Configuration ---
*** AutoSecure configuration enhances the security of
the router but it will not make router absolutely secure
from all security attacks ***
```

A beállítás néhány egyszerű lépésből áll, amelyek alkalmazhatók a legtöbb operációs rendszer esetében is:

- Az alapértelmezett felhasználóneveket és jelszavakat azonnal meg kell változtatni.
- A rendszer erőforrásaihoz való hozzáférést csak az erre jogosult személyek számára szabad engedélyezni.
- A szükségtelen szolgáltatásokat és alkalmazásokat lehetőség szerint ki kell kapcsolni vagy le kell törölni.

Mivel a gyártótól szállított berendezések hosszabb időt is tölthetnek raktárakban, nincsenek naprakész állapotban. Fontos, hogy beüzemelés előtt frissítsük a szoftvereket és telepítsük a biztonsági javításokat.

Jelszavak

A hálózati eszközök védelme érdekében fontos az erős jelszavak használata. Kövessük az alábbi szabványos irányelveket:

- Használjunk legalább 8, de inkább 10, vagy annál több karakterből álló jelszavakat. A hosszabb jelszó biztonságosabb.
- Alkalmazzunk bonyolult jelszavakat. Legyenek bennük kis- és nagybetűk, számok, speciális karakterek és szóközök, minden, ami megengedett.
- A jelszavakban kerüljük az ismétlődéseket, gyakori szavakat, betű- vagy számsorozatokat, felhasználóneveket, rokonok vagy háziállatok neveit, életrajzi adatokat, mint a születési dátumok, azonosító számok, szülők nevei, vagy bármely könnyen azonosítható információ.
- Írjuk szándékosan rosszul a kiválasztott szót. Például: Smith = Smyth = 5mYth vagy Security = 5ecur1ty.
- Cseréljük gyakran a jelszavakat. Így ha a jelszó mégiscsak kitudódik, a támadónak kevesebb ideje marad annak használatára.
- Ne írjuk le a jelszavakat és ne hagyjuk őket látható helyen, az asztalon vagy a monitoron.

Megjegyzés: Cisco eszközökön a vezető szóközök törlődnek a jelszavakból, de az első karakter után begépeltek megmaradnak. Erős jelszót kapunk, ha a szóköz billentyű segítségével több szóból álló kifejezést hozunk létre. Ezt jelmondatnak (passphrase) is hívják. Egy jelmondatot könnyebb megjegyezni mint egy bonyolult jelszót. Hosszabb és nehezebb is kitalálni.

További jelszóbiztonsági beállítások

Az erős jelszavak is csak akkor hasznosak, ha titokban maradnak. Cisco router és switch esetében a következő lépések segíthetik a jelszavak titokban tartását:

- A szöveges jelszavak titkosítása
- A minimális elfogadható jelszóhossz beállítása
- A jelszótalálgatás (brute-force) típusú támadások megakadályozása
- Az inaktív, EXEC módú hozzáférés kiléptetése meghatározott idő elteltével

A **service password-encryption** parancs megakadályozza a jogosulatlan személyeket abban, hogy

megnézhessék a konfigurációs állományban lévő szöveges jelszavakat (lásd ábra). Ez a parancs titkosítja az összes egyszerű jelszót. Figyeljük meg a példában, hogy a „cisco” jelszó titkosított formája „03095A0F034F”.

A jelszavak minimális hosszának biztosítására használjuk a **security passwords min-length length** parancsot globális konfigurációs módban. A példában minden új jelszónak legalább nyolc karakterből kell állnia.

A támadók jelszótörő szoftvert használhatnak egy hálózati eszköz ellen történő brute-force támadására. Ez a támadás újra és újra megpróbálja kitalálni az érvényes jelszavakat, amíg az egyik be ne válik. Használjuk a **login block-for # attempts # within #** globális konfigurációs parancsot az ilyen típusú támadások megakadályozására. A példában a **login block-for 120 attempts 3 within 60** parancs letiltja a bejelentkezést 120 másodperc időtartamra, ha 3 sikertelen kísérletet érzékel 60 másodpercen belül.

A rendszergazdák figyelme is kihagyhat, és véletlenül egy EXEC módú munkamenetet hagyhatnak nyitva a terminálon. Ez lehetővé teszi egy belső támadó számára az eszköz konfigurációjának módosítását vagy törlését.

Alapértelmezés szerint a Cisco eszközök 10 perces inaktivitás után kijelentkeznek az EXEC munkamenetből. Ezt az értéket azonban az **exec-timeout** perc másodperc vonali konfigurációs paranccsal csökkenthetjük. A parancs alkalmazható konzol, aux és vty vonalakon is. A példában szereplő parancs automatikusan kilépteti a vty vonalon levő inaktív felhasználót 5 perc 30 másodperc tétlenség után.

```
R1(config)# service password-encryption
R1(config)# security passwords min-length 8
R1(config)# login block-for 120 attempts 3 within 60
R1(config)# line vty 0 4
R1(config-line)# password cisco
R1(config-line)# exec-timeout 5 30
R1(config-line)# transport input ssh
R1(config-line)# end
R1#
R1# show running-config | section line vty
line vty 0 4
 password 7 094F471A1A0A
 exec-timeout 5 30
 login
 transport input ssh
R1#
```

Az SSH engedélyezése

A Telnet leegyszerűsíti a távoli eszközök elérését, de nem biztonságos. A Telnet csomagokban lévő adatok titkosítás nélkül kerülnek átvitelre. Éppen ezért a biztonságos távoli eléréshez nagyon ajánlott az SSH engedélyezése az eszközön.

Az SSH-támogatás Cisco eszközön való konfigurálásának négy lépése:

1. lépés Konfiguráljunk egy egyedi eszköznevet. Az eszköznek az alapértelmezettől eltérő, egyedi állomásnévvel kell rendelkeznie.

2. lépés Az IP-tartománynév beállítása. Konfiguráljuk a hálózat IP-tartománynevét az ip-domain name globális konfigurációs paranccsal.

3. lépés Hozzunk létre kulcsot az SSH-forgalom titkosításához. Az SSH titkosítja a forrás és a cél közötti forgalmat. Ehhez azonban egyedi hitelesítési kulcsot kell generálni a **crypto key generate rsa general-keys modulus** *bitek száma* globális konfigurációs parancs használatával. A *bitek száma* határozza meg a kulcs méretét, amely 360 és 2048 között érték lehet. Minél nagyobb a szám, annál biztonságosabb a kulcs. Nagyobb bitérték esetén azonban tovább tart az információk titkosítása és visszafejtése. Az ajánlott minimális modulus hossz 1024 bit.

4. lépés Helyi adatbázis bejegyzés ellenőrzése vagy létrehozása. Hozzunk létre helyi felhasználót. Erre szolgál a **username** globális konfigurációs parancs. A példában a **secret** paraméter szerepel, így a jelszó titkosítva lesz MD5 használatával.

5. lépés Hitelesítés a helyi adatbázisban. A **login local** vonali konfiguráció paranccsal a vty vonal használata a helyi adatbázisból történő hitelesítéssel történik.

6. lépés Engedélyezzük a vty vonalon bejövő SSH-munkameneteket. Alapértelmezés szerint a vty vonalakon nem engedélyezett a bejövő kapcsolat. A **transport input [ssh | telnet]** paranccsal több bemeneti protokollt is megadhatunk, beleértve a Telnetet és az SSH-t is.

A példában az R1 router a span.com tartományban van. Ez az információ a **crypto key generate rsa general-keys modulus** parancsban megadott bitértékkel együtt a titkosítási kulcs létrehozásához szükséges.

A következő parancsban létrejön egy Bob nevű felhasználó a helyi adatbázisban. Végül a vty vonalak konfigurációja következik, amely szerint a bejelentkezések a helyi adatbázisból kerülnek hitelesítésre, és csak SSH-munkamenetek jöhetnek létre.

```
Router# configure terminal
Router(config)# hostname R1
R1(config)# ip domain name span.com
R1(config)# crypto key generate rsa general-keys modulus 1024
The name for the keys will be: Rl.span.com % The key modulus size is 1024
bits
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
Dec 13 16:19:12.079: %SSH-5-ENABLED: SSH 1.99 has been enabled
R1(config)#
R1(config)# username Bob secret cisco
R1(config)# line vty 0 4
R1(config-line)# login local
R1(config-line)# transport input ssh
R1(config-line)# exit
R1(config)#
```

Nem használt szolgáltatások letiltása

A Cisco routerek és switch-ek bekapcsolásakor sok olyan szolgáltatás is elindul, amelyekre esetleg nincs szükség a hálózatban. Tiltsuk le a nem használt szolgáltatásokat a rendszererőforrások (például a CPU és a RAM) megőrzése érdekében, egyúttal megakadályozva a támadókat ezen szolgáltatások kihasználásában. Az alapértelmezés szerint bekapcsolt szolgáltatások típusa az IOS verziójától függően változhat. Például az IOS-XE esetében csak HTTPS- és DHCP- portok lesznek nyitva. Ezt a **show ip ports all** paranccsal ellenőrizhetjük (lásd kimenet).

```
Router# show ip ports all
Proto Local Address               Foreign Address             State
PID/Program Name
TCB       Local Address               Foreign Address             (state)
tcp   :::443                       :::*                        LISTEN
309/[IOS]HTTP CORE
tcp   *:443                        *:*                         LISTEN
309/[IOS]HTTP CORE
udp   *:67                          0.0.0.0:0
387/[IOS]DHCPD Receive
Router#
```

Az IOS-XE előtti IOS-verziók a **show control-plane host open-ports** parancsot használják. Ezt a parancsot azért említjük, mert régebbi eszközökkel is sokszor találkozhatunk. A kimenet hasonló. Figyeljük meg azonban, hogy ez a régebbi router HTTP-kiszolgálót és a Telnetet futtat, amelyek nem biztonságosak. Mindkét szolgáltatást le kell tiltani. A HTTP kikapcsolása a **no ip http server** globális konfigurációs paranccsal történik. A Telnet letiltása és csak az SSH engedélyezése a transport input ssh vonali konfigurációs paranccsal lehetséges.

```
Router# show control-plane host open-ports
Active internet connections (servers and established)
Prot        Local Address      Foreign Address                 Service
State
 tcp                *:23                *:0                    Telnet
LISTEN
 tcp                *:80                *:0                 HTTP CORE
LISTEN
 udp                *:67                *:0            DHCPD Receive
LISTEN
Router# configure terminal
Router(config)# no ip http server
Router(config)# line vty 0 15
Router(config-line)# transport input ssh
```