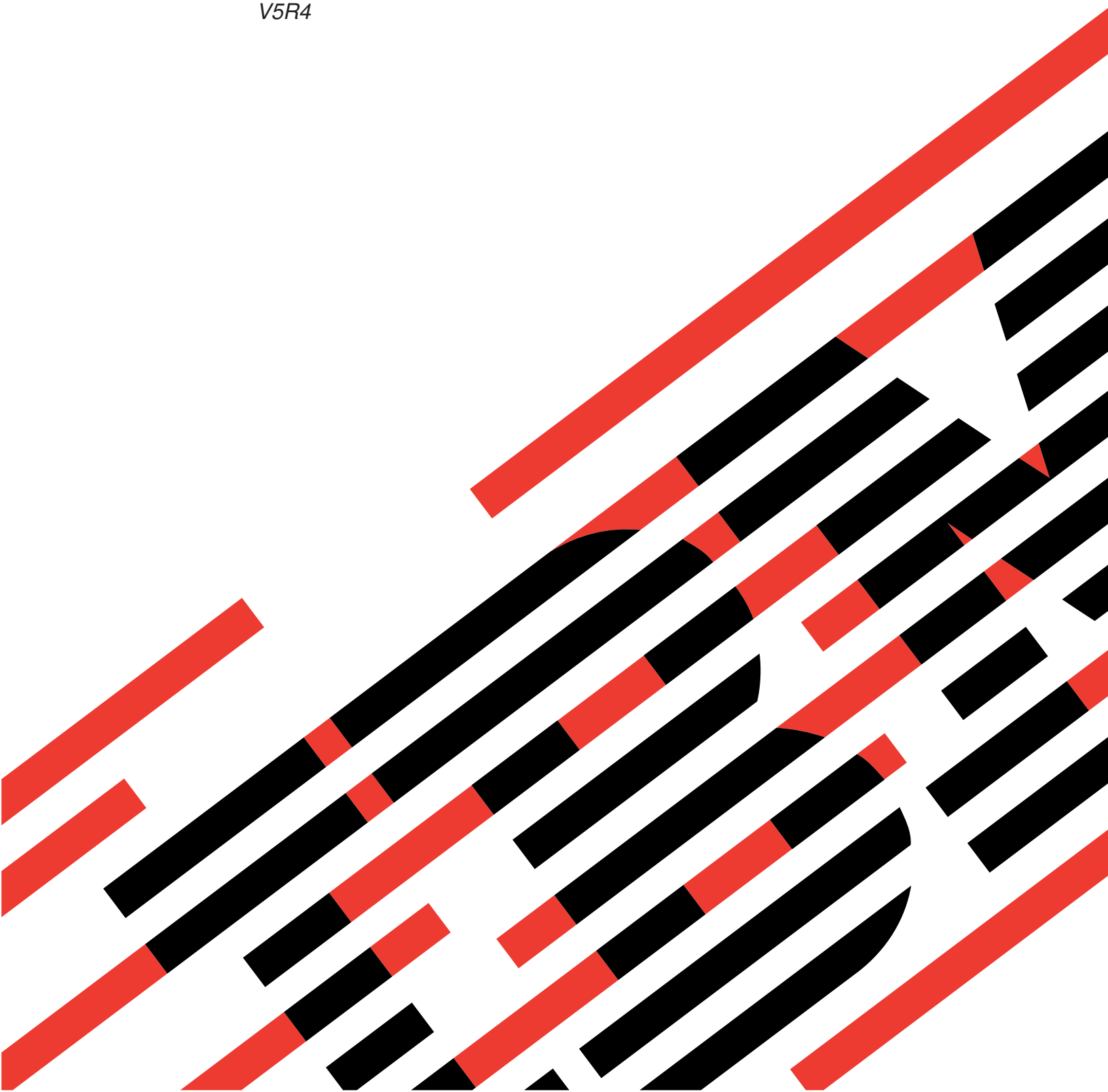
IBM Systems - iSeries

Biztonság
Az iSeries és az Internet biztonsága

V5R4



IBM Systems - iSeries

Biztonság
Az iSeries és az Internet biztonsága

V5R4

Megjegyzés

Mielőtt a jelen leírást és a vonatkozó terméket használná, olvassa el a “Nyilatkozatok” oldalszám: 35 helyen lévő tájékoztatót.

Hetedik kiadás (2006. február)

Ez a kiadás a V5R4M0 szintű IBM i5/OS (száma: 5722-SS1) termékre, és minden azt követő változatra és módosításra vonatkozik, amíg ez másképpen nincs jelezve. Ez a verzió nem fut minden csökkentett utasításkészletű (RISC) rendszeren és CISC modellen.

Tartalom

Az iSeries és az Internet biztonsága

A hálózat fejlődésében nagy lépés az Internet elérése a helyi hálózatról (LAN), amely megköveteli, hogy újra áttekintse a biztonsági követelményeket.

Szerencsére az IBM @server iSeries szerver beépített szoftver megoldásokkal és biztonsági felépítéssel járul ahhoz hozzá, hogy erős védelmet építsen ki a lehetséges Internet biztonsági csapdákkal és behatolókkal szemben. Az iSeries biztonsági ajánlatainak megfelelő használata garantálja, hogy ügyfelei, alkalmazottai és üzleti partnerei megkaphatják az üzletkötéshez számukra szükséges adatokat biztonságos környezetben.

Az itt található információkat felhasználhatja saját maga oktatására a jól ismert biztonsági fenyegetésekről, továbbá a kockázatok és az Internet, valamint az e-business célok kapcsolatáról. Tanulmányozhatja azt is, hogyan mérheti fel a kockázatokat, összevetve őket a különféle biztonsági beállítások használatából eredő előnyökkel, amelyet az iSeries nyújt az ilyen kockázatok kezelésére. Végül, meghatározhatja azt is, hogyan lehet felhasználni ezeket az információkat a hálózatbiztonsági terv elkészítéséhez, amely eleget tesz az üzleti igényeknek.

Nyomtatható PDF

A témakör az itt leírtak PDF változatának megtekintését vagy nyomtatását ismerteti.

A PDF változat megtekintéséhez vagy letöltéséhez válassza ki az iSeries és az Internet biztonsága (416 KB vagy 60 oldal).

Az alábbi kapcsolódó témaköröket is megtekintheti vagy letöltheti:

- Intrusion detection (kb. 160 KB). Létrehozhat behatolást észlelő szabályzatot, amely megvizsgálja a TCP/IP hálózaton keresztül érkező gyanús behatolási kísérleteket, mint például a helytelenül létrehozott IP csomagokat. Írhat is egy olyan alkalmazást, amely elemzi az ellenőrző adatot és riportot a biztonsági adminisztrátor számára, amikor elkezdődik hasonló TCP/IP behatolás.
- Vállalati azonosság leképezés (EIM) (kb. 700 KB). A Vállalati azonosság leképezés (EIM) által biztosított mechanizmus lehetővé teszi személyek és más entitások (például szolgáltatások) leképezését a vállalat különböző felhasználói nyilvántartásaiban meghatározott megfelelő felhasználói azonosságokra.
- Single signon (kb. 600 KB). Az egyszeri bejelentkezés csökkenti a felhasználható által végrehajtandó bejelentkezések számát, valamint a jelszavak számát is, amelyekkel a felhasználó elérheti a különféle alkalmazásokat és szervereket.
- Rendszerbiztonság tervezése és beállítása (kb. 3500 KB).

PDF fájlok mentése

A PDF fájl munkaállomáson történő mentése megjelenítés vagy nyomtatás céljából:

1. Kattintson a jobb egérgombbal a PDF fájlra a böngészőjében (kattintás a jobb oldali egérgombbal a fenti hivatkozásra).
2. Kattintson a PDF helyi mentésére szolgáló opcióra.
3. Válassza ki azt a könyvtárat, ahová menteni kívánja a PDF fájlt.
4. Kattintson a **Mentés** gombra.

Adobe Acrobat Reader letöltése

A PDF állományok megtekintéséhez vagy nyomtatásához telepített Adobe Acrobat Reader programra van szükség.

Ingyenes példányát letöltheti az Adobe honlapjáról (www.adobe.com/products/acrobat/readstep.html) .

Kapcsolódó fogalmak

Behatolás felismerés

Vállalati azonosság leképezés (EIM)

Egyetlen bejelentkezés

Rendszerbiztonság tervezése és beállítása

---

iSeries és Internet biztonsági megfontolások

Áttekintést nyújt az iSeries biztonsági erősségeiről és lehetőségeiről.

A második kérdésre (Mit kell tudnom a biztonság és az Internet kapcsolatáról?) az a válasz , hogy ez attól függ, hogyan akarja használni az Internetet. Az Internethez kapcsolódó biztonsági kérdések igen jelentősek. Hogy melyik kérdéssel kell foglalkoznia, az azon alapszik, hogyan tervezi az Internet használatát. Az első ügylete az Internettel az lehet, hogy hozzáférést biztosít a belső hálózat felhasználóinak a világhálóhoz és az Internet e-mail funkcióhoz. Szándékában állhat érzékeny információk átvitele is az egyik helyről a másikra. Végső fokon tervezheti azt, hogy az Internetet elektromos kereskedelem céljára használja, vagy hogy létrehoz egy extranet hálózatot a vállalat és üzleti partnerei, valamint beszállítói között.

Mielőtt az Internet részévé válna, gondolja végig, mit akar csinálni és hogyan akarja azt csinálni. Az Internet használatáról és az Internet biztonságáról szóló döntés meghozatala igen bonyolult. Hasznos lehet áttekinteni az IBM Systems Szoftver információs központ *Forgatókönyv: JKL Toy Company e-business tervek* című lapját, amikor saját Internet felhasználási tervét készíti. (Megjegyzés: Ha számára ismeretlenek a biztonsággal és az Internettel kapcsolatos kifejezések, nézze át az IBM Systems Szoftver információs központ *biztonsági szakkifejezések* című részét, amikor ezt a könyvet használja.)

Amint rájön, hogyan akarja használni az Internetet elektromos kereskedelem céljára, vele együtt a biztonsági kérdésekre is, és a biztonsági eszközök, funkciók és ajánlatok rendelkezésre állnak, kidolgozhatja a biztonsági irányelveket és célokat. Számos tényező fogja befolyásolni a választását, amit a biztonsági irányelvek kidolgozásakor tesz meg. Amikor szervezete az Internet irányába terjeszkedik, biztonsági irányelvei fontos sarokkövek annak garantálásában, hogy a rendszerek és az erőforrások biztonságosak legyenek.

Az iSeries szerver biztonsági jellemzői

A számos egyedi biztonsági ajánlaton (amelyek az Internethez csatlakozó rendszer védelmére hivatottak) túlmenően az iSeries szerver nagyon erős rendszer biztonsági jellemzőkkel rendelkezik, mint például:

- Beépített biztonság, amelyet különösen nehéz kijátszani, összehasonlítva a más rendszereken ajánlott, beépülő biztonsági szoftver csomagokkal.
- Objektum alapú architektúra, amely technikailag nehézzé teszi vírus létrehozását és elterjesztését. Az iSeries szerveren egy fájl nem keltheti azt a látszatot, mintha program lenne, és egy adott program sem tud megváltoztatni egy másik programot. Az iSeries sértetlenségi funkciók megkövetelik, hogy a rendszer által biztosított kezelőfelületeken keresztül érje el az objektumokat. Nem tudja közvetlenül elérni az objektumot címe alapján a rendszerben. Nem tud eltolással sem próbálkozni, de mutató ″gyártásával″ sem. A mutató manipuláció a hackerek népszerű eljárása az egyéb felépítésű rendszereken.
- Rugalmasság, amely lehetővé teszi, hogy a rendszer biztonságot saját szükségleteihez igazodva állítsa be. Használhatja az @server Biztonsági tervezőt, amelynek segítségével meghatározhatja, hogy mely biztonsági javaslatok illeszkednek biztonsági igényeihez.

Az iSeries további biztonsági ajánlatai

Az iSeries szervernek van néhány különleges biztonsági ajánlata, amelyeket felhasználva fokozhatja rendszerének biztonságát, amikor az Internethez csatlakozik. Az Internet használat módjától függően, szándékában állhat az alábbi ajánlatokból egy vagy több ajánlat előnyét kihasználni:

- Virtuális saját hálózatok (VPN), amelyek a vállalati magán intranet hálózat kiterjesztései olyan nyilvános hálózatokon keresztül, mint például az Internet. A VPN használata révén létrehozhat biztonságos magán összeköttetéseket, lényegében úgy, hogy magán ″alagutat″ hoz létre a nyilvános hálózaton. A VPN az i5/OS beépített funkciója, amelyet az iSeries navigátorból érhet el. A VPN funkcióról további tájékoztatást talál az IBM Systems Szoftver információs központ ″Virtuális saját hálózat (VPN)″ című témakörében.
- A Csomag szabály az i5/OS beépített funkciója, amelyet az iSeries navigátorból érhet el. Ez a kiegészítő lehetővé teszi az IP csomagszűrő és a hálózati címfordítás (NAT) szabályainak konfigurálását, amely révén vezérelni tudja az iSeries szerverre bemenő és a szerverről kimenő TCP/IP forgalmat. A csomag szabályokról további tájékoztatást talál az IBM Systems Szoftver információs központ ″Csomag szabályok″ című részében.
- Védett socket réteg (SSL) alkalmazás kommunikációs biztonság lehetővé teszi az alkalmazások konfigurálását SSL használatára, aminek hatására védett kapcsolat jön létre a szerver alkalmazások és azok kliensei között. Az SSL-t eredetileg a web böngészők és a szerver alkalmazások védelmére fejlesztették ki, de más alkalmazásoknál is engedélyezhető a használata. Számos iSeries szerver alkalmazás képes az SSL használatára, beleértve az IBM HTTP Server for iSeries, az iSeries Access Express, a File Transfer Protocol (FTP), a Telnet és egyéb termékeket is. Az SSL biztonságról az IBM Systems Szoftver információs központ ″Alkalmazások biztonságossá tétele SSL segítségével″ című témakörében olvashat.

Amint rájön, hogyan akarja használni az Internetet, vele együtt a biztonsági kérdésekre is, és a biztonsági eszközök, funkciók és ajánlatok rendelkezésre állnak, kidolgozhatja a biztonsági irányelveket és célokat. Számos tényező fogja befolyásolni a választását, amit a biztonsági irányelvek kidolgozásakor tesz meg. Amikor szervezete az Internet irányába terjeszkedik, a biztonsági irányelvek fontos sarokkövek annak garantálásában, hogy rendszere biztonságos legyen.

Megjegyzés: Nézze át az alábbiakat, ha részletesebb tájékoztatást keres arról, hogyan kell elkezdeni az Internetet üzleti célra használni:

- IBM Systems Szoftver információs központ *Csatlakozás az Internethez* című témaköre.
- *AS/400 Internet Security: Protecting Your AS/400 from HARM on the Internet* (SG24-4929) című Redbook kiadvány.

Kapcsolódó fogalmak

“Biztonsági irányelvek és célok” oldalszám: 6
A leírtak segítségével meghatározhatja, hogy mit védjen, és mit várjon el a felhasználóktól.

Az Internet biztonság tervezése

Tájékoztatást nyújt olyan biztonsági szabályzat létrehozásáról, amely magában foglalja az Internet biztonsággal kapcsolatos szükségleteket.

Amikor Internet használati tervét készíti, gondosan fogalmazza meg Internet biztonsági igényeit. Részletesen tájékozódni kell az Internet használati tervekről, és dokumentálni kell a belső hálózat konfigurációját. Az összes begyűjtött információ eredményeképpen pontosan kiértékelheti biztonsági igényeit.

Például, a következő dolgokat kell dokumentálni és ismertetni:

- A hálózat aktuális konfigurációját.
- A DNS és az e-mail szerver konfigurációját.
- Az Internet szolgáltatóval (ISP) való kapcsolatot.
- Az Internetről igénybe venni kívánt szolgáltatásokat.
- Az Internet felhasználóknak nyújtani kívánt szolgáltatásokat.

Az ilyen jellegű információk dokumentálása segít annak eldöntésében, hol vannak biztonsági kockázatok, és milyen biztonsági intézkedéseket kell bevezetni az ilyen kockázatok minimalizálása érdekében.

Például, úgy dönt, lehetővé teszi a belső felhasználóknak, hogy Telnet kapcsolaton keresztül elérjék egy speciális kutatóhely gazdagépeit. A belső felhasználóknak szükségük van erre, hogy segítse őket a cég új termékeinek fejlesztésében. Azonban van néhány szempontja a bizalmas adatokra vonatkozóan, amelyek védtelenül haladnak át az Interneten. Ha a versenytársak befogják és feltárják ezeket az adatokat, a cég pénzügyi kockázatokkal találná szembe magát. Ha azonosítja az igényeket (Telnet), és az ahhoz társuló kockázatokat (a bizalmas információk nyilvánosságra kerülése), meghatározhatja azokat a járulékos biztonsági intézkedéseket, amelyeket be kell vezetni ahhoz, hogy az adatok bizalmas jellege megmaradjon a használat során (Védett socket réteg (SSL) alkalmazhatóság).

Az alábbi témakörök áttekintése hasznos lehet az Internet használat és a biztonsági terv kidolgozásakor:

- *A réteges védelem elve a biztonságért* című rész ismerteti az átfogó biztonsági terv elkészítésével kapcsolatos kérdéseket.
- A *Biztonsági irányelvek és célok* című rész segít annak meghatározásában, hogy a biztonsági irányelvek részeként mit kell dokumentálni.
- A *Forgatókönyv: JKL Toy Company e-business tervek* című rész egy cég jellemző Internet felhasználásának és biztonsági tervének gyakorlati modelljét mutatja be.

A réteges védelem elve a biztonságért

A **biztonsági irányelve** meghatározza, hogy mit akar védeni, és mit vár el a rendszer felhasználóitól.

Alapot szolgáltat a biztonság tervezéséhez, amikor új alkalmazásokat tervez, vagy amikor bővíti meglévő hálózatát. Leírja a felhasználó felelősségi körébe tartozó dolgokat, mint például a bizalmas információk védelmét és a megfelelő (nem triviális) jelszók alkalmazását.

Megjegyzés: A biztonsági irányelveket meg kell alkotni és el kell rendelni a szervezete számára, hogy minimálisra csökkentse a belső hálózat kockázati tényezőit. Az iSeries rendszerrel velejáró biztonsági funkciók számos kockázati tényező minimalizálását biztosítják, ha megfelelően konfigurálják őket. Azonban, amikor az iSeries rendszert az Internetre kapcsolja, további biztonsági intézkedésekre van szükség ahhoz, hogy a belső hálózat biztonsága megmaradjon.

Számos kockázat társul az Internet hozzáféréssel, amely irányítja az üzleti tevékenységet. Valahányszor megalkotja a biztonsági irányelveket, egyensúlyoznia kell a szolgáltatások nyújtása, valamint a funkciókhoz és az adatokhoz való hozzáférés vezérlése között. Hálózatba kötött számítógépek esetén a biztonság fenntartása még nehezebb, mivel maga a kommunikációs csatorna van kiszolgáltatva a támadásoknak.

Egyes Internet szolgáltatások még sebezhetőbbek bizonyos típusú támadásokkal szemben, mint mások. Ennek következtében, nagyon fontos, hogy tisztán lássa a kockázatokat, amelyek rárakódnak az egyes szolgáltatásokra, amelyeket nyújtani vagy használni akar. Továbbá, a lehetséges biztonsági kockázatok megértése hozzásegíti ahhoz, hogy tisztán meghatározza a biztonsági célokat.

Az Internet otthont ad olyan egyéneknek is, akik magatartásukkal fenyegetést jelentenek az Internet kommunikáció biztonságára. A következő felsorolás leír néhány jellemző biztonsági kockázatot, amelyekkel számolnia kell:

- **Passzív támadás**: Passzív támadás esetén a perpetrator megfigyeli a hálózati forgalmat, s így próbálja megfejteni a titkot. Az ilyen jellegű támadás lehet hálózati alapú (a kommunikációs csatolások követése), vagy rendszer alapú (a rendszer összetevőjének cseréje egy ″trójai faló″ programra, amely ravaszul elfogja az adatokat. A passzív támadást a legnehezebb észrevenni. Ennek következtében azt kell feltételezni, hogy minden Interneten bonyolódó kommunikációt valaki megfigyel.
- **Aktív támadás:** Aktív támadás esetén a perpetrator megpróbálja feltörni a védelmet, és bejutni a hálózati rendszerekre. Az aktív támadásnak több típusa lehet:
  - A **rendszer hozzáférési kísérletekben**, a támadó megkísérli feltárni a biztonsági lyukakat, hogy hozzáféréshez és vezérléshez jusson a kliens vagy a szerver rendszeren keresztül.

– A **hamisítás** során a támadó megkísérli úgy áttörni a védelmet, hogy megbízható rendszernek álcázza magát, illetve egy felhasználó arra ösztökéli, hogy küldjön neki titkos információkat.
– A **szolgáltatás leállítása jellegű támadásokban**, a támadó megpróbálja megzavarni vagy lezárni a műveleteket azáltal, hogy átirányítja a forgalmat vagy limlommal bombázza a rendszert.
– A **titkosítási támadásokban** a támadó megpróbálja kitalálni vagy ellopni a jelszavakat, vagy speciális eszköz segítségével igyekszik megfejteni a titkosított adatokat.

Többszintű védelem

Mivel a potenciális Internet biztonsági kockázatok különféle szinteken fordulnak elő, olyan biztonsági intézkedéseket kell hozni, amelyek a védelem területén is különféle szinteken jelentkeznek a kockázatokkal szemben. Általánosságban azt lehet mondani, amikor az Internetre kapcsolódik, nem kell meglepődni, **ha** behatolási kísérleteket vagy szolgáltatás visszautasítást tapasztal. Helyette rögtön tételezze fel, hogy biztonsági problémákat **fog** tapasztalni. Következésképpen a legjobb védekezés a gondos, előrelátó támadás. A többszintű védekezési szemlélet alkalmazása az Internet biztonsági stratégia tervezésében biztosítja azt, hogy a támadó, aki áthatol az egyik védelmi szinten, az ezt követő szinten fennakad.

A biztonsági stratégiájának tartalmaznia kell azokat az intézkedéseket, amelyek védelmet nyújtanak a hagyományos hálózati számítástechnikai modell következő szintjein. Általában, a biztonságot a legalapvetőbb szinttől (rendszer szintű biztonság) kezdve egészen a legbonyolultabb szintig (tranzakciós szintű biztonság) kell megtervezni.

Rendszer szintű biztonság

A rendszer biztonsági intézkedések az Internet alapú biztonsági problémákkal szembeni védekezés legalsó szintjét képviselik. Következésképpen, a teljeskörű Internet biztonsági stratégia első lépéseként meg kell arról győződnie, hogy erős alapszintű biztonságot állított be a rendszeren. A témakör ismerteti, milyen beállításokat kell használni, amikor az Internethez kapcsolódik.

Hálózati szintű biztonság

A Hálózati biztonságra vonatkozó intézkedései irányítják az iSeries és az egyéb hálózati rendszerek elérhetőségét. Amikor a hálózatot az Internethez csatlakoztatja, mindenképpen ellenőrizze, hogy kellő hálózati szintű biztonsági intézkedéseket vezetett be, amelyek megvédik a belső hálózati erőforrásokat a jogosulatlan eléréstől és betolakodástól. A tűzfal a hálózati biztonság biztosításának legáltalánosabb eleme. Az Internet szolgáltató (ISP) fontos eleme kell, hogy legyen a hálózati biztonságról szóló tervének. A hálózati biztonság sémája körvonalazza, milyen biztonsági intézkedéseket fog nyújtani az ISP, mint például szűrési szabályokat az ISP útválasztó összeköttetéshez, vagy elővigyázatossági lépéseket a nyilvános Tartománynév szolgáltatáshoz (DNS). A Hálózati biztonság ismerteti azokat a biztonsági intézkedéseket, amelyeket alkalmazni kell a hálózat szintjén a belső erőforrások védelme érdekében.

Alkalmazás szintű biztonság

Az Alkalmazás szintű biztonsági intézkedések meghatározzák, hogy mennyi felhasználó működhet együtt egy adott alkalmazással. Általában konfigurálni kell a biztonság beállításokat minden egyes alkalmazás esetében, amelyet használ. Azonban különleges figyelmet kell fordítani a biztonság beállítására azoknál az alkalmazásoknál, amelyeket az Internetről használ, illetve az Internet számára nyújt. Az ilyen alkalmazások és szolgáltatások sebezhetőek, a jogosulatlan felhasználók visszaélve ezzel módot találhatnak arra, hogy hozzáférjenek a hálózat rendszereihez. Az elhatározott biztonsági intézkedéseknek tartalmazni kell a szerver- és a kliens oldali biztonsági kockázatokat is. Az Alkalmazás szintű biztonsági beállítások című rész ismerteti a biztonsági kockázatokat és az ilyen kockázatok kezeléséhez rendelkezésre álló opciókat számos népszerű Internetes alkalmazás és szolgáltatás esetében.

Átvitel szintű biztonság

Az Átvitel szintű biztonsági intézkedések védik az adatkommunikációt a hálózaton belül és a hálózatok között. Amikor az Internethez hasonló nem megbízható hálózattal kommunikál, nem tudja irányítani a forgalom folyását a forrás- és a célhely között. A hálózat által szállított forgalom és adatok több különféle szerveren haladnak át, amelyeket nem tud irányítani. Mindaddig, amíg nem állítja be a biztonsági intézkedések szerinti védelmet, mint például az alkalmazások konfigurálása Védett socket réteg (SSL) használatára, a továbbított adatokat bárki láthatja és használhatja. Az átvitel szintű biztonsági intézkedések védik adatait,

amíg azok a biztonsági szintek határai között mozognak. Az Átvitel szintű biztonság ismerteti azokat a biztonsági intézkedéseket, amelyeket bevezethet az adatok védelmében, amíg azok az Internethez hasonló nem megbízható hálózatokban haladnak.

Amikor az átfogó biztonsági irányelveket alakítja ki, minden szintre egyedileg ki kell dolgozni biztonsági stratégiáját. Ezen túlmenően le kell írni, hogyan fognak együttműködni az egyes stratégiai csoportok egymással, hogy széleskörű biztonsági védelemmel ellátott hálózatot adjanak üzletmenetéhez.

Kapcsolódó fogalmak

“Biztonsági szintek az alapszintű Internet eléréshez” oldalszám: 10
Ismerteti, hogy milyen rendszer biztonságot kell kialakítani, mielőtt az Internethez csatlakozna.

“Hálózatbiztonsági beállítások” oldalszám: 11
Az itt leírtak segítségével tanulmányozhatja a hálózatszintű biztonsági intézkedéseket, amelyek használatát meg kell fontolni a belső erőforrások védelme érdekében.

“Alkalmazásbiztonsági beállítások” oldalszám: 16
Ismerteti a biztonsági kockázatokat és az ilyen kockázatok kezelésére szolgáló opciókat számos népszerű Internetes alkalmazás és szolgáltatás esetében.

“Átvitelbiztonsági beállítások” oldalszám: 23
A leírtak segítségével tanulmányozhatja azokat a biztonsági intézkedéseket, amelyek alkalmazásával megvédheti az adatokat, amikor azok nem megbízható hálózaton (mint például Internet) haladnak át. Ide tartozik a Védett socket réteg (SSL) protokoll, az iSeries Access Express program és a Virtuális magánhálózat (VPN) kapcsolat is.

“Biztonsági irányelvek és célok”
A leírtak segítségével meghatározhatja, hogy mit védjen, és mit várjon el a felhasználóktól.

“E-mail biztonság” oldalszám: 20
Az Interneten vagy más nem megbízható hálózaton keresztül küldött e-mail biztonsági kockázatot jelent, amellyel szemben nem feltétlenül nyújt védelmet a tűzfal használata.

Virtuális magánhálózat (VPN)

“FTP biztonság” oldalszám: 22
Az FTP (fájlátviteli protokoll) fájlátviteli képességet biztosít egy kliens (egy felhasználó egy másik rendszeren) és a szerver között.

Kapcsolódó hivatkozás

Biztonsági szakkifejezések

Biztonsági irányelvek és célok

A leírtak segítségével meghatározhatja, hogy mit védjen, és mit várjon el a felhasználóktól.

Biztonsági irányelvek

Minden Internet szolgáltatás, amelyet használ vagy nyújt, kockázatot jelent az iSeries rendszer számára, és annak a hálózatnak is, amelyikhez csatlakozik. A biztonsági irányelv valójában egy olyan szabálykészletet jelent, amely a szervezethez tartozó számítógépek és kommunikációs erőforrások tevékenységére vonatkozik. Ezek a szabályok felölelik a fizikai, a személyi, az adminisztrációs és a hálózati biztonság területét.

A **biztonsági irányelve** meghatározza, hogy mit akar védeni, és mit vár el a rendszer felhasználóitól. Alapot szolgáltat a biztonság tervezéséhez, amikor új alkalmazásokat tervez, vagy amikor bővíti meglévő hálózatát. Leírja a felhasználó felelősségi körébe tartozó dolgokat, mint például a bizalmas információk védelmét és a megfelelő (nem triviális) jelszók alkalmazását. A biztonsági irányelvekben ki kell térni arra is, hogyan fogja felügyelni a biztonsági intézkedések hatékonyságát. Az ilyen jellegű felügyelet segítségével meghatározhatja, hogy megkísérelte-e valaki kijátszani a védelmet.

A biztonsági irányelvek kialakításához világosan meg kell fogalmazni biztonsági céljait. A biztonsági stratégia létrehozása után lépéseket kell tenni a bennefoglalt szabályok életbeléptetésére. A lépések körébe tartozik az alkalmazottak kiképzése, valamint a szabályok betartásához szükséges szoftver és hardver bővítések elvégzése. Amikor a számítástechnikai környezetében végez változtatásokat, azzal összhangban a biztonsági irányelveket is frissíteni kell.

Így biztosíthatja azt, hogy felkészüljön minden új kockázatra, amelyet a változtatások hoznak magukkal. Az IBM Systems Szoftver információs központ ″Alapvető rendszerbiztonság és tervezése″ című témakörében lévő példa a JKL Toy Company biztonsági irányelveit mutatja be.

Biztonsági célok

Amikor létrehozza és végrehajtja a biztonsági irányelveket, világos célokkal kell rendelkezni. A biztonsági célok az alábbi, egy vagy több kategóriába esnek:

erőforrás védelem
Az erőforrás védelem sémája garantálja, hogy csak jogosult felhasználók férhetnek hozzá a rendszeren lévő objektumokhoz. Nagy erősség, hogy a rendszer erőforrások minden típusa védhető az iSeries rendszeren. Gondosan határozza meg a felhasználók különböző kategóriáit, akik elérhetik a rendszert. A biztonsági irányelvek készítésének részeként azt is meg kell határozni, milyen hozzáférési jogosultságokat akar adni a felhasználók ezen csoportjainak.

hitelesítés
Biztosítja vagy ellenőrzi, hogy a szekció másik oldalán levő erőforrás (emberi vagy gépi) valóban az, amit magáról állít. Az egyértelmű hitelesítés megvédi a rendszert a megszemélyesítés biztonsági kockázatával szemben, amikor is a küldő vagy a fogadó hamis azonosságot használ a rendszer eléréséhez. Hagyományosan, a rendszerek jelszavakat és felhasználói neveket használnak a hitelesítéshez, azonban a digitális igazolások biztonságosabb hitelesítési módszert eredményeznek, miközben más biztonsági előnyöket is ajánlanak. Amikor a rendszere nyilvános hálózathoz - például Internethez - kapcsolódik, a felhasználói hitelesítés új dimenziókat hoz magával. Fontos különbség az Internet és a saját intranetje között az, hogy az intraneten megbízhat a bejelentkező felhasználó azonosságában. Éppen ezért érdemes komolyan megfontolni jobb hitelesítési módszerek használatát, mint amit a hagyományos felhasználónév és jelszó alapú bejelentkezési eljárás nyújt. A hitelesített felhasználók különböző típusú engedélyekkel rendelkezhetnek a jogosultsági szintjüknek megfelelően.

jogosultság
Biztosíték arra, hogy a szekció másik végén lévő személynek vagy számítógépnek van engedélye a kérés végrehajtásához. A jogosultság annak meghatározási folyamata, hogy ki vagy mi érheti el a rendszer erőforrásait, és ki vagy mi hajthat végre bizonyos tevékenységeket a rendszeren. Általában, a jogosultság a hitelesítés szövegkörnyezetében fordul elő.

sértetlenség
Biztosíték arra, hogy a megérkező információ ugyanaz, mint az elküldött. A sértetlenség ismerete megköveteli az adat- és rendszer sértetlenség alapelveinek megértését.

- **Adat sértetlenség**: Az adatok védve vannak a jogosulatlan változtatásoktól és hamisításoktól. Az adat sértetlenség véd a kezelés biztonsági kockázataival szemben, amelyben valaki elfogja és megváltoztatja az információt, amihez egyébként nincs jogosultsága. A hálózaton belül tárolt adatok védelmén túlmenően, további biztonsági elemekre lehet szükség az adat sértetlenség biztosításához, amikor adatok lépnek be a rendszerére nem megbízható forrásból. Amikor a rendszerre belépő adatok nyilvános hálózatból jönnek, szüksége lehet biztonsági módszerekre úgy, hogy megtehesse a következőket:
  - Védje adatait a “szimatolástól” és az értelmezéstől, általában titkosítás útján.
  - Győződjön meg arról, hogy az átvitel során nincs módosulás (adat sértetlenség).
  - Ellenőrizze, hogy az átvitel megtörtént-e (letagadhatatlanság). A jövőben szüksége lehet az ajánlott vagy regisztrált posta elektronikus megfelelőjére.
- **Rendszer sértetlenség**: A rendszer konzisztens abban, hogy az elvárt eredményt hozza az elvárt teljesítmény mellett. Az iSeries rendszer sértetlenség a biztonság leggyakrabban áttekintett összetevője, mivel ez az iSeries architektúra alapvető része. Például, az iSeries architektúra különösen nehézzé teszi egy ″bajkeverő″ számára, hogy változtatásokat kezdeményezzen az operációs rendszer programjában, amikor a biztonsági szintje 40 vagy 50.

letagadhatatlanság
A ″letagadhatatlanság″ tulajdonképpen egy ellenőrzés arról, hogy a tranzakció megtörtént-e, illetve, hogy elküldött-e vagy megkapott-e egy üzenetet. A digitális igazolások és a nyilvános kulcsok titkosításának

igénybe vétele a tranzakciók, az üzenetek és a dokumentumok jelzésére támogatja ezt a funkciót. A küldő és a fogadó is egyetért abban, hogy a csere megtörtént. Az adatok digitális aláírása biztosítja a szükséges ellenőrzést.

megbízhatóság
Biztosíték arra, hogy az érzékeny információk megmaradnak magán jellegűnek, és nem láthatók a vonalcsapolók számára. A megbízhatóság nagyon fontos a teljeskörű adatbiztonsághoz. Az adatok titkosítása digitális igazolások és Védett socket réteg (SSL) segítségével garantálja a titkosságot, amikor adatokat visz át nem megbízható hálózatokon keresztül. A biztonsági irányelveknek arra is választ kell adniuk, hogyan biztosítja az információk megbízhatóságát a hálózaton belül, illetve akkor, amikor az információ elhagyja a hálózatát.

Biztonsági tevékenységek ellenőrzése
A biztonságot illető események figyelése naplót szolgáltat a sikeres és a sikertelen (visszautasított) hozzáférésekről egyaránt. A sikeres hozzáférést jelölő rekordok megmondják, ki és mit csinál a rendszereken. A sikertelen (visszautasított) hozzáférésről szóló rekordok megmondják, hogy valaki megkísérelte feltörni a biztonsági védelmet, vagy azt, hogy valakinek nehézségei támadtak a rendszer elérésében.

A biztonsági célok megértése segít olyan biztonsági irányelvek kidolgozásában, amelyek kitérnek a hálózat és az Internet összes biztonsági szükségletére. Hasznos lehet áttekinteni a JKL Toy Company e-business forgatókönyvét, amikor meghatározza céljait és létrehozza biztonsági irányelveit. A vállalat Internet felhasználási forgatókönyve és a biztonsági terv számos valós megvalósítást képvisel.

Kapcsolódó fogalmak

“iSeries és Internet biztonsági megfontolások” oldalszám: 2
Áttekintést nyújt az iSeries biztonsági erősségeiről és lehetőségeiről.

“A réteges védelem elve a biztonságért” oldalszám: 4
A **biztonsági irányelve** meghatározza, hogy mit akar védeni, és mit vár el a rendszer felhasználóitól.

Digitális igazolások

Védett socket réteg (SSL)

“Forgatókönyv: JKL Toy Company e-business tervek”
A forgatókönyv egy tipikus vállalkozást, a JKL Toy Company nevű céget írja le, amely elhatározta, hogy üzleti célkitűzéseit kibővíti az Internet használattal. Annak ellenére, hogy a cég kitaláció csupán, terveik - nevezetesen az Internet használata elektronikus kereskedelem céljára - és az ennek eredményeképpen felmerülő biztonsági igények, számos valós nemzetközi vállalat helyzetét képviselik.

Forgatókönyv: JKL Toy Company e-business tervek

A forgatókönyv egy tipikus vállalkozást, a JKL Toy Company nevű céget írja le, amely elhatározta, hogy üzleti célkitűzéseit kibővíti az Internet használattal. Annak ellenére, hogy a cég kitaláció csupán, terveik - nevezetesen az Internet használata elektronikus kereskedelem céljára - és az ennek eredményeképpen felmerülő biztonsági igények, számos valós nemzetközi vállalat helyzetét képviselik.

A JKL Toy Company kicsi, de gyorsan növekvő, játékgyártó cég, termékskálájuk az ugrókötéltől kezdve a sárkányokon át egészen az ölelni való, kitömött leopárdokig tart. A cég elnöke elkötelezett híve a vállalkozás gyarapodásának, és azt is látja, hogy az új iSeries rendszer könnyedén elbírja a növekedés terheit. Sharon Jones főkönyvelő felelős az iSeries rendszer adminisztrációjáért és biztonságáért.

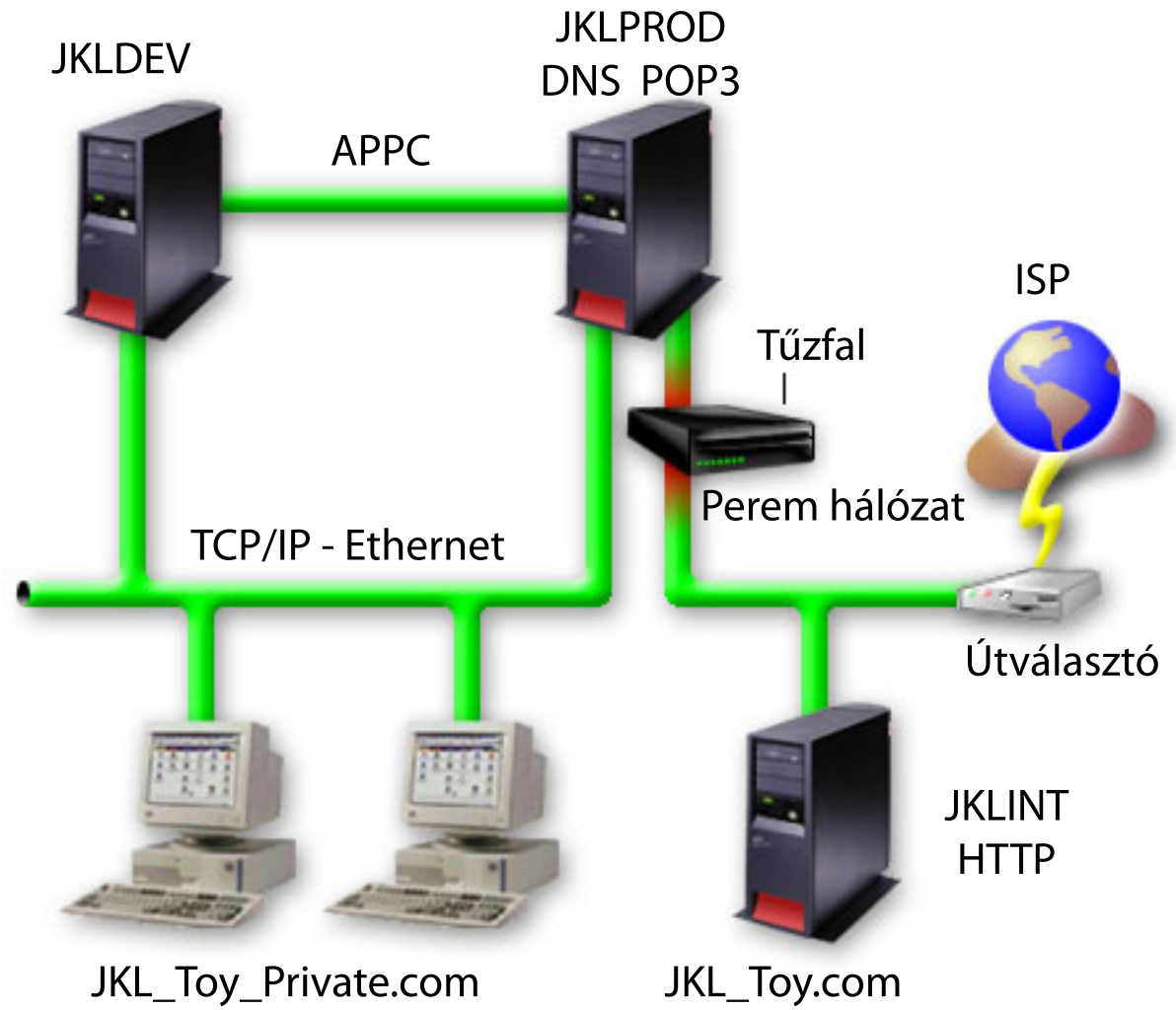
A JKL Toy Company évek óta sikeresen használja a belső alkalmazásokra vonatkozó biztonsági irányelveit. A cég most tervezi egy intranet létrehozását a belső információk hatékonyabb megosztása érdekében. A cég egyúttal az Internet használatát is tervbe vette további üzleti céljai alapján. A célok között szerepel a vállalati marketing Internetes jelenlétének létrehozása, beleértve egy online katalógust is. Szándékukban áll az Interneten érzékeny információkat is küldeni távoli kirendeltségeikről a vállalat központi telephelyére. Ezenkívül, a cég meg kívánja engedni a tervező laboratórium alkalmazottainak, hogy Internet hozzáférésük legyen kutatási és fejlesztési célokból. Végül, a cég meg akarja engedni vásárlóinak, hogy azok felhasználhassák saját webhelyeiket közvetlen, online vásárlásra. Sharon elkészítette jelentését az ilyen tevékenységekre jellemző, potenciális biztonsági kockázatokról, valamint azokról a

biztonsági rendszabályokról, amelyeket a cégnek alkalmazni kell az ilyen kockázatok minimalizálása érdekében. Sharon lesz a felelős a cég biztonsági irányelveinek frissítéséért, valamint a vállalat által elhatározott biztonsági intézkedések gyakorlati megvalósításáért.

A megnövekedett Internetes jelenlét céljai a következők:

- Átfogó marketing kampány részeként az általános vállalati megjelenés és jelenlét bevezetése.
- Online termékkatalógus biztosítása a vásárlóknak és az értékesítési személyzetnek.
- Ügyfélszolgálat javítása.
- E-mail és világháló hozzáférés az alkalmazottaknak.

Miután meggyőződtek arról, hogy az iSeries szerverek igen erős alapszintű rendszer biztonsággal rendelkeznek, a JKL Toy company elhatározta egy tűzfal termék megvásárlását és bevezetését, hogy hálózatszintű védelmük legyen. A tűzfal megvédi a belső hálózatot számtalan potenciális, Internet jellegű kockázattól. Az alábbi ábra illusztrálja a cég Internet/hálózat konfigurációját.



Ahogy az ábrán is látható, a JKL Toy Company két elsődleges iSeries szerverrel rendelkezik. Az egyik rendszert használják fejlesztésre (JKLDEV), míg a másikat termelési (JKLPROD) alkalmazásokra. Mindkét rendszer életbevágó adatokat és alkalmazásokat kezel. Következésképpen, nem lenne kényelmes az Internet alkalmazásokat ezeken a rendszereken futtatni. Helyette, egy új iSeries szerver (JKLINT) beállítását választották az ilyen alkalmazások futtatásához.

A vállalat a hálózat peremén helyezte el az új rendszert, tűzfalat használ az új gép és a cég fő belső hálózata között, hogy jobban el tudja különíteni a saját hálózatot az Internettől. Ez az elkülönítés csökkenti az Internetes kockázatokat, amelyek sebezhetnék a belső rendszereket. A cég a hálózati biztonság kezelésének bonyolultságát is csökkenti azzal, hogy az új iSeries szervert kizárólag Internet szervernek jelöli ki.

A vállalat semmilyen fontos alkalmazást sem futtat pillanatnyilag az új iSeries szerveren. Az elektronikus kereskedelemre vonatkozó tervüknek ebben a fázisában az új rendszer csak az állandó nyilvános webhelyet szolgáltatja. A cég azonban biztonsági intézkedéseket kíván bevezetni, hogy védje a rendszert és a nyilvános webhelyet a szolgáltatás megszakításának és a lehetséges támadások megakadályozása érdekében. Következésképpen, a vállalat csomagszűrő- és hálózati címfordítási (NAT) szabályokkal fogja védeni a rendszert, valamint hatékony alapszintű biztonsági intézkedésekkel.

Ahogy a vállalat újabb nyilvános alkalmazásokat fejleszt (mint például e-kereskedelem webhely vagy extranet hozzáférés), további biztonsági intézkedéseket vezet be.

Kapcsolódó fogalmak

“Biztonsági irányelvek és célok” oldalszám: 6
A leírtak segítségével meghatározhatja, hogy mit védjen, és mit várjon el a felhasználóktól.

“Hálózatbiztonsági beállítások” oldalszám: 11
Az itt leírtak segítségével tanulmányozhatja a hálózatszintű biztonsági intézkedéseket, amelyek használatát meg kell fontolni a belső erőforrások védelme érdekében.

“Átvitelbiztonsági beállítások” oldalszám: 23
A leírtak segítségével tanulmányozhatja azokat a biztonsági intézkedéseket, amelyek alkalmazásával megvédheti az adatokat, amikor azok nem megbízható hálózaton (mint például Internet) haladnak át. Ide tartozik a Védett socket réteg (SSL) protokoll, az iSeries Access Express program és a Virtuális magánhálózat (VPN) kapcsolat is.

Biztonsági szintek az alapszintű Internet eléréshez

Ismerteti, hogy milyen rendszer biztonságot kell kialakítani, mielőtt az Internethez csatlakozna.

A rendszer biztonsági intézkedések az Internet alapú biztonsági problémákkal szembeni védekezés legalsó szintjét képviselik. Következésképpen, a teljeskörű Internet biztonsági stratégia első lépéseként megfelelően be kell állítani az i5/OS alapszintű biztonsági elemeit. Ahhoz, hogy a rendszer biztonság eleget tegyen a minimális követelményeknek, tegye a következőt:

- Állítsa be a biztonsági szintet (QSECURITY rendszerváltozó) 50-es értékre. Az 50-es biztonsági szint a sérthetetlenség legmagasabb fokát biztosítja, ami erőteljesen ajánlott a rendszer védelméhez olyan magas kockázati tényezőjű környezetben, mint az Internet. Az iSeries egyes biztonsági szintjeiről részletesebb tájékoztatást itt talál: Rendszerbiztonság tervezése és beállítása.

  Megjegyzés: Ha pillanatnyilag az 50-esnél alacsonyabb biztonsági szinten dolgozik, szükségessé válhat a működési eljárások vagy az alkalmazások frissítése. Olvassa el az iSeries biztonsági leírást a magasabb biztonsági szintre történő váltás előtt.

- A biztonsággal kapcsolatos rendszerváltozókat legalább korlátozó állapotba állítsa az ajánlott értékekhez képest. Az ajánlott biztonsági értékek beállításához használja az iSeries navigátor Biztonsági varázslóját.
- Győződjön meg róla, hogy egyetlen felhasználói profil (beleértve az IBM által szállított felhasználói profilokat is) sem az alapértelmezett jelszavakkal rendelkezik. Az Analyze Default Passwords (ANZDFTPWD) parancs segítségével ellenőrizheti, hogy rendelkezik-e alapértelmezett jelszavakkal.
- A fontos rendszer erőforrásokat védje objektum jogosultsággal. A rendszeren a korlátozó megközelítést alkalmazza. Ez azt jelenti, hogy alapértelmezés szerint mindenkit (PUBLIC *EXCLUDE) jogosultságra korlátoz az olyan rendszer erőforrások tekintetében, mint a könyvtárak vagy katalógusok. Csupán néhány felhasználónak enged hozzáférést ezekhez a korlátozott erőforrásokhoz. Internetes környezetben nem elegendő a menükön keresztüli hozzáférés korlátozása.
- Be **kell** állítani objektum jogosultságot a rendszeren. .

A minimális rendszer biztonsági követelmények konfigurálásában segít a @server **Biztonsági tervező** (elérhető az IBM Systems Szoftver információs központ honlapján) vagy a **Biztonsági varázsló** (elérhető az iSeries navigátorból). A Biztonsági tervező biztonsági ajánlásokat szolgáltat, miután válaszol egy sor feltett kérdésre. Azután felhasználhatja ezeket az ajánlásokat a szükséges rendszer biztonsági elemek beállításához. A Biztonsági varázsló ugyancsak biztonsági ajánlásokat tesz, miután válaszol egy sor feltett kérdésre. A Security Advisor funkcióval szemben, itt varázslóval rendelkezik, amely felhasználhatja az ajánlásokat a rendszer biztonsági elemeinek beállításához.

Az iSeries rendszerben rejlő biztonsági funkciók számos kockázatot tudnak minimalizálni, ha megfelelően konfigurálja és kezeli őket. Azonban, amikor az iSeries szervert Internethez csatlakoztatja, további biztonsági intézkedéseket kell foganatosítani a belső hálózat biztonsága érdekében. Ha meggyőződött arról, hogy az iSeries jó általános rendszer biztonsággal rendelkezik, készen áll arra, hogy az Internet használat céljából készült átfogó biztonsági terv részeként járulékos biztonsági intézkedéseket hajtson végre.

Kapcsolódó fogalmak

“A réteges védelem elve a biztonságért” oldalszám: 4
A **biztonsági irányelve** meghatározza, hogy mit akar védeni, és mit vár el a rendszer felhasználóitól.

Kapcsolódó tájékoztatás

iSeries Biztonsági szakkönyv

Hálózatbiztonsági beállítások

Az itt leírtak segítségével tanulmányozhatja a hálózatszintű biztonsági intézkedéseket, amelyek használatát meg kell fontolni a belső erőforrások védelme érdekében.

Amikor egy nem megbízható hálózathoz kapcsolódik, a biztonsági irányelveknek tartalmaznia kell egy átfogó biztonsági sémát, beleértve azokat a biztonsági intézkedéseket, amelyeket a hálózat szintjén meg akar valósítani. A tűzfal telepítése az egyik legjobb eszköze a hálózati biztonság átfogó készletének felvonultatásához.

Az Internet szolgáltató (ISP) fontos eleme kell, hogy legyen a hálózati biztonságról szóló tervének. A hálózati biztonság sémája körvonalazza, milyen biztonsági intézkedéseket fog nyújtani az Internet szolgáltató (ISP), mint például szűrési szabályokat az ISP útválasztó összeköttetéshez, vagy elővigyázatossági lépéseket a nyilvános Tartománynév szolgáltatáshoz (DNS).

Annak ellenére, hogy a tűzfal bizonyosan a védekezés egyik legfontosabb pontját képviseli a teljeskörű biztonsági tervben, nem szabad, hogy a védekezés **csak** ebből a pontból álljon. Mivel a potenciális Internet biztonsági kockázatok különféle szinteken fordulnak elő, olyan biztonsági intézkedéseket kell hozni, amelyek a védelem területén is különféle szinteken jelentkeznek a kockázatokkal szemben.

Bár a tűzfal erős védelmet nyújt bizonyos típusú támadások ellen, a tűzfal csak része a teljes biztonsági megoldásnak. A tűzfal például nem tudja szükségszerűen megvédeni azokat az adatokat, amelyeket olyan alkalmazások segítségével küld az Interneten keresztül, mint az SMTP levelezés, az FTP és a TELNET. Hacsak nem dönt ezen adatok titkosítása mellett, bárki elérheti ezeket az adatokat az Interneten, miközben céljuk felé tartanak.

Erőteljesen meg kell fontolni a tűzfal használatát, mint a védekezés fő eszközét, valahányszor az Internethez kapcsolja az iSeries szervert vagy a belső hálózatát. Annak ellenére, hogy az IBM Firewall for AS/400 termék már nem vásárolható meg és a támogatása is megszűnt, számos más terméket használhat helyette. A különféle áttérési forgatókönyvekről olvassa el az All You Need to Know When Migrating from IBM Firewall for AS/400 című kiadványt.

Mivel a kereskedelmi forgalomban lévő tűzfal termékek a hálózati biztonságot adó technológiák teljes körét biztosítják, a JKL Toy Company kiválasztotta az egyiket az e-business biztonsági forgatókönyvben saját hálózata védelméhez. Azonban, tűzfala nem nyújt védelmet az új iSeries Internet szerver számára. Következésképpen, úgy határozott a cég, hogy megvalósítja az iSeries Csomag szabályok funkciót, amely révén létrehozza a szűrő- és NAT szabályokat az Internet szerver forgalmának vezérlésére.

Az iSeries csomag szabályokról

A csomagszűrő szabályok révén megvédheti számítógépes rendszereit azzal, hogy visszautasítja vagy elfogadja az IP csomagokat a megadott feltételek alapján. A NAT szabályok lehetővé teszik, hogy eltakarja a rendszer belső információit a külső felhasználók elől, amit úgy ér el, hogy lecseréli az egyik IP címet egy másik, nyilvános IP címre. Annak ellenére, hogy az IP csomagszűrés és a NAT szabályok a hálózatok biztonsági technológiájának magjai, nem nyújtanak olyan szintű védelmet, mint egy teljes funkciójú tűzfal termék. Gondosan elemeznie kell biztonsági igényeit és céljait, amikor döntést hoz a teljeskörű tűzfal termék és az iSeries csomag szabályok funkció közötti választásról.

Tekintse át az iSeries hálózati biztonság opcióinak kiválasztása című részt, amely segít eldönteni azt, hogy melyik megközelítés elégíti ki biztonsági igényeit.

Kapcsolódó fogalmak

"A réteges védelem elve a biztonságért" oldalszám: 4
A **biztonsági irányelve** meghatározza, hogy mit akar védeni, és mit vár el a rendszer felhasználóitól.

"Forgatókönyv: JKL Toy Company e-business tervek" oldalszám: 8
A forgatókönyv egy tipikus vállalkozást, a JKL Toy Company nevű céget írja le, amely elhatározta, hogy üzleti célkitűzéseit kibővíti az Internet használattal. Annak ellenére, hogy a cég kitaláció csupán, terveik - nevezetesen az Internet használata elektronikus kereskedelem céljára - és az ennek eredményeképpen felmerülő biztonsági igények, számos valós nemzetközi vállalat helyzetét képviselik.

"iSeries csomag szabályok" oldalszám: 14
Az iSeries csomag szabályok az i5/OS beépített funkciója, amelyet az iSeries navigátorból érhet el.

"Az iSeries hálózatbiztonsági beállítások kiválasztása" oldalszám: 15
Tömör leírást ad arról, hogy milyen biztonsági beállításokat kell kiválasztani az Internet használati tervek alapján.

Kapcsolódó tájékoztatás

All You Need to Know When Migrating from IBM Firewall for AS/400

Tűzfalak

A tűzfal gát egy biztonságos belső hálózat és egy nem megbízható hálózat (például az Internet) között.

A legtöbb cég tűzfalat használ a belső hálózatuk biztonságos Internet kapcsolatához, bár a tűzfalak segítségével az intraneten is elkülöníthető egy biztonságos belső hálózat egy másiktól.

A tűzfal egyetlen, ellenőrzött kapcsolódási ponttal rendelkezik (úgynevezett fojtópont) a biztonságos belső hálózat és a nem megbízható hálózat között. A tűzfal:

- Lehetővé teszi a belső hálózat felhasználói számára a külső hálózaton található engedélyezett erőforrások használatát.
- Megakadályozza, hogy a külső hálózat jogosulatlan felhasználói a belső hálózat erőforrásait használják.

Amikor az Internethez (vagy más hálózathoz) tűzfalat használ átjáróként, akkor meglehetősen csökkenti a belső hálózat kockázatát. A tűzfal használata a hálózat adminisztrációját is egyszerűsíti, mert a tűzfal funkciók biztonsági stratégiájának legtöbb feladatát átvállalják.

A tűzfal működése

A tűzfal működésének megértéséhez képzelje el azt, hogy az Ön hálózata egy épület, amelynek az elérését ellenőrizni szeretné. Az épület egyetlen belépési pontja az előcsarnok. Az előcsarnokban a recepciósok üdvözlik a vendégeket, a biztonsági őrök figyelik a vendégeket, a videokamerák felveszik a vendégek tevékenységeit, a kártyaleolvasók pedig azonosítják az épületbe belépő vendégeket.

Ezek az intézkedések jól működhetnek egy épület esetében. Ha viszont egyszer egy jogosulatlan személynek sikerül bejutnia az épületbe, akkor már nem lehet megvédeni az épületet a behatoló cselekményeitől. Ha azonban figyeli a behatoló mozdulatait, esélye lesz a behatoló bármely gyanús tevékenységének felfedezésére.

Tűzfal összetevők

A tűzfal hardver és szoftver elemek olyan gyűjteménye, amelyek együttesen a hálózat egy részének jogosulatlan elérését gátolják meg. A tűzfal az alábbi összetevőkből áll:

- Hardver. A tűzfal hardver általában egy külön számítógépből vagy eszközből áll, amely kizárólag a tűzfal szoftver funkcióit futtatja.
- Szoftver. A tűzfal szoftver különféle alkalmazásokat nyújt. A hálózati biztonság fogalmával összhangban a tűzfal biztonsági vezérléseket nyújt a különféle technológiák révén:
  - Internet protokoll (IP) csomagszűrés
  - Hálózati cím fordítás (NAT) szolgáltatások
  - SOCKS szerver
  - Proxy szerverek különféle szolgáltatásokkal, például HTTP, Telnet, FTP, és így tovább
  - Levéltovábbítási szolgáltatás
  - Tartománynév szolgáltatások (DNS) felosztása
  - Naplózás
  - Valós idejű megfigyelés

Megjegyzés: Egyes tűzfal termékek virtuális saját hálózat (VPN) szolgáltatást nyújtanak, amely lehetővé teszi titkosított szekciók beállítását a tűzfal és más kompatíbilis tűzfalak között.

Tűzfal technológiák használata

A belső felhasználók számára az Internet szolgáltatások biztonságos elérését tűzfal, proxy, SOCKS szerverek vagy NAT segítségével biztosíthatja. A proxy és SOCKS szerverek a tűzfalnál megszakítják a TCP/IP kapcsolatokat a belső hálózat információinak elrejtéséhez a nem megbízható hálózatok elől. A szerverek naplózási lehetőségeket is biztosítanak.

A NAT segítségével biztosíthatja az Internet felhasználóinak a tűzfalon belüli nyilvános szerver könnyű elérését. A tűzfal továbbra is védi a hálózatát, mivel a NAT elrejti a belső IP címeket.

A tűzfal azzal is védi a belső információkat, hogy DNS szervert biztosít saját maga általi felhasználásra. Valójában két DNS szerverrel rendelkezik: az egyik a belső hálózat adatait tartalmazza, míg a másik (a tűzfalban lévő) a külső hálózatoknak és magának a tűzfalnak az adatait tartalmazza. Ez lehetővé teszi, hogy vezérelje a belső rendszerek információinak kívülről történő elérését.

A tűzfal stratégia átgondolásakor azt gondolhatja, hogy elég az összes kockázati lehetőséget megtiltani, és minden mást engedélyezni. A számítógépes bűnözők azonban új és új támadási módszereket találnak ki, így ezek megelőzésére is gondolni kell. Az épület példájához hasonlóan az olyan jeleket is figyelni kell, amelyek arra utalhatnak, hogy valaki valahogyan megsértette a védelmi rendszert. Általában jóval károsabb és drágább a betörések következményeinek orvoslása, mint azok megakadályozása.

A tűzfalak esetében ezért a legjobb megoldás az, hogy csak azokat az alkalmazásokat engedélyezi, amelyek a tesztek során megbízhatónak bizonyultak. Ha ezt a stratégiát követi, akkor kimerítően definiálnia kell a tűzfalon futtatni kívánt szolgáltatások listáját. Minden szolgáltatást jellemezhet a kapcsolat irányával (bentről kifelé, vagy kintről befelé). Továbbá sorolja fel azokat a felhasználókat, akik számára az egyes szolgáltatásokat engedélyezi, és a gépeket, amelyek kapcsolódhatnak ezekhez a szolgáltatásokhoz.

Amitől a tűzfal meg tudja védeni a hálózatot

A tűzfal telepítésére a saját hálózat és az Internet (vagy más megbízhatatlan hálózat) csatlakozási pontján kerül sor. Ezután a tűzfal lehetővé teszi a hálózati belépési pontok számának korlátozását. A tűzfal egyetlen kapcsolódási ponttal

rendelkezik (úgynevezett fojtópont) a belső hálózat és az Internet között. Mivel csak egyetlen kapcsolódási pont van, széleskörűbb ellenőrzéssel rendelkezik afelett, hogy milyen forgalmat engedélyezzen a hálózatba be-, illetve kiáramlani.

A tűzfal a nyilvánosság számára egyetlen címként jelenik meg. A tűzfal a nem megbízható hálózathoz proxy vagy SOCKS szervereken vagy Hálózati cím fordításon (NAT) keresztül tesz lehetővé kapcsolatot, miközben elrejti a belső hálózati címeket. Ebből következően a tűzfal fenntartja a belső hálózat bizalmasságát. A tűzfal a hálózattal kapcsolatos információk bizalmasságának megőrzésével csökkenti a megszemélyesítéses támadások (hamisítások) kockázatát.

A tűzfal lehetővé teszi a hálózatba be- és kiáramló forgalom felügyeletét a hálózatot érintő támadások kockázatának minimálisra csökkentése érdekében. A tűzfal biztonságosan szűri a hálózatba belépő összes forgalmat, hogy csak meghatározott típusú címzetthez vagy helyre irányuló forgalom léphessen be. Ez minimálisra csökkenti annak kockázatát, hogy valaki a TELNET vagy a fájlátviteli protokoll (FTP) segítségével hozzáférhessen a belső rendszerekhez.

Amitől a tűzfal nem tudja megvédeni a hálózatot

Bár a tűzfal erős védelmet nyújt bizonyos típusú támadások ellen, a tűzfal csak része a teljes biztonsági megoldásnak. A tűzfal például nem tudja szükségszerűen megvédeni azokat az adatokat, amelyeket olyan alkalmazások segítségével küld az Interneten keresztül, mint az SMTP levelezés, az FTP és a TELNET. Hacsak nem dönt ezen adatok titkosítása mellett, bárki elérheti ezeket az adatokat az Interneten, miközben céljuk felé tartanak.

iSeries csomag szabályok

Az iSeries csomag szabályok az i5/OS beépített funkciója, amelyet az iSeries navigátorból érhet el.

A csomag szabályok lehetővé teszik két hálózati biztonsági technológia konfigurálását, amelyekkel vezérelheti a TCP/IP forgalmat az iSeries rendszer védelme érdekében:

- Hálózati cím fordítás (NAT)
- IP csomagszűrés

Mivel a NAT és az IP szűrés az i5/OS részei, ezért gazdaságos módszert jelentenek a rendszer biztonságossá tételéhez. Bizonyos esetekben ezek a biztonsági technológiák minden igényt kielégítenek anélkül, hogy további eszközöket kellene vásárolnia. Ugyanakkor ezek a technológiák nem hoznak létre valós, működő tűzfalat. Az IP csomag biztonságot használhatja egymagában is, vagy tűzfallal, a biztonsági szükségleteitől és céljaitól függően.

Megjegyzés: Ne törekedjen költség megtakarításra, amikor a biztonságot tervezi az iSeries termelési rendszeren. Az ilyen helyzetekben a rendszer biztonságának szempontjait előnyben kell részesíteni a költségekhez képest. Gondolja meg a tűzfal használatát, ha biztos akar abban lenni, hogy maximális védelmet biztosít a termelési rendszernek.

Mi a NAT és az IP csomagszűrés, hogyan működnek együtt?

A hálózati címfordítás (NAT) megváltoztatja a rendszeren átmenő csomagok forrás vagy cél IP címeit. A NAT átláthatóbb alternatívát jelent, mint a tűzfal proxy és SOCKS szerverei. A NAT ugyancsak egyszerűsítheti a hálózat konfigurálását, ha engedélyezi inkompatíbilis címzésű hálózatoknak, hogy egymáshoz kapcsolódjanak. Következésképpen, használhatja úgy a NAT szabályokat, hogy az iSeries rendszer átjáróként működhessen a két hálózat között, amelyek konfliktusban állnak egymással inkompatíbilis címzési sémájuk miatt. A NAT funkcióval eltakarhatja a hálózat valós IP címeit azáltal, hogy dinamikusan lecseréli őket egy vagy több címre. Mivel az IP csomagszűrés és a NAT kiegészíti egymást, gyakran együtt használja a hálózati biztonság javítása érdekében.

A NAT használatával könnyebbé tehető a nyilvános webszerver működése a tűzfal mögött. A webszerver nyilvános IP címeit lefordítja saját belső IP címekre. Ez csökkenti a szükséges, regisztrált IP címek számát, és minimalizálja a meglévő hálózatra gyakorolt hatását. Eljárást biztosít a belső felhasználóknak ahhoz, hogy elérjék az Internetet, miközben eltakarja a saját belső IP címeket.

Az **IP csomagszűrés** lehetőséget biztosít ahhoz, hogy szelektíven blokkolja vagy védje az IP forgalmat a csomag fejlécben lévő információk alapján. Az iSeries navigátor Internet beállítási varázslójával gyorsan és könnyen konfigurálhatja az alapszintű szűrő szabályokat a nemkívánatos hálózati forgalom blokkolása érdekében.

Az IP csomagszűrést a következőkhöz használhatja:

- A szűrő szabályok létrehozásával megadhatja, mely IP csomagokat engedi be a hálózatba, és melyeknek utasítja vissza a hálózathoz való hozzáférést. Amikor létrehozza a szűrő szabályokat, egy fizikai interfészhez alkalmazza őket (például Token ring vagy Ethernet vonal). A szabályokat több fizikai interfészhez is alkalmazhatja, de különböző szabályokat is alkalmazhat minden egyes interfészhez.
- A szabályok létrehozásával engedélyez vagy visszautasít bizonyos csomagokat, ami a következő fejléc információkon alapul:
  - Cél IP cím
  - Forrás IP cím protokoll (például TCP, UDP és így tovább)
  - Célport (például a 80-as port a HTTP-hez)
  - Forrásport
  - IP adatcsomag irány (befelé vagy kifelé tartó)
  - Továbbított vagy helyi
- Megakadályozhatja, hogy a nemkívánatos vagy szükségtelen forgalom elérje a rendszeren lévő alkalmazásokat. Ehhez hasonlóan, megakadályozhatja a forgalom továbbítását más rendszerekhez is. Ez magában foglalja az alacsony szintű ICMP csomagokat (például PING csomagok), amelyekhez nincs szükség különleges alkalmazás szerverre.
- Megadhatja, hogy a szűrő szabály hozzon-e létre naplóbejegyzést a rendszernaplóban a szabályoknak eleget tevő csomagokról. Mihelyt az információ a rendszernaplóba kerül, a naplóbejegyzést nem változtathatja meg. Következésképpen, a napló ideális eszköz a hálózati tevékenység ellenőrzéséhez.

Kapcsolódó fogalmak

“Hálózatbiztonsági beállítások” oldalszám: 11
Az itt leírtak segítségével tanulmányozhatja a hálózatszintű biztonsági intézkedéseket, amelyek használatát meg kell fontolni a belső erőforrások védelme érdekében.

Hálózati cím fordítás (NAT)

IP csomagszűrés

Az iSeries hálózatbiztonsági beállítások kiválasztása

Tömör leírást ad arról, hogy milyen biztonsági beállításokat kell kiválasztani az Internet használati tervek alapján.

A jogosulatlan hozzáférés ellen védő hálózatbiztonsági megoldások általában tűzfal technológiákra épülnek. Az iSeries rendszer védelméhez választhat egy teljes funkciójú tűzfal terméket, vagy életbe léptethet bizonyos hálózatbiztonsági technológiákat az i5/OS TCP/IP megvalósítás részeként. Ez a megvalósítás a Csomag szabályokból (amely magában foglalja az IP szűrést és a NAT funkciót) és a HTTP for iSeries proxy szerver funkcióból áll.

A hálózati környezettől, a hozzáférési követelményektől és a biztonsági igényektől függ az, hogy a Csomag szabályokat választja vagy egy tűzfal terméket. A védekezés fő erejeként **erősen** fontolja meg a tűzfal használatát, valahányszor az iSeries szervert vagy a belső hálózatot Internethez vagy egyéb, nem megbízható hálózathoz csatlakoztatja.

Ebben az esetben a tűzfal előnyösebb, mivel a tűzfal jellemzően olyan dedikált hardver- és szoftver eszköz, amely korlátozott számú interfészt biztosít a külső hozzáférések számára. Amikor i5/OS TCP/IP technológiákat alkalmaz az Internet elérés védelméhez, egy olyan általános célú számítástechnikai platformot használ, amely számtalan csatolófelületet és alkalmazást nyit meg a külső hozzáférések számára.

A különbség több okból is fontos. Például, a dedikált tűzfal termék semmilyen egyéb funkciót vagy alkalmazást nem biztosít azon túlmenően, mint amit maga a tűzfal tartalmaz. Következésképpen, ha egy támadó sikeresen feltöri is a tűzfalat, és így hozzáférést nyer, nem sokat tud tenni. Ugyanakkor, ha a támadó a TCP/IP biztonsági funkciókat töri fel

az iSeries szerveren, potenciálisan elérheti a különféle hasznos alkalmazásokat, szolgáltatásokat és adatokat. A támadó ezek segítségével nagymértékben tönkreteheti magát a rendszert, vagy hozzáférhet a belső hálózat más rendszereihez.

Szóval, valaha is elfogadható az iSeries TCP/IP biztonsági funkciók használata? Mint minden biztonsággal kapcsolatos döntést, a költségek és az elviselhető kompromisszumok összevetésén alapulva kell meghozni. Elemezni kell üzleti céljait, és el kell dönteni, milyen kockázatokat tud elfogadni, szembeállítva ezzel azt a költséget, amennyiért nyújtani tudja a kockázatokat minimalizáló biztonságot. A következő táblázat ismerteti, hogy mikor alkalmasabb a TCP/IP biztonsági funkciók használata a teljes funkciójú tűzfalnál. A táblázat segítségével meghatározhatja, hogy a tűzfalat, a TCP/IP biztonsági funkciókat vagy a kettő kombinációját használja-e a hálózat és a rendszer védelme érdekében.

Biztonsági technológia	Legjobb az i5/OS TCP/IP technológia használata	Legjobb a teljes funkciójú tűzfal használata
IP csomagszűrés	• **További** védelmet nyújt az egyedi iSeries szervereknek, mint például egy nyilvános webszervernek vagy egy érzékeny adatokkal rendelkező intranet rendszernek. • A vállalati **intranet** egyik alhálózatát védi, amikor az iSeries rendszer átjáróként szerepel (alkalmanként útválasztóként) a hálózat többi része számára. • A kommunikációt vezérli, ami egy némiképp megbízható partnerrel folyik **magán hálózaton** vagy extraneten keresztül, ahol az iSeries szerver átjáróként szerepel.	• Az egész vállalati hálózatot védi az **Internet** vagy más nem megbízható hálózat (amelyhez a hálózata csatlakozik) kockázataitól. • Az erős forgalommal rendelkező, nagy alhálózatot védi a vállalati hálózat maradékával szemben.
Hálózati cím fordítás (NAT)	• Kapcsolatot engedélyez két **magánhálózat** között, amelyek inkompatíbilis címzési struktúrával rendelkeznek. • Eltakarja a címeket az alhálózatban a kevésbé megbízható hálózatok elől.	• Eltakarja a kliens címeket, amikor **Internethez** vagy más, nem megbízható hálózathoz csatlakozik. A proxy és a SOCKS szerverek alternatívájaként használhatja. • A magán hálózat rendszerének szolgáltatásait elérhetővé teszi az **Internet** felhasználóknak.
Proxy szerver	• A **távoli helyszíneket** bevonja a vállalati hálózatba, amikor egy központi tűzfal biztosítja az Internet hozzáférést.	• Az egész vállalati hálózatot fogja át az **Internet** hozzáférés során.

Az alábbi helyeken tanulmányozhatja az i5/OS TCP/IP biztonsági funkciókat:

- *Csomag szabályok (szűrés és NAT)* témakör a V5R1 IBM Systems Szoftver információs központban.
- *HTTP Server Documentation Center* a következő címen:
  `http://www.iseries.ibm.com/domino/reports.htm`
- AS/400 Internet Security Scenarios: A Practical Approach redbook (SG24-5954).

Kapcsolódó fogalmak

“Hálózatbiztonsági beállítások” oldalszám: 11
Az itt leírtak segítségével tanulmányozhatja a hálózatszintű biztonsági intézkedéseket, amelyek használatát meg kell fontolni a belső erőforrások védelme érdekében.

Alkalmazásbiztonsági beállítások

Ismerteti a biztonsági kockázatokat és az ilyen kockázatok kezelésére szolgáló opciókat számos népszerű Internetes alkalmazás és szolgáltatás esetében.

Az alkalmazásszintű biztonsági intézkedések azt vezérlik, hogy a felhasználók hogyan működhetnek együtt az adott alkalmazásokkal. Általában konfigurálni kell a biztonság beállításokat minden egyes alkalmazás esetében, amelyet

használ. Azonban, különös figyelmet kell fordítani a biztonság beállítására azoknál az alkalmazásoknál és szolgáltatásoknál, amelyeket igénybe vesz vagy szolgáltat az Interneten. Az ilyen alkalmazások és szolgáltatások sebezhetőek, a jogosulatlan felhasználók visszaélve ezzel módot találhatnak arra, hogy hozzáférjenek a hálózat rendszereihez. A biztonsági intézkedéseknek le kell fedni a szerver- és a kliens oldali biztonsági kockázatokat.

Miközben nagyon fontos, hogy minden alkalmazást biztonságossá tegyen, ezek a biztonsági intézkedések csak egy kis részét jelentik az átfogó biztonsági irányelvek megvalósításának.

Az alábbi lapokon tanulmányozhatja, hogyan tehet biztonságossá számos, általános Internet alkalmazást:

Kapcsolódó fogalmak

“A réteges védelem elve a biztonságért” oldalszám: 4
A **biztonsági irányelve** meghatározza, hogy mit akar védeni, és mit vár el a rendszer felhasználóitól.

Web szolgáltatás biztonsága

Amikor hozzáférést biztosít a saját honlapja látogatóinak, nem áll szándékában tájékoztatni őket arról, hogyan állította be a helyet, és milyen kódolást használt a lap generálásához.

Azt szeretné, hogy honlapjának meglátogatása könnyű, gyors és gördülékeny legyen a színfalak mögött végzett összes munka megjelenésével együtt. Adminisztrátorként bizonyos akar abban lenni, hogy biztonsági gyakorlata nincs negatív hatással a webhelyre. Amikor az iSeries webszerverként működik, fontolja meg az alábbi pontokat:

- Az adminisztrátornak direktívákat kell megadnia a szerveren, mielőtt a kliens együttműködne a HTTP szerverrel. A biztonsági ellenőrzés céljára két módszer kínálkozik: általános szerver direktívák és szerver védelmi direktívák. A webszerverhez érkező bármilyen kérés eleget kell, hogy tegyen a direktívák által meghatározott összes korlátozásnak, mielőtt a szerver elfogadná a kérést.
- A szerver konfigurációt meghatározó szerver adminisztrációs weblapon hozhatja létre és szerkesztheti ezeket a direktívákat. A szerver direktívák lehetővé teszik a webszerver viselkedésének átfogó vezérlését. A szerver védelmi direktívák lehetővé teszik biztonsági modell megadását és vezérlését, amelyet a szerver saját maga által kezelt, megadott URL címekre használ.
- A szerver konfigurálásához használhatja a kiosztási (map) vagy az átengedési (pass) direktívákat és a szerver adminisztrációs weblapjait.
  - A kiosztási vagy az átengedési direktívák segítségével maszkolhatja a fájl neveket az iSeries webszerveren. Még pontosabban, a PASS és a MAP szerver direktívák vezérlik az alkönyvtárakat, ahonnan a webszerver kiszolgálja az URL címeket. Létezik egy EXEC szerver direktíva is, amely vezérli a könyvtárakat, ahol a CGI-BIN programok találhatók.

    Minden egyes szerver URL-hez meghatározhat védelmi direktívákat. Nem minden URL igényel védelmi direktívát. De, ha vezérelni kívánja, hogy melyik URL erőforrás legyen elérhető és ki által, akkor az adott URL címhez szükség van védelmi direktívára.
  - Inkább a szerver adminisztrációs weblapját használja a szerver konfigurálásához, mint a WRKHTTPCFG (Work with HTTP Configuration) parancsot és a direktívák begépelését. A védelmi direktívák kezelése nagyon bonyolult lehet a parancssori kezelőfelületen keresztül. Ennek következtében ajánlatos a szerver Admin weblapok használata, hogy megbizonyosodjon arról, a direktívák beállítása helyes.

A HTTP lehetőséget nyújt az adatbázis fájl adatainak megjelenítésére, de módosításukra nem. Mindazonáltal, van néhány olyan alkalmazás, amit írni fog, és amelyeknek frissíteniük kell egy adatbázis fájlt. Ehhez a CGI-BIN programokat használhatja. Például, létre akar hozni olyan űrlapokat, amelyeket később a felhasználó tölt ki, és frissíti vele az iSeries adatbázist. Biztonsági adminisztrátorként ellenőrizze a felhasználói profil és a funkciók jogosultságait, amelyeket a CGI programok végrehajtanak. Vizsgálja meg azt is, hogy mely érzékeny objektumok rendelkezhetnek nem megfelelő nyilvános jogosultsággal.

Megjegyzés: A Common Gateway Interface (CGI) egy ipari szabvány a webszerver és a rajta kívül található számítógépes programok közötti információcsere céljára. A programok minden olyan programozási nyelven íródhatnak, amelyet támogat a webszervert futtató gép operációs rendszere.

A CGI programokon kívül szándékában állhat Java használata is a weblapokon. Ismerje meg a Java biztonságot, mielőtt Java résszel bővítené weblapjait.

A HTTP szerver hozzáférési naplót készít, amelyet felhasználhat a szerver hozzáférések és a hozzáférési kísérletek figyelésére.

A proxy szerver fogadja a HTTP kéréseket a web böngészőtől és elküldi őket a webszervereknek. A webszerverek, amelyek fogadják ezeket a kéréseket, csak a proxy szerver IP címére vannak felkészítve. Ők nem tudják meghatározni a kéréseket kezdeményező PC-k nevét vagy címét. A proxy szerver kezelni tudja a HTTP, a File Transfer Protocol (FTP), a Gopher és a WAIS funkciókra vonatkozó URL kéréseket.

Használhatja az IBM HTTP Server for iSeries HTTP proxy támogatását is a web hozzáférés állandósítása céljából. A proxy szerver ugyancsak naplózza az összes URL kérést követési célból. Azután átnézheti a naplót, hogy ellenőrizze a hálózati erőforrások használatát és a velük való visszaélést. A HTTP proxy szerver használatáról további tájékoztatást talál az IBM HTTP Server for iSeries dokumentációs központjában a következő URL címen:

| `http://www.ibm.com/eserver/iseries/products/http/docs/doc.htm`

Kapcsolódó fogalmak

"Java Internet biztonság"
A Java programozás egyre szélesebb körben terjed napjaink számítástechnikai környezetében.

Java Internet biztonság

A Java programozás egyre szélesebb körben terjed napjaink számítástechnikai környezetében.

Például, használhatja az IBM Toolbox for Java vagy az IBM Development Kit for Java termékeket a rendszeren az új alkalmazások fejlesztéséhez. Következésképpen, fel kell készülnie a Java nyelvhez tartozó biztonsági kérdések kezeléséhez. Bár a tűzfal jó védekezési mód a legáltalánosabb Internetes biztonsági kockázatokkal szemben, azonban nem nyújt védelmet számos Java alapú kockázat ellen. A biztonsági irányelvekben ki kell egészíteni a rendszer védelmét három Java jellegű terület (alkalmazások, kisalkalmazások, és szerver kisalkalmazások) szempontjaival. Azt is meg kell ismerni, hogyan működik együtt a Java és az erőforrás biztonság a Java programokra vonatkozó hitelesítési és jogosultsági kifejezésekkel.

Java alkalmazások

Mint programozási nyelv, a Java rendelkezik néhány olyan jellemzővel, ami védi a Java programozókat attól, hogy a sértetlenséget veszélyeztető, akaratlan hibákat kövessenek el. (A PC-s alkalmazásokhoz általánosan használt egyéb nyelvek, mint például a C vagy a C++, nem védik a programozókat az akaratlan tévedésektől olyan erősen, mint ahogy azt a Java teszi.) Például, a Java erőteljes gépelést használ, ami védi a programozót attól, hogy az objektumokat meg nem fontolt módon használja. A Java nem engedi meg a mutató manipulációt, ami védi a programozót attól, hogy véletlenül is kilépjen a program memóriahatárán kívülre. Az alkalmazásfejlesztés szempontjából a Java ugyan olyannak tekinthető, mint a többi magas szintű nyelv. Ugyanazokat a biztonsági szabályokat kell alkalmazni az alkalmazás tervezésénél, mint amelyeket más nyelvekre is alkalmaz az iSeries szerveren.

Java kisalkalmazások

A Java kisalkalmazások kicsi Java programok, amelyeket magukban foglalhatnak a HTML lapok. Mivel a kisalkalmazások a kliensen futnak, ezért amit csinálnak, a kliensnél kell figyelembe venni. Mindazonáltal, a Java kisalkalmazás rendelkezik az iSeries szerver elérési lehetőségével. (A hálózatban lévő PC-n működő ODBC vagy fejlett program-program kommunikáció (APPC) programok ugyancsak elérhetik az iSeries szervert.) Általánosságban elmondható, hogy a Java kisalkalmazások csak azzal a szerverrel tudnak szekciót létrehozni, amelyiktől a kisalkalmazás ered. Ennek következtében, a Java kisalkalmazás csak akkor érheti el az iSeries szervert a kapcsolódó PC-ről, ha a kisalkalmazás az iSeries szerverről jött (például a webszerveréről).

| A kisalkalmazás megpróbálhatja a kapcsolódást a szerver bármelyik TCP/IP portján. Nem kell egyeztetni a Java
| nyelven írt szoftver szerverrel. De, az IBM Toolbox for Java segítségével írt szerverek esetében, a kisalkalmazásnak
| felhasználói azonosítót és jelszót kell szolgáltatni, amikor kapcsolatot létesít vissza a szerverhez. Ebben az anyagban a
| leírt szerverek mindegyike iSeries szerver. (A Java nyelven írt szervernek nem kell használni az IBM Toolbox for Java
| terméket). Jellemzően, az IBM Toolbox for Java osztály bekéri a felhasználótól a felhasználói azonosítót és a jelszót az
| első kapcsolat során.

A kisalkalmazás csak akkor hajthat végre funkciókat az iSeries szerveren, ha a felhasználói profil rendelkezik az adott funkciókhoz szükséges jogosultságokkal. Ennek következtében, elengedhetetlen egy jó erőforrás biztonsági séma megléte, amikor elkezd Java kisalkalmazásokat használni új alkalmazási funkciók nyújtásához. Amikor a rendszer feldolgozza a kisalkalmazásoktól jövő kéréseket, nem alkalmazza a felhasználó profiljában lévő, korlátozott képességre vonatkozó értéket.

A kisalkalmazás megjelenítő lehetővé teszi a kisalkalmazás tesztelését a szerver rendszeren - mindazonáltal - ez nem esik a böngésző biztonsági korlátozásai alá. Ennek következtében, a kisalkalmazás megjelenítőt mindig csak a saját kisalkalmazásainak tesztelésére használja, soha ne futtasson külső forrásból származó kisalkalmazásokat. A Java kisalkalmazások gyakran írnak a felhasználó PC meghajtójára, ami alkalmat adhat arra a kisalkalmazásnak, hogy romboló hatású műveletet hajtson végre. Mindazonáltal, használhatja a digitális igazolást a Java kisalkalmazás aláírásához, hogy létrehozza a hitelesítést. Az aláírt kisalkalmazás írhat a PC helyi meghajtóira még akkor is, ha a böngésző alapértelmezett beállítása megakadályozza ezt. Az aláírt kisalkalmazás leképezett meghajtókra is képes írni az iSeries szerveren, mert a PC számára helyi lemezegységekként jelennek meg.

Megjegyzés: A fent leírt viselkedés általában igaz a Netscape Navigator és az MS Internet Explorer esetében. Hogy mi is történik valójában, az attól függ, hogyan konfigurálja és kezeli a böngészőket, amiket használ.

Az iSeries szerverről eredő Java kisalkalmazások esetén, esetleg alá kell írnia a kisalkalmazásokat. Mindazonáltal, utasítani kell a felhasználókat, hogy lehetőleg ne fogadjanak el aláírt alkalmazásokat ismeretlen forrásból.

A V4R4 változat óta használhatja az IBM Toolbox for Java programot a Védett socket réteg (SSL) környezet beállításához. Használhatja az IBM Developer Toolkit for Java programot is, hogy biztonságossá tegye a Java alkalmazást az SSL segítségével. Ha a Java alkalmazásokhoz SSL-t használ, biztosítja az adatok titkosítását, beleértve a felhasználói azonosítót és a jelszót is, ami így átadható a kliens és a szerver között. A regisztráltatott Java programok SSL használatra való konfigurálásához használja a Digitális igazolás kezelő című témakört.

Java szerver kisalkalmazások

A szerver kisalkalmazások szerver oldali, Java nyelven írt összetevők, amelyek dinamikusan kiterjesztik a webszerver funkcionalitását a webszerver kód megváltoztatása nélkül. Az IBM WebSphere Application Server, amely az IBM HTTP Server for iSeries termékkel együtt érkezik, támogatja a szerver kisalkalmazások használatát az iSeries rendszereken.

Erőforrás biztonságot kell beállítani azokra a szerver kisalkalmazás objektumokra, amelyeket a szerver használ. Azonban, az erőforrás biztonság alkalmazása a szerver kisalkalmazásra még jelent elegendő védelmet. Amint a webszerver betölti a szerver kisalkalmazást, az erőforrás biztonság már nem tudja megakadályozni azt, hogy mások is futtassák. Következésképpen, az erőforrás biztonság mellett használni kell a HTTP szerver biztonsági vezérléseket és direktívákat is. Például, ne engedélyezze, hogy a szerver kisalkalmazások csupán a webszerver profilja alatt fussanak. Továbbá, irányítsa, hogy ki futtathatja a szerver kisalkalmazást (maszk kulcsszavak a védelmi direktívában) a HTTP szerver csoportok és hozzáférés vezérlési listák (ACL) bevonásával. Valamint használja a szerver kisalkalmazás fejlesztőeszközei által nyújtott biztonsági funkciókat, mint amilyeneket a WebSphere Application Server for iSeries tartalmaz.

A Java általános biztonsági rendszabályait az alábbi helyen tanulmányozhatja: IBM Systems Szoftver információs központ.

- *IBM Developer Kit for Java Java biztonság*.
- *IBM Toolbox for Java biztonsági osztályok*.

Java hitelesítés és erőforrás jogosultság

Az IBM Toolbox for Java biztonsági osztályokat tartalmaz, amely ellenőrzi a felhasználó azonosságát, és választhatóan hozzárendeli ezt az azonosságot az operációs rendszer végrehajtási szálához egy alkalmazás vagy egy szerver kisalkalmazás számára, amely az iSeries rendszeren fut. Ezt követően ellenőrzi az erőforrás biztonságot a hozzárendelt

azonosság alatt. A biztonsági osztályokról részletesebb tájékoztatást ad az IBM Toolbox for Java Hitelesítési szolgáltatások című témaköre az IBM Systems Szoftver információs központban.

Az IBM Developer Kit for Java támogatja a Java Authentication and Authorization Service (JAAS) funkciókat, amelyek a Java 2 Software Development Kit (J2SDK) szabványos kiadás kiegészítői. Pillanatnyilag a J2SDK hozzáférés vezérlést nyújt, amely azon alapul, honnan ered a kód és ki írta alá (kód forrásalapú hozzáférés vezérlés). A J2SDK használatát ismerteti a Java Hitelesítési szolgáltatások című rész az IBM Developer Kit for Java témakör alatt az IBM Systems Szoftver információs központban.

Java alkalmazások SSL védelemmel

A Védett socket réteg (SSL) segítségével biztonságossá teheti az IBM Developer Kit for Java programmal fejlesztett iSeries alkalmazások kommunikációját. Az IBM Toolbox for Java programot használó kliens alkalmazások ugyancsak kihasználhatják az SSL előnyeit. Az SSL engedélyezésének folyamata a saját Java alkalmazásokra kicsit eltér attól, mint amikor más alkalmazásokra engedélyezi.

A Java alkalmazások Védett socket réteg adminisztrációjáról olvassa el az IBM Systems Szoftver információs központ témaköreit:

- IBM Toolbox for Java Védett socket réteg (SSL) környezet.
- IBM Developer Toolkit for Java: Java alkalmazás biztonságossá tétele SSL segítségével.

Kapcsolódó fogalmak

“Web szolgáltatás biztonsága” oldalszám: 17
Amikor hozzáférést biztosít a saját honlapja látogatóinak, nem áll szándékában tájékoztatni őket arról, hogyan állította be a helyet, és milyen kódolást használt a lap generálásához.

Digitális igazolás kezelő

Hitelesítési szolgáltatások

Kapcsolódó feladatok

Java alkalmazás biztonságossá tétele SSL segítségével

Kapcsolódó tájékoztatás

Java hitelesítés és hitelesítési szolgáltatás

Védett socket réteg (SSL) környezet

E-mail biztonság

Az Interneten vagy más nem megbízható hálózaton keresztül küldött e-mail biztonsági kockázatot jelent, amellyel szemben nem feltétlenül nyújt védelmet a tűzfal használata.

Feltétlenül meg kell ismerni ezeket a kockázatokat ahhoz, hogy meggyőződjön róla, biztonsági irányelvei leírják az ilyen kockázatok minimalizálásának módját.

Az e-mail olyan, mint a kommunikáció többi formája. Nagyon fontos, hogy igen meggondolt legyen, mielőtt bármilyen bizalmas információt elküldene e-mail formájában. Mivel az e-mail sok szerveren áthalad, mielőtt megkapja, ezért adódhat olyan lehetőség, hogy valaki elfogja és elolvassa azt. Következésképpen, biztonsági intézkedéseket kíván hozni azért, hogy megvédje az e-mail bizalmas jellegét.

Általános e-mail biztonsági kockázatok

Néhány jellegzetes e-mail jellegű kockázat:

- **Árasztás** (a szolgáltatás jellegű támadás visszautasításának egyik típusa) akkor fordul elő, amikor a rendszer túlterheltté válik a többszörös e-mail üzenetek miatt. Aránylag könnyű feladat egy támadó számára, hogy írjon egy egyszerű programot, amely milliószámra küld e-mail üzeneteket (beleértve üres üzeneteket is) egy e-mail szervernek, megpróbálva elárasztani ezzel a szervert. Megfelelő biztonság nélkül, a célszerver szerver visszautasítást

tapasztalhat, mivel a szerver tároló lemeze megtelik haszontalan üzenetekkel. Vagy a szerver leállítja a válaszolást, mivel a szerver összes erőforrását lefoglalja a támadásból származó levéláradat feldolgozása.

- A **haszontalan e-mail** (hulladék e-mail) halmazok küldése is egy általános támadás az elektronikus levelezés ellen. Az Interneten keresztüli e-kereskedelem növekvő volumene magával hozza a nemkívánatos vagy regisztrálatlan üzleti jellegű levelek robbanásszerű növekedését is. Az ilyen haszontalan levelek, amelyeket széles terjesztési lista alapján küldenek, megtöltik az egyes felhasználók postaládáit.
- **Titkosság** az Interneten egy másik személynek szánt e-mail elküldéséhez tartozó kockázat. Az e-mail sok szerveren áthalad, mielőtt megérkezik a címzetthez. Ha nem titkosítja az üzenetet, a hacker felkaphatja és elolvashatja a levelet a kézbesítési útvonal bármely pontján.

E-mail biztonsági beállítások

Az elektronikus levelekkel való elárasztás és a haszontalan levelek ellen úgy védekezhet, ha helyesen állítja be az e-mail szervert. A szerver alkalmazások többsége biztosít módszereket az ilyen típusú támadások kezelésére. Az Internet szolgáltatóval (ISP) együttműködve meggyőződhet arról, hogy az ISP is biztosít bizonyos további védelmet az ilyen támadásokkal szemben.

A titkosság szükséges mértékétől, valamint az e-mail alkalmazás által nyújtott biztonsági funkcióktól függ, hogy milyen további biztonsági intézkedésekre van szükség. Például, elégséges az, ha csak az e-mail üzenet tartalma marad titkos? Vagy, az e-mail üzenethez tartozó összes információt titokban kívánja tartani, mint például a küldő és a címzett IP címeit?

Néhány alkalmazás saját beépített biztonsági funkciókkal rendelkezik, amelyek biztosítják a szükséges védelmet. Például a Lotus Notes Domino számos beépített biztonsági funkcióval rendelkezik, beleértve az egész dokumentum vagy egy kis részének titkosítási képességét.

A levél titkosítása céljából a Lotus Notes Domino létrehoz egy egyedi nyilvános- és egy magánkulcsot minden felhasználó számára. A felhasználó a magánkulcsát használva titkosítja az üzenetet úgy, hogy az üzenet csak azok számára lesz olvasható, akik rendelkeznek az adott felhasználó nyilvános kulcsával. A felhasználó azoknak küldi el a nyilvános kulcsát, akiknek szánja az üzenetét, akik így felhasználhatják azt a titkosított üzenet megfejtéséhez. Ha valaki titkosított levelet küld, a Lotus Notes Domino a küldő nyilvános kulcsát fogja felhasználni az üzenet megfejtéséhez.

A program online súgója ismerteti a Notes titkosítási funkciók használatát.

Az iSeries és a rajta futó Domino biztonságáról, az alábbi helyeken találhat részletesebb tájékoztatást:

- Lotus Domino dokumentáció könyvtár a következő címen:
  `http://www.ibm.com/eserver/iseries/domino/library.htm`
- Lotus Notes és Domino R5.0 Security Infrastructure Revealed (SG24-5341)
- Lotus Domino for AS/400 Internet Mail and More (SG24-5990)

Pár opció akkor is rendelkezésre áll, amikor nagyobb titkosságot kíván biztosítani a kirendeltségek, a távoli kliensek vagy az üzleti partnerek között folyó elektronikus levelezésnek vagy egyéb információknak.

Ha az e-mail szerveren lévő alkalmazás támogatja, használhatja a Védett socket réteg (SSL) protokollt ahhoz, hogy biztonságossá tegye a szerver és az e-mail kliensek közötti kommunikációs szekciókat. Az SSL támogatja a nem kötelező kliens oldali hitelesítést is, amikor a kliens alkalmazás úgy van megírva, hogy ezt használja. Mivel az egész szekció titkosítva van, az SSL ugyancsak garantálja az adatok épségét az átvitel alatt.

A másik lehetősége, hogy Virtuális magánhálózat (VPN) kapcsolatot konfigurál. A V4R4 változattól kezdve az iSeries segítségével különféle VPN kapcsolatokat konfigurálhat, beleértve a távoli kliensek és az iSeries rendszer közötti kapcsolatokat is. Amikor VPN kapcsolatot használ, a kommunikációs végpontok között folyó teljes forgalom titkosítva van, ami biztosítja az adatok titkosságát és sérthetetlenségét.

Kapcsolódó fogalmak

Virtuális magánhálózat (VPN)

“FTP biztonság”
Az FTP (fájlátviteli protokoll) fájlátviteli képességet biztosít egy kliens (egy felhasználó egy másik rendszeren) és a szerver között.

“A réteges védelem elve a biztonságért” oldalszám: 4
A **biztonsági irányelve** meghatározza, hogy mit akar védeni, és mit vár el a rendszer felhasználóitól.

Kapcsolódó hivatkozás

Biztonsági szakkifejezések

FTP biztonság

Az FTP (fájlátviteli protokoll) fájlátviteli képességet biztosít egy kliens (egy felhasználó egy másik rendszeren) és a szerver között.

A távoli parancs segítségével elküldhet parancsokat a szervernek. Következésképpen, az FTP nagyon hasznos a távoli rendszerek kezeléséhez, illetve a fájlok rendszerek közötti mozgatásához. Azonban az FTP használata Interneten vagy egyéb nem megbízható hálózatokon keresztül, bizonyos biztonsági kockázatokkal jár. Feltétlenül meg kell ismerni ezeket a kockázatokat ahhoz, hogy meggyőződjön róla, biztonsági irányelvei leírják az ilyen kockázatok minimalizálásának módját.

- Az objektum jogosultsági sémája nem biztos, hogy elégséges védelmet nyújt, amikor engedélyezve van az FTP a rendszeren.

  Például, az objektumok nyilvános jogosultsága *USE lehet, de a felhasználók többségét most megakadályozhatja az ilyen objektumok elérésében az úgynevezett ″menü biztonság″ segítségével. (A menü biztonság megakadályozza a felhasználókat abban, hogy valamit is csináljanak, ami nem a saját menüjük része.) Mivel az FTP felhasználók nincsenek menüre korlátozva, a rendszeren lévő összes objektumot elolvashatják.

  Néhány lehetőség az ilyen biztonsági kockázatok vezérlésére:

  – Léptesse életbe az iSeries teljes objektum biztonságát a rendszeren (másszóval, változtassa meg a rendszer biztonsági modelljét ″menü biztonságról″ ″objektum biztonságra″. Ez a legjobb, legbiztonságosabb beállítás.
  – Írjon kilépési programokat az FTP funkcióhoz, hogy azokra a fájlokra korlátozza a hozzáférést, amelyek átvihetők az FTP funkcióval. Ezeknek a kilépési programoknak legalább olyan biztonságot kell adniuk, mint amilyet a menü program biztosít. Sok ügyfél valószínűleg még jobban szeretné korlátozni az FTP hozzáférés vezérlést. Ez a beállítás csak az FTP funkcióra vonatkozik, más illesztőfelületekre, mint például ODBC, DDM vagy DRDA, nem.

    Megjegyzés: A fájl *USE jogosultsága megengedi a felhasználónak a fájl letöltését. A fájl *CHANGE jogosultsága megengedi a felhasználónak a fájl feltöltését.

- A hacker az FTP szerver felhasználásával képes ″szolgáltatás visszautasítást″ elérni a rendszeren, és egyúttal a felhasználói profilokat letiltatni. Ez történik, amikor egy felhasználói profillal érvénytelen jelszót használva addig próbál ismételten bejelentkezni, amíg a felhasználói profilt le nem tiltja a rendszer. Az ilyen jellegű támadás letiltja a profilt, ha a kísérletek száma eléri a hármat, azaz a maximális bejelentkezési számot.

  Az ilyen kockázatok elkerüléséért azt teheti, hogy elemzi a kompromisszumokat, aminek két oldala van: egyrészt a támadás kockázatának minimalizálása céljából a biztonság elfogadható szintre emelése, másrészt ezzel szemben a felhasználóknak nyújtott könnyű hozzáférés biztosítása. Az FTP szerver rendszerint ráerőlteti a QMAXSIGN rendszerváltozóra, hogy az megakadályozza a hackereket a korlátlan bejelentkezési kísérletektől, amivel kitalálhatnák a jelszót és ennek következtében támadást hajthatnának végre. Néhány lehetőség, amelyet érdemes megfontolni:

  – Alkalmazzon bejelentkezési programot az FTP szerveren, amellyel visszautasíthatja az összes rendszer felhasználói profil bejelentkezési kísérletét, valamint az olyan felhasználói profilokét is, amelyeknek nem óhajtja megengedni az FTP hozzáférést. (Amikor ilyen programot használ, a szerver bejelentkezés kilépési pontja visszautasítja azoknak a felhasználói profiloknak a bejelentkezési kísérleteit, amelyeket blokkolt, és ezek **nem** lesznek számolva a QMAXSIGN számlálóval.)
  – Az FTP szerver bejelentkezési program segítségével korlátozza a kliens számítógépeket, amelyekről az adott felhasználói profilnak megengedi az FTP szerver elérését. Például, ha a Könyvelésről engedélyezte egy

személynek az FTP hozzáférést, akkor az adott felhasználói profillal csak arról a számítógépről engedje a bejelentkezést az FTP szerverre, amelynek IP címe a Könyvelési osztályhoz tartozik.

– Az FTP szerver bejelentkezési program segítségével naplózza az összes bejelentkezési kísérletnél használt felhasználónevet és IP címet. Nézze át a naplókat rendszeresen, és akkor is, amikor a rendszer letilt egy profilt a jelszó kísérletek maximális számának túllépése miatt. Az IP cím segítségével azonosítsa az elkövetőt, és tegye meg a megfelelő intézkedést.

– A behatolás érzékelő segítségével észlelheti a ″szolgáltatás visszautasítása″ jellegű támadásokat a rendszeren.

Az FTP szerver kilépési pontok segítségével úgynevezett ″anonim″ (anonymous) FTP funkciót biztosíthat a vendég felhasználók számára. A biztonságos anonim FTP szerver beállítása kilépési programokat igényel az FTP szerverre való bejelentkezéshez **és** az FTP szerverkérések ellenőrzéséhez tartozó kilépési pontokhoz is.

Használhatja a Védett socket réteg (SSL) protokollt, amellyel biztonságossá teheti az FTP szerver kommunikációs szekciót. Az SSL biztosítja, hogy az összes FTP átvitel titkosított legyen az FTP szerver és a kliens között áthaladó összes adat titkosságának megőrzése érdekében, beleértve a felhasználó neveket és a jelszavakat is. Az FTP szerver támogatja a digitális igazolásokat a kliens hitelesítésekhez.

A fenti FTP opciókon kívül szándékában állhat az Anonymous FTP használata is, hogy kényelmes módszert nyújtson a felhasználóknak a bizalmasnak nem minősülő anyagok könnyű elérésére. Az Anonymous FTP engedélyezi a kiválasztott információk védelem nélküli elérését (nincs szükség jelszóra). A távoli hely határozza meg, hogy mely információkat teszi általánosan elérhetővé. Az ilyen információ nyilvánosan elérhetőnek, és bárki által elolvashatónak tekinthető. Mielőtt konfigurálja az Anonymous FTP-t, mérlegelnie kell a biztonsági kockázatokat, és el kell gondolkodnia azon, hogy kilépési programokkal védje az FTP szervert.

- Anonymous FTP konfigurálása.
- Hozzáférés kezelése FTP kilépési programokkal.

Az alábbi helyeken tovább tanulmányozhatja az FTP funkciót, annak kockázatait, és a rendelkezésre álló biztonsági lehetőségeket:

- Az FTP biztonság megvalósítása című témakör az IBM Systems Szoftver információs központban.
- Az Anonymous FTP témakör az IBM Systems Szoftver információs központban.
- Az FTP biztonságossá tétele SSL segítségével című témakör az IBM Systems Szoftver információs központban.

Kapcsolódó fogalmak

“E-mail biztonság” oldalszám: 20
Az Interneten vagy más nem megbízható hálózaton keresztül küldött e-mail biztonsági kockázatot jelent, amellyel szemben nem feltétlenül nyújt védelmet a tűzfal használata.

Virtuális magánhálózat (VPN)

“A réteges védelem elve a biztonságért” oldalszám: 4
A **biztonsági irányelve** meghatározza, hogy mit akar védeni, és mit vár el a rendszer felhasználóitól.

Behatolás felismerés

Kapcsolódó hivatkozás

Biztonsági szakkifejezések

Átvitelbiztonsági beállítások

A leírtak segítségével tanulmányozhatja azokat a biztonsági intézkedéseket, amelyek alkalmazásával megvédheti az adatokat, amikor azok nem megbízható hálózaton (mint például Internet) haladnak át. Ide tartozik a Védett socket réteg (SSL) protokoll, az iSeries Access Express program és a Virtuális magánhálózat (VPN) kapcsolat is.

Emlékezzen rá, hogy a JKL Toy Company forgatókönyve két elsődleges iSeries rendszerrel rendelkezik. Ebből az egyiket fejlesztésre használják, míg a másikat a termelési alkalmazásokra. Mindkét rendszer életbevágó adatokat és alkalmazásokat kezel. Következésképpen, az új iSeries rendszert a hálózat peremére tették, hogy kezelje az intranet és az Internet alkalmazásait.

A peremhálózat létrehozása garantálja, hogy bizonyos fizikai elkülönítés van a belső hálózat és az Internet között. Ez az elkülönítés csökkenti az Internetes kockázatokat, amelyek sebezhetnék a belső rendszereket. A cég a hálózati biztonság kezelésének bonyolultságát is csökkenti azzal, hogy az új iSeries szervert kizárólag Internet szervernek jelöli ki.

Mivel egy Internetes környezetben kiterjedt biztonsági igény jelentkezik, az IBM folyamatosan fejleszti biztonsági megoldásait, hogy garantálni lehessen a biztonságos hálózati környezetet a vezető e-business megoldások számára. Internetes környezetben biztosítani kell azt, hogy mind rendszerre-, mind alkalmazásra jellemző biztonságot nyújtson. Azonban, ha bizalmas információkat mozgat a cég intranet hálózatában, vagy egy Internet összeköttetésen keresztül, akkor növekszik annak szükségessége, hogy egy erősebb biztonsági megoldást valósítson meg. A kockázatok elleni küzdelem során valósítsa meg a gyakorlatban biztonsági intézkedéseit, hogy megvédje az adatok átvitelét, miközben azok az Interneten keresztül haladnak.

A nem megbízható rendszereken áthaladó információkhoz tartozó kockázatokat minimalizálhatja két, sajátos átviteli szintű iSeries funkcióval: Védett socket réteg (SSL) biztonságos kommunikáció és Virtuális magánhálózat (VPN) kapcsolatok.

Alkalmazások biztonságossá tétele SSL segítségével

A Védett socket réteg (SSL) protokoll valójában egy ipari szabvány, amely a kliensek és a szerverek közötti kommunikációt teszi biztonságossá. Az SSL protokollt eredetileg web böngésző alkalmazások számára fejlesztették ki, de egyre több egyéb alkalmazás is képes az SSL használatára. Az iSeries esetén az alábbiak tartoznak ide:

- IBM HTTP Server for iSeries (eredeti és Apache eredetű)
- FTP szerver
- Telnet szerver
- Osztott relációs adatbázis architektúra (DRDA) és osztott adatkezelés and distributed data management
- (DDM) szerver
- Kezelőközpont az iSeries navigátorban
- Címtár szolgáltatások szerver (LDAP)
- iSeries Access Express alkalmazások, beleértve az iSeries navigátort, és az olyan alkalmazásokat, amelyeket az iSeries Access Express alkalmazásprogramozási csatolókhoz (API) írtak
- Developer Kit for Java eszközzel fejlesztett programok, és IBM Toolkit for Java programot használó kliens alkalmazások
- A Védett socket réteg (SSL) programozható csatolójával (API) fejlesztett programok. Az API révén engedélyezhető az SSL használata az alkalmazásra. Olvassa el a Védett socket réteg API részt az SSL protokollt használó programok írásáról.

Számos ilyen alkalmazás támogatja a digitális igazolásokat és a kliens hitelesítéseket is. Az SSL a digitális igazolásokra támaszkodik a kommunikációs felek hitelesítésében és a biztonságos kapcsolat létrehozásában.

iSeries virtuális magánhálózatok (VPN)

Két végpont közötti biztonságos kommunikációs csatorna létrehozásához használhatja az iSeries rendszer VPN kapcsolatát. Az SSL kapcsolathoz hasonlóan, a két végpont között haladó adatok titkosíthatók, ezáltal biztosítva az adatok bizalmas voltát és sértetlenségét. A VPN kapcsolatok azonban lehetővé teszik a megadott végpontokhoz menő forgalom korlátozását, valamint a kapcsolat által használható forgalom típusának korlátozását is. Ennek következtében, a VPN kapcsolatok bizonyos hálózati szintű biztonsággal is bírnak, amellyel hozzájárulnak a hálózati erőforrások jogosulatlan hozzáféréssel szembeni védelméhez.

A módszer, amit használni kell

Mindkét biztonsági módszer garantálja a biztonságos hitelesítést, az adatok bizalmas voltát és sérthetetlenségét. Számos tényezőtől függ, hogy melyik módszert kell használni. A megfontolandó tényezők közé tartozik az, hogy kivel

folytat kommunikációt, milyen alkalmazásokat használ a velük folytatott kommunikációhoz, mennyire kell biztonságosnak lenni a kommunikációnak, továbbá milyen költséget és teljesítményt kész elfogadni a biztonságossá tétel érdekében.

Ha egy adott alkalmazást SSL protokollal kíván használni, akkor az alkalmazást be kell állítani az SSL használatához. Annak ellenére, hogy sok alkalmazás még nem tudja kihasználni az SSL előnyeit, számos más, mint a Telnet és az iSeries Access Express, rendelkeznek SSL képességgel. A VPN azonban lehetővé teszi az összes IP forgalom védelmét, amely az adott kapcsolat végpontjai között zajlik.

Például, használhatja az SSL feletti HTTP-t, amely pillanatnyilag lehetővé teszi az üzleti partnernek, hogy kommunikálni tudjon a belső hálózat egyik web szerverével. Ha csupán a web szerver az egyetlen biztonságos alkalmazás, amelyre szükség van a cég és az üzleti partner között, akkor lehet, hogy nem áll szándékában VPN kapcsolatra váltani. Azonban, ha ki akarja terjeszteni a kommunikációt, szándékában állhat a VPN kapcsolat kiépítése. Lehet olyan helyzetben is, hogy csak a hálózat egy részében kell védeni az adatokat, de nem akarja egyedileg konfigurálni a klienseket és a szervereket az SSL használatához. Ilyenkor hozzon létre egy átjáró-átjáró VPN kapcsolatot a hálózat adott részére. Ez biztonságossá teszi a forgalmat, de a kapcsolat átlátszó lesz az egyes szerverek és kliensek számára a kapcsolat bármelyik végén.

Kapcsolódó fogalmak

“A réteges védelem elve a biztonságért” oldalszám: 4
A **biztonsági irányelve** meghatározza, hogy mit akar védeni, és mit vár el a rendszer felhasználóitól.

“Forgatókönyv: JKL Toy Company e-business tervek” oldalszám: 8
A forgatókönyv egy tipikus vállalkozást, a JKL Toy Company nevű céget írja le, amely elhatározta, hogy üzleti célkitűzéseit kibővíti az Internet használattal. Annak ellenére, hogy a cég kitaláció csupán, terveik - nevezetesen az Internet használata elektronikus kereskedelem céljára - és az ennek eredményeképpen felmerülő biztonsági igények, számos valós nemzetközi vállalat helyzetét képviselik.

“Digitális igazolások használata SSL-hez”
A digitális igazolások, mint a hitelesítés eszközei, a biztonságos kommunikáció céljára szolgáló Védett socket réteg (SSL) használatának alapját jelentik.

“Virtuális magánhálózatok (VPN) a biztonságos magán kommunikáció céljára” oldalszám: 27
A Virtuális magánhálózat (VPN) felhasználásával különállóan és biztonságosan kommunikálhat saját szervezetével.

Kapcsolódó hivatkozás

Védett socket réteg API-k

Digitális igazolások használata SSL-hez

A digitális igazolások, mint a hitelesítés eszközei, a biztonságos kommunikáció céljára szolgáló Védett socket réteg (SSL) használatának alapját jelentik.

Az iSeries szerveren az i5/OS beépített kiegészítőjeként a Digitális igazolás kezelő (DCM) lehetőséget nyújt a digitális igazolások egyszerű létrehozására és kezelésére a rendszerek és a felhasználók számára.

Továbbá, egyes alkalmazások, mint például az IBM HTTP Server for iSeries konfigurálhatók a digitális igazolások használatára, ami a kliens hitelesítésnek hatékonyabb módszere, mint a felhasználónév és a jelszó.

Mi a digitális igazolás?

A digitális igazolás valójában egy digitális jogosítvány, ami megerősíti az igazolás tulajdonosának kilétét, hasonlóan mint ahogy az útlevél. Egy megbízható harmadik fél, az úgynevezett **Igazolási hatóság (CA)** adja ki a digitális igazolásokat a felhasználóknak és a szervereknek. A CA iránti bizalom az alapja annak, hogy az igazolást érvényes jogosítványnak tekintjük.

Minden egyes CA rendelkezik olyan előírással, ami alapján meghatározza, hogy milyen azonosítási információkat igényel az igazolás kiadása céljából. Egyes Internet CA-k lehet, hogy nagyon kevés információt igényelnek, mint például megkülönböztető nevet csak. Ez a személynek vagy a szervernek az a neve, amire a CA kiadja a digitális igazolás címet és a digitális e-mail címet. Minden egyes igazoláshoz generál egy magán- és egy nyilvános kulcsot. Az

| igazolás tartalmazza a nyilvános kulcsot, míg a böngésző vagy biztonságos fájl tárolja a magánkulcsot. Az igazoláshoz
| társuló kulcspárok használhatók fel az adatok - mint például a felhasználók és a szerverek között elküldött üzenetek és
| dokumentumok - ″aláírására″ és titkosítására. Az ilyen digitális aláírások garantálják az elem eredetének
| megbízhatóságát, és védik annak sértetlenségét.

| A digitális igazoláskezelő használatáról további tájékoztatást talál az IBM Systems Szoftver információs központban.

Annak ellenére, hogy sok alkalmazás még nem tudja kihasználni az SSL előnyeit, számos más, mint a Telnet és az
| iSeries Access Express, rendelkeznek SSL képességgel. Az IBM Systems Szoftver információs központ **Alkalmazások biztonságossá tétele SSL segítségével** című témakörét tanulmányozva megtudhatja, hogyan használható az SSL az iSeries alkalmazásokkal.

Kapcsolódó fogalmak

“Átvitelbiztonsági beállítások” oldalszám: 23
| A leírtak segítségével tanulmányozhatja azokat a biztonsági intézkedéseket, amelyek alkalmazásával megvédheti az
| adatokat, amikor azok nem megbízható hálózaton (mint például Internet) haladnak át. Ide tartozik a Védett socket
| réteg (SSL) protokoll, az iSeries Access Express program és a Virtuális magánhálózat (VPN) kapcsolat is.

Digitális igazolás kezelő

Alkalmazások biztonságossá tétele SSL segítségével

Kapcsolódó hivatkozás

Biztonsági szakkifejezések

Telnet hozzáférés biztonságossá tétele SSL segítségével

A Telnet szervert konfigurálhatja Védett socket réteg (SSL) használatával, hogy biztonságossá tegye a Telnet kommunikációs szekciókat.

| Ahhoz, hogy a Telnet szervert SSL használatra állítsa be, a Digitális igazolás kezelő (DCM) segítségével igazolást kell
| létrehozni a Telnet szerver számára. Alapértelmezés szerint a Telnet szerver kezeli a biztonságos és a nem biztonságos
| kapcsolatokat is. Azonban, úgy is beállíthatja a Telnet szervert, hogy az csak a biztonságos Telnet szekciókat
| engedélyezze. Továbbá, a pontosabb kliens hitelesítés érdekében konfigurálhatja úgy a Telnet szervert, hogy használja
| a digitális igazolásokat.

| Ha az SSL és Telnet használatát választja, néhány fontos biztonsági előnyt nyer vele. Telnet esetén, a szerver
| hitelesítésén túl az adatok is titkosításra kerülnek a Telnet protokoll adatfolyama előtt. Amint az SSL szekció létrejön,
| az összes Telnet protokoll, beleértve a felhasználói azonosító és a jelszó cseréjét is, titkosítva van.

A legfontosabb tényező, amit figyelembe kell venni a Telnet szerver használatakor, a kliens szekcióban használt információ érzékenysége. Ha az információ érzékeny vagy magán jellegű, akkor előnyösnek találhatja, ha az iSeries Telnet szervert SSL használattal állítja be. Amikor digitális igazolást konfigurál a Telnet alkalmazáshoz, a Telnet szerver működni tud SSL és nem SSL kliensekkel is. Ha biztonsági irányelvei megkövetelik, hogy mindig titkosítsa a Telnet szekciókat, akkor letilthatja az összes nem SSL Telnet szekciót. Ha nincs szükség SSL Telnet szerverre, kikapcsolhatja az SSL portot. A portokat az ADDTCPPORT parancs segítségével tilthatja le. Mihelyt kikapcsolta a portot, a szerver nem SSL Telnet szekciókat szolgáltat a klienseknek, és az SSL Telnet szekciókat letiltja.

| Tanulmányozhatja a Telnet szervert és biztonsági szempontjait SSL funkcióval vagy anélkül. Az IBM Systems Szoftver
| információs központ Telnet témaköre tájékoztatást nyújt a funkció iSeries szerveren való használatáról.

| **Kapcsolódó fogalmak**

| Biztonságos Telnet

| Digitális igazolás

| iSeries Access Express biztonságossá tétele SSL segítségével

| Az iSeries Access Express szervereket konfigurálhatja Védett socket réteg (SSL) használatával, hogy biztonságossá
| tegye az iSeries Access Express kommunikációs szekcióit.

Az SSL révén az iSeries Access Express szekció összes forgalma titkosítva lesz. Ez megakadályozza azt, hogy az adatokat valaki elolvassa, míg azok a helyi és a távoli gazdagépek között mozognak.

Az IBM Systems Szoftver információs központ alábbi témakörei további tájékoztatást adnak az SSL és az iSeries Access Express használatáról:

- Védett socket réteg adminisztráció
- IBM Developer Kit for Java SSL
- IBM Java Toolbox SSL

Virtuális magánhálózatok (VPN) a biztonságos magán kommunikáció céljára

A Virtuális magánhálózat (VPN) felhasználásával különállóan és biztonságosan kommunikálhat saját szervezetével.

A virtuális magánhálózat (VPN) és az általa nyújtott biztonság felhasználásában történt előrejutás alapján a JKL Toy cég számára lehetővé válik az adatok továbbítása az Interneten keresztül. Nemrég megszereztek egy másik kisebb játékgyárat, amelyet leányvállalatként kívánnak üzemeltetni. A JKL számára fontos a két cég közötti információ mozgás. Mindkét cég iSeries szervert használ, és a VPN kapcsolatot biztosíthatja a két hálózat közötti kommunikációhoz szükséges biztonságot. A VPN a hagyományos nem kapcsolt vonal használatánál is takarékosabb mód.

A VPN kapcsolatok segítségével vezérelhetővé és biztonságossá teheti az egyes kirendeltségek, a mozgó alkalmazottak, a beszállítók, az üzleti partnerek és mások közötti kapcsolatokat.

Néhány terület, ahol előnyös a VPN kapcsolat:

- Távoli és mozgó felhasználók.
- Otthon és kirendeltség vagy egyéb külső helyszín között.
- Üzlet és üzlet kommunikációk.

Biztonsági kockázat akkor jelentkezik, ha nem korlátozza a felhasználók hozzáférését az érzékeny rendszerekhez. Ha nem korlátozza, hogy kik érhetik el a rendszert, megnöveli annak az esélyét, hogy a vállalati információk nem maradnak bizalmasak. Szükség van egy tervre, amely csak azoknak ad hozzáférést a rendszerhez, akik között meg kell osztani az információt. A VPN lehetővé teszi, hogy vezérelje a hálózati forgalmat, miközben fontos biztonsági funkciókat - mint például hitelesítést és adat sérthetetlenséget - nyújt. Ha több VPN kapcsolatot létesít, azt is vezérelheti, hogy ki melyik rendszert érheti el az egyes kapcsolatokon keresztül. Például, a Könyvelés és a Humán erőforrás saját VPN kapcsolataikon át érhetők el.

Amikor megengedi, hogy a felhasználók Interneten keresztül kapcsolódjanak a rendszerhez, esetleg érzékeny vállalati adatok mehetnek át nyilvános hálózatokon, ami támadásnak teheti ki ezeket az adatokat. A küldött adatok védelmének egyik lehetséges módja a titkosítási és a hitelesítési módszerek használata, amelyek biztosíthatják az adatok magán jellegét és biztonságát a külsőkkel szemben. A VPN kapcsolatok megoldást jelentenek egy jellemző biztonsági igényre: a rendszerek közötti kommunikáció biztonságára. A VPN kapcsolatok védelmezik a kapcsolat két végpontja közötti adatfolyamot. Ezen túlmenően, használhat csomag szabályokat, amelyben meghatározhatja, mely IP csomagok haladhatnak át a VPN kapcsolaton.

VPN kapcsolattal létrehozhat biztonságos összeköttetést vezérelt és megbízható végpontok között, az ott folyó adatforgalom védelme érdekében. Azonban elővigyázatosnak kell lenni abban, hogy mennyi hozzáférést biztosít VPN partnereinek. A VPN kapcsolat titkosítani tudja az adatokat a nyilvános hálózaton való áthaladás céljából. De, konfigurálástól függően, az Interneten áthaladó adatok lehet, hogy nem haladnak át a VPN kapcsolaton. Ilyen esetekben, az adatok nem lesznek titkosítva az adott kapcsolaton keresztül kommunikáló belső hálózatokon való áthaladás idején. Következésképpen, gondosan tervezze meg, hogyan állítja be az egyes VPN kapcsolatokat. Győződjön meg arról, hogy VPN partnerei csak azokhoz a gazdagépekhez vagy erőforrásokhoz férnek hozzá a belső hálózaton, amelyekhez valóban elérést kívánt adni.

Például, lehet egy olyan szállítója, akinek arra az információra van szüksége, hogy milyen alkatrészek vannak raktáron. Ez az információ egy adatbázisban található, amelyet az intraneten lévő weblapok frissítésére használ. Szeretné megengedni ennek a partnernek, hogy közvetlenül elérje ezeket a lapokat VPN kapcsolaton keresztül. Ugyanakkor, azt nem akarja, hogy a partner elérhessen más rendszer erőforrásokat is, mint például magát az adatbázist. Sajnos a VPN kapcsolatot úgy konfigurálhatja, hogy a két végpont közötti forgalmat a 80-as portra korlátozza. A HTTP forgalom alapértelmezés szerint a 80-as portot használja. Következésképpen, a partner csak HTTP kéréseket és válaszokat tud küldeni és fogadni a kapcsolaton keresztül.

Mivel korlátozta a VPN kapcsolaton keresztül haladó forgalom típusát, maga a kapcsolat biztosítja a hálózatszintű biztonság mértékét. Azonban a VPN nem olyan módon működik, mint ahogy egy tűzfal szabályozza a rendszer bemenő és kimenő forgalmát. A VPN kapcsolat nem az egyetlen módja annak, hogy biztonságossá tegye a kommunikációt az iSeries és más rendszerek között. A biztonsági igényektől függően lehet, hogy az SSL használatát jobbnak találja.

Az, hogy a VPN kapcsolat nyújtja-e azt a biztonságot amire szüksége van, attól függ, hogy mit akar védeni. Továbbá attól is függ, hogy milyen kompromisszumokat hajlandó kötni az adott biztonság érdekében. Bármilyen döntést is hoz a biztonságról, mindig arra kell gondolni, hogyan támogatja a VPN kapcsolat saját biztonsági irányelveit.

A VPN kapcsolatok használatáról az IBM Systems Szoftver információs központ *Virtuális magánhálózatok* című témakörében olvashat.

Kapcsolódó fogalmak

“Átvitelbiztonsági beállítások” oldalszám: 23

A leírtak segítségével tanulmányozhatja azokat a biztonsági intézkedéseket, amelyek alkalmazásával megvédheti az adatokat, amikor azok nem megbízható hálózaton (mint például Internet) haladnak át. Ide tartozik a Védett socket réteg (SSL) protokoll, az iSeries Access Express program és a Virtuális magánhálózat (VPN) kapcsolat is.

Virtuális magánhálózatok (VPN)

Biztonsági szakkifejezések

Ez a témakör tartalmazza a biztonsági információk körében használt szakkifejezések meghatározását.

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

A

hitelesítés
Annak ellenőrzése, hogy a távoli kliens vagy szerver tényleg az-e, akinek mondja magát. A hitelesítés biztosítja a távoli fél iránti bizalmat.

B

C

igazolási hatóság (CA)
Digitális igazolásoknak is nevezett biztonsági meghatalmazások kibocsátásával és kezelésével foglalkozó megbízható hatóság.

rejtjel Egy másik kifejezés a titkosítás algoritmusokra.

rejtjelszöveg
Titkosított szöveg vagy adat.

cracker
Rosszindulatú, jellemzően károkozási céllal dolgozó hacker.

kriptográfia
Az adattitkosítás tudománya. A kriptográfia lehetővé teszi az információk olyan tárolását vagy átvitelét egy partnerhez, hogy a nem érintett felek ne tudják értelmezni a tárolt vagy átvitt információkat. A titkosítás az

értelmezhető szöveget értelmetlen adattá (rejtjelszöveg) alakítja. Az értelmezhetetlen adatokból az értelmes szöveget a visszafejtés állítja vissza. Mindkét folyamat egy matematikai formula vagy algoritmus és egy titkos adat (kulcs) felhasználásával dolgozik.

A kriptográfiának két fajtája van:

- **Szimmetrikus:** A kommunikáló feleknek közös titkos kulcsuk van, és ezt használják fel a titkosításhoz és a visszafejtéshez is. Osztott kulcsú kriptográfiának is nevezik.
- **Aszimmetrikus:** A kommunikáló felek mindegyike két kulccsal rendelkezik, egy nyilvános kulccsal és egy magánkulccsal. Bár a két kulcs matematikai viszonyban van egymással, a nyilvános kulcs alapján a magánkulcs kiszámítása gyakorlatilag lehetetlen. A kulcsok kialakítása olyan, hogy egy bizonyos nyilvános kulccsal titkosított üzenet csakis és kizárólag a társított magánkulcs segítségével fejthető vissza. A másik felhasználási terület, amikor egy szerver vagy felhasználó a magánkulcs segítségével ″aláír″ egy dokumentumot, amely esetben a megfelelő nyilvános kulccsal lehet visszafejteni a digitális aláírást. Ha az aláírásnak a nyilvános kulcs melletti visszafejtésével kapott kivonat megegyezik a dokumentum valós időben előállított kivonatával, akkor az aláírás érvényesnek, a dokumentum forrása pedig ellenőrzöttnek minősül. Nyilvános kulcsú kriptográfiának is nevezik.

D

bizalmasság
Elrejti az üzenetek tartalmát, általában valamilyen titkosítás használatával.

integritás
Biztosítja, hogy az adatcsomagok tartalma ne változhasson meg az átvitel közben véletlen hibák vagy szándékos cselekmények hatására.

eredet hitelesítés
Ellenőrzi, hogy az adatcsomagok valóban attól származnak-e, aki ezt állítja magáról.

szolgáltatás megbénítási támadás
Más néven DoS támadás. A hálózat elárasztása IP csomagokkal, melynek hatására egy szolgáltatás, például egy webszerver elérhetetlen vagy használhatatlan lesz.

digitális igazolás
Olyan digitális dokumentum, amely az útlevélhez hasonlóan igazolja az igazolás tulajdonosának (személy)azonosságát. A digitális igazolásokat egy igazolási hatóságnak nevezett megbízható szervezet adja ki a felhasználók és szerverek számára. Az igazolás mint érvényes azonosító irányi bizalom alapja az igazolási hatóság irányi bizalom. Az igazolások a következőkre használhatók:

- Azonosítás - azonosítja a tulajdonost
- Hitelesítés - biztosítja, hogy a tulajdonos az, akinek mondja magát
- Integritás - biztosítja a dokumentumok tartalmának változatlanságát
- Letagadhatatlanság - bizonyítja az elvégzett műveletek végrehajtását. Például a felhasználó nem vitathatja az igazolás felhasználásával végzett elektronikus tranzakciókat.

digitális aláírás
Megegyezik az írott dokumentumokon lévő személyes aláírásokkal. A digitális aláírás bizonyíthatóan azonosítja a dokumentum eredetét. Az igazolás tulajdonosa az igazoláshoz tartozó magánkulccsal ″aláírja″ a dokumentumot. A dokumentum fogadója a megfelelő nyilvános kulccsal visszafejti az aláírást, így ellenőrizve a küldőt.

Digitális igazolás kezelő (DCM)
Lehetővé teszi az iSeries szerver helyi igazolási hatóságként működését. A DCM segítségével szerver- és felhasználói digitális igazolások hozhatók létre. Emellett importálhat más igazolási hatóságok által kiállított igazolásokat is. A digitális igazolások társíthatók egy i5/OS felhasználói profilhoz. A DCM segítségével állíthatók be az alkalmazások a Védett socket réteg (SSL) kommunikáció használatára is.

megkülönböztetett név
A személy vagy szerver neve, akinek az igazolási hatóság a digitális igazolást kiadja. Az igazolás ezzel a

névvel jelzi az igazolás tulajdonjogát. Az igazolási hatóság által az igazolások kibocsátásakor követett eljárástól függően a megkülönböztetett név további hitelesítési információkat is tartalmazhat.

tartománynév rendszer (DNS)
Az egyéni digitális igazolások birtokosainak azonosítására szolgáló adatkészlet. Az 1-es osztályú digitális igazolásokon belül ezek az információk egyebek között a nevet, e-mail címet és a digitális igazolás kibocsátóját (például VeriSign) tartalmazhatják.

Az Internet csatlakozás során a csatlakozáshoz használt kliens egy DNS szerver segítségével határozza meg a hosztrendszer IP címét, amellyel kommunikálni kíván.

E

titkosítás
Az adatokat olyanra alakítja, hogy a megfelelő visszafejtési módszer és kulcs hiányában ezek mindenki számára olvashatatlanok legyenek. A jogosulatlan felek még ilyenkor is elfoghatják az információkat. A megfelelő visszafejtési módszer és kulcs nélkül azonban az információk használhatatlanok.

Vállalati azonosság leképezés (EIM)
Az EIM az egyéneknek vagy egyedeknek a vállalaton belüli különböző nyilvántartások megfelelő felhasználói azonosságaira képezésére (társítására) szolgáló mechanizmus. Az EIM által biztosított alkalmazás programozási felületek (API) segítségével a leképezési viszonyok létrehozása, kezelése és lekérdezése is lehetséges.

extranet
Több, egymással együttműködő szervezet vállalati tűzfalakon kívüli magán üzleti hálózata. Az extranet szolgáltatások a meglévő Internet infrastruktúrát használják, beleértve a szabványos szervereket, e-mail klienseket és web böngészőket. Ennek eredményeként az extranet használata gazdaságosabb, mint egy saját hálózat kiépítése és fenntartása. Az extranetek az Internet lehetőségeinek kibővítésével lehetővé teszik a közös érdekeltségű kereskedelmi partnereknek, szállítóknak és vásárlóknak a szoros üzleti kapcsolatok fenntartását és a kommunikáció biztonságát.

F

tűzfal A belső hálózat és a külső hálózat közötti logikai korlát. A tűzfal hardver- és szoftverrendszerekből áll. Felügyeli a védett és megbízható rendszerek illetve a nem biztonságos és nem megbízható rendszerek közötti hozzáférést és információáramlást.

G

H

hacker Hálózatbiztonsági értelemben a rendszerbe jogosulatlanul, de nem kifejezett rosszindulatú szándékkal bejutni szándékozó személy.

hiperszöveg hivatkozások
Az online információmegjelenítés egy módja, ahol az információk bizonyos darabjait (hiperszöveg csomópontok) kapcsolatok (hiperszöveg hivatkozások) kötik össze.

Hiperszöveg leírónyelv (HTML)
A hiperszöveges dokumentumok meghatározására szolgáló nyelv. A HTML segítségével határozható meg a dokumentumok megjelenése (például stílusa és betűkészlete), illetve hogy hogyan kapcsolódik más dokumentumokhoz vagy objektumokhoz.

Hiperszöveg átviteli protokoll (HTTP)
A hiperszöveges dokumentumok elérésére szolgáló szabványos módszer.

I

Internet
Az egymáshoz kapcsolt ″hálózatok hálózata″. Emellett egy olyan alkalmazáskészlet, amely lehetővé teszi a ″hálózatok hálózatához″ csatlakozó számítógépeknek az egymással folytatott kommunikációt. Az Internet egyebek között információk böngészését, fájlátvitelt, távoli bejelentkezést, elektronikus levelezést és hírszolgáltatást biztosít. Gyakran hívják ″Net″-nek is.

Internet kliens
Internetet használó program (vagy felhasználó), amely kéréseket ad ki egy Internetes szerver programnak, és fogadja annak válaszait. A különféle kliensprogramok különböző Internet szolgáltatásokhoz biztosítanak hozzáférést. Ilyen kliensprogram például a web böngésző. Egy másik a fájlátviteli protokoll (FTP).

Internetes hoszt
Az Internethez vagy egy intranethez csatlakozó számítógép. Az Internet hosztok egynél több Internetes szerver programot is futtathatnak. Egy Internet hoszt futtathat például FTP szervert, amely válaszol az FTP kliens alkalmazások által kiadott kérésekre. Ugyanaz a hoszt futtathat egy HTTP szervert is, amely a kliensek web böngészői által küldött kérésekre válaszol. A szerver programok általában a hoszt rendszer háttérfeladataként futnak.

Internet kulcscsere (IKE) protokoll
A virtuális magánhálózatokkal kapcsolatosan lehetővé teszi a biztonsági megegyezések automatikus egyeztetését, valamint a kriptográfiai kulcsok automatikus előállítását és frissítését.

Internetes név
Az IP címek álneve. Az IP címek hosszú számformátuma (például 10.5.100.75) nehezen jegyezhető meg. Az IP címhez internetes név, például system1.vnet.ibm.com rendelhető. Az internetes neveket teljes képzésű tartománynévnek is nevezik. A hirdetésekben és hasonló helyeken (″Látogasson el honlapunkra″) általában az internetes nevet használják az IP cím helyett, mivel az internetes nevet könnyebben meg lehet jegyezni. A teljes képzésű tartománynevek több részből állnak. A system1.vnet.ibm.com például a következő részekből áll:

com: Minden kereskedelmi célú hálózat. A tartománynévnek ezt a részét az internetes hatóságok (külső szervezetek) osztják ki. A különböző hálózatokhoz különböző nevek tartoznak, például *com* a kereskedelemhez és *edu* az oktatási intézményekhez.

ibm: A szervezet azonosítója. A tartománynévnek ezt a részét szintén az internetes hatóság osztja ki, és ez egyedi. Csak egy szervezet azonosítója lehet ibm.com.

vnet: Egy rendszercsoport az ibm.com-on belül. Ezt az azonosítót a szervezet hozza létre magának. Az ibm.com adminisztrátora tetszőleges számú csoportot hozhat létre.

system1:
Az egyik internetes hoszt neve a vnet.ibm.com csoporton belül.

Internet szerver
Olyan program (vagy programkészlet), amely az Interneten keresztül fogadja a megfelelő kliensprogramok által küldött kéréseket, és válaszol ezekre. A Internet szerver olyan helyként képzelhető el, amelyet az Internet kliensek látogatnak. A különböző szerver programok különböző szolgáltatásokat biztosíthatnak, például:

- Böngészés. Egy ″honlap″, amely más dokumentumokra és objektumokra tartalmaz hivatkozásokat.
- Fájlátvitel. E kliens kérheti a szerveren tárolt fájlok átvitelét a kliensre. Ilyen fájlok lehetnek például szoftverfrissítések, termékleírások vagy dokumentumok.
- Elektronikus kereskedelem, például információk kérése vagy termékek megrendelése.

Internet szolgáltató (ISP)
Olyan szervezet, amely Internet kapcsolatot biztosít az előfizetői számára. Hasonló a telefontársaságokhoz, akik az előfizetőiknek a telefonhálózathoz biztosítanak hozzáférést.

intranet
Egy szervezet belső hálózata, amely az Internet eszközeit használja fel.

behatolásfelismerés
Általános kifejezés többféle nemkívánatos tevékenység felismerésére. A behatolások célja többféle lehet, általában olyan információk megszerzésére irányul, amelyekre valaki nem jogosult (információrablás). Emellett a behatolás célja lehet károkozás egy hálózat, rendszer vagy alkalmazás használhatatlanná tételével (szolgáltatás megbénítása), illetve jogosulatlan hozzáférés egy rendszerhez további behatolások céljából. A legtöbb behatolás az információgyűjtés, hozzáférési kísérlet majd támadások mintáját követi. A célrendszer bizonyos támadásokat felismerhet, és semlegesíthet. Egyes támadásokat azonban a célrendszer nem feltétlenül tud hatékonyan semlegesíteni. A támadások nagy része ″hamisított″ csomagokkal is operál, amelyek eredete

csak nehezen határozható meg. Emellett számos támadásban érintettek olyan jogosulatlanul használt, ártatlan gépek vagy hálózatok, amelyek a támadó azonosságának elrejtésére szolgálnak. Mindeme okok miatt az információgyűjtés, a hozzáférési kísérletek és támadások felismerése a behatolásfelismerés alapvető fontosságú része.

IP cím A TCP/IP hálózatok (például az Internet) elemeinek egyedi azonosítója. Az Internet szerverek általában hozzárendelt, egyedi IP címet használnak. Az Internet kliensek gyakran ideiglenes, de egyedi IP címet használnak, amit az Internet szolgáltató oszt ki számukra.

IP adatcsomag
TCP/IP hálózaton küldött információs egység. Az IP adatcsomagok (más néven IP csomagok) adatokból és fejléc információkból állnak. Ez utóbbi adja meg például a csomag forrását és célját.

IP szűrők
A megadott szabályok alapján végzett csomagszűréssel meghatározza, hogy milyen csomagok léphetnek be a hálózatba, illetve milyen csomagok hagyhatják el azt. Ez megvédi a biztonságos hálózatot a különféle rosszindulatú technikákat (például portszkennelés vagy IP cím hamisítás) alkalmazó külső felhasználóktól. A szűrési szolgáltatást úgy kell tekinteni, mint a további eszközök létrehozására szolgáló alapot. Ez biztosítja az infrastruktúrát a különféle védelmi eszközök működése számára, amelyek a legtöbb cracker ellen megfelelő védelmet biztosítanak.

IP biztonsági (IPSec) protokoll
Olyan protokollkészlet, amely a csomagok hálózati réteg szintű biztonságos továbbítását teszi lehetővé. Az IPSec egy szabványkészlet, amelyet az i5/OS és más rendszerek virtuális magánhálózatok kialakítására használnak.

IP cím hamisítás
Olyan hozzáférési kísérlet egy rendszerhez, amelyben a támadó egy a rendszer által megbízhatónak tekintett másik rendszerként állítja be magát. A támadó ezt úgy oldja meg, hogy beállít egy rendszert egy megbízhatónak tekintett IP címre. Az útválasztók gyártói számos védelmi módszert dolgoztak ki az IP cím hamisítás felismerésére és visszautasítására.

J

K

L

M

N

hálózati cím fordítás (NAT)
A proxy és SOCKS szervereknél átlátszóbb alternatíva a hálózat védelmére. Emellett a hálózati konfigurációt is leegyszerűsíti, mivel lehetővé teszi az egymással nem kompatíbilis címzési sémával rendelkező hálózatok összekapcsolását. A NAT alapvetően két funkciót biztosít. Védelmet nyújt azáltal, hogy a szerverek ″valódi″ címét olyan címek mögé rejti, amelyek elérhetővé tehetők a nyilvánosság számára is. Ez megvédi például az olyan nyilvános webszervereket, amelyek a belső hálózaton találhatók. A NAT emellett lehetőséget nyújt a belső felhasználóknak az Internet elérésére úgy, hogy közben a belső IP címek láthatatlanok maradnak a külvilág számára. A belső felhasználók Internet hozzáférésének engedélyezésekor a NAT a védelmet a belső címek elrejtésével biztosítja.

letagadhatatlanság
Lehetőséget nyújt bizonyos tranzakciók megtörténtének bizonyítására. A digitális igazolások és a nyilvános kulcsú kriptográfia lehetővé teszi az ezt támogató tranzakciók, üzenetek és dokumentumok ″aláírását″.

O

P

csomag
TCP/IP hálózaton küldött információs egység. A csomagok (más néven adatcsomagok) adatokból és fejléc információkból állnak. Ez utóbbi adja meg például a csomag forrását és célját, továbbá a protokollra vonatkozó információkat.

proxy szerver
Olyan TCP/IP alkalmazás, amely újraküldi a védett belső hálózaton található kliensek és a megbízhatatlan hálózat szerverei közötti kéréseket és válaszokat. A proxy szerver megszakítja a TCP/IP kapcsolatot a külső hálózati szerverek és a belső hálózati kliensek között, így a belső hálózati információk nem válnak nyilvánossá. A hálózaton kívüli hosztok a proxy szervert fogják a kommunikáció forrásának tartani, így a belső hálózati és külső hálózati hosztok között nem lesz közvetlen csatlakozás.

nyilvános kulcs infrastruktúra (PKI)
Digitális igazolások igazolási hatóságok és más regisztrációs hatóságok, amelyek az Internet tranzakciókban részes felek azonosságát hitelesítik.

Q

R

újraküldés elleni védelem
Biztosítja, hogy az elfogott adatcsomagok ne legyenek újraküldhetők későbbi időpontban.

S

Védett socket réteg (SSL)
A Netscape által létrehozott ipari szabvány a kliensek és szerverek közötti szekciók titkosítására. Az SSL szimmetrikus kulcsú titkosítást alkalmaz a szerver és kliens (felhasználó) között. A kliens és szerver a szekciókulcsot a digitális igazolások cseréjekor egyezteti. Minden kliens és szerver SSL szekció más-más kulcsot alkalmaz. Ennek következtében ha a jogosulatlan felhasználók el is fognak egy szekciókulcsot (ami már önmagában valószínűtlen), azt nem fogják tudni felhasználni más SSL szekciók visszafejtéséhez.

egyszeri bejelentkezés (SSO)
Olyan hitelesítési forma, amely lehetővé teszi, hogy egy felhasználó egyszer hitelesítse magát, és utána több rendszerhez vagy alkalmazáshoz is hozzáférjen. Lásd: Vállalati azonosság leképezés.

lehallgatás (sniffelés)
Elektronikus átvitelek megfigyelése és megcsapolása. Az Interneten keresztülhaladó információk több útválasztón is áthaladhatnak a céljuk felé. Az útválasztók gyártói, az Internet szolgáltatók és az operációs rendszerek fejlesztői mindent megtesznek azért, hogy az Internetes gerinchálózatokon a lehallgatás ne legyen lehetséges. A sikeres lehallgatások gyakorisága egyre csökken. Ezek többsége is leginkább az Internethez csatlakozó belső hálózatokon történik, nem magán az Internet gerinchálózaton. Ennek ellenére a lehallgatási lehetőségre figyelemmel kell lenni, mivel a TCP/IP átvitelek gyakran nem titkosítottak.

SOCKS
Olyan kliens/szerver architektúra, amely a TCP/IP forgalmat egy biztonságos átjárón keresztül szállítja. A SOCKS szerver általában a proxy szerverek szolgáltatásait biztosítja.

címhamisítás
Olyan támadás, amelynek során a támadó egy rendszer megpróbál megbízható rendszerként beállítani.

T

TCP/IP
Az Internet elsődleges kommunikációs protokollja. A TCP/IP jelentése Átvitelvezérlési protokoll/Internet Protokoll. A TCP/IP belső hálózatokon is alkalmazható.

trójai Hasznos és ártatlan funkcióval rendelkezőnek kinéző számítógépes program, parancs vagy parancsfájl. Ennek ellenére tartalmaz olyan rejtett funkciókat, amely külső felek számára is kihasználhatóvá teszi a programot futtató felhasználóhoz jogszerűen tartozó jogosultságokat. Lemásolhatja például a belső hitelesítési információkat, és visszaküldheti ezeket a trójai program szerzőjének.

U

V

virtuális magánhálózat (VPN)
A vállalati intranet kiterjesztése. Segítségével saját ″alagutak″ létrehozásával biztonságos kapcsolatok alakíthatók ki nyilvános hálózatokon, például az Interneten keresztül. A virtuális magánhálózatok az információk biztonságos Internetes továbbításával lehetővé teszik a felhasználók csatlakozását a helyi rendszerre. Ilyen felhasználók például a következők:

- Távoli felhasználók
- Telephelyek
- Üzleti partnerek és szállítók

W

web böngésző
A HTTP protokoll kliensalkalmazása. A web böngészők a HTML forrásnyelv elemzésével hiperszöveges dokumentumokat jelenítenek meg a felhasználóknak. A felhasználó a hivatkozott objektumokat az aktuális dokumentum egy adott területének kiválasztásával (kattintással) érheti el. Az ilyen területeket néha **aktív pontnak** is nevezik. Web böngésző például a Netscape Navigator és a Mozilla.

World Wide Web (WWW)
Egymáshoz csatlakozással rendelkező szerverek és kliensek hálója, amely közös szabványos formátumot használ a dokumentumok létrehozására (HTML) és elérésére (HTTP). A szerverről szerverre és dokumentumról dokumentumra vezető hivatkozások szövevényes hálózatát gyakran egyszerűen csak úgy hívják: **a web**.

X

Y

Z

Nyilatkozatok

Ezek az információk az Egyesült Államokban forgalmazott termékekre és szolgáltatásokra vonatkoznak.

Az IBM lehet, hogy nem ajánlja az ebben a dokumentációban tárgyalt termékeket, szolgáltatásokat vagy kiegészítőket más országokban. Kérjen tanácsot a helyi IBM képviselettől az adott területen pillanatnyilag rendelkezésre álló termékekről és szolgáltatásokról. Bármely hivatkozás IBM termékre, programra vagy szolgáltatásra nem szándékozik azt állítani vagy sugallni, hogy csak az az IBM termék, program vagy szolgáltatás alkalmazható. Bármely funkcionálisan azonos termék, program vagy szolgáltatás, amely nem sérti az IBM érvényes szellemi tulajdonával kapcsolatos jogokat, használható helyette. Bármely nem IBM termék, program vagy szolgáltatás működésének kiértékelése és ellenőrzése azonban a felhasználó felelőssége.

Az IBM-nek lehetnek szabadalmai, vagy szabadalmi intézés alatt álló alkalmazásai, amelyek fedik az ebben a dokumentumban leírt témákat. Ennek a dokumentumnak az átadása azonban nem jelenti ezen szabadalmak licencjogának átadását is. Licencjog iránti kéréseit írásban az alábbi címre küldje:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

Ha duplabyte-os (DBCS) információkkal kapcsolatban van szüksége licencre, akkor lépjen kapcsolatba saját országában az IBM szellemi tulajdon osztályával, vagy írjon a következő címre:

IBM World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106-0032, Japan

A következő bekezdés nem vonatkozik az Egyesült Királyságra, valamint azokra az országokra, amelyeknek jogi szabályozása ellentétes a bekezdés tartalmával: AZ INTERNATIONAL BUSINESS MACHINES CORPORATION JELEN KIADVÁNYT “ÖNMAGÁBAN”, BÁRMIFÉLE KIFEJEZETT VAGY VÉLELMEZETT GARANCIA NÉLKÜL ADJA KÖZRE, IDEÉRTVE, DE NEM KIZÁRÓLAG A JOGSÉRTÉS KIZÁRÁSÁRA, A KERESKEDELMI ÉRTÉKESÍTHETŐSÉGRE ÉS BIZONYOS CÉLRA VALÓ ALKALMASSÁGRA VONATKOZÓ VÉLELMEZETT GARANCIÁT. Bizonyos államok nem engedélyezik egyes tranzakciók kifejezett vagy vélelmezett garanciáinak kizárását, így elképzelhető, hogy az előző bekezdés Önre nem vonatkozik.

Jelen dokumentum tartalmazhat technikai, illetve szerkesztési hibákat. Az itt található információk bizonyos időnként módosításra kerülnek; a módosításokat a kiadvány új kiadásai tartalmazzák. Az IBM mindennemű értesítés nélkül fejlesztheti és/vagy módosíthatja a kiadványban tárgyalt termékeket és/vagy programokat.

A könyvben a nem IBM webhelyekre történő hivatkozások csupán kényelmi célokat szolgálnak, és semmilyen módon sem kívánják azt a látszatot kelteni, hogy az IBM jóváhagyná ezeket a webhelyeket. Az ilyen webhelyeken található anyagok nem képezik az adott IBM termék dokumentációjának részét, így ezek használata csak saját felelősségre történhet.

Az IBM legjobb belátása szerint bármilyen formában felhasználhatja és továbbadhatja a felhasználóktól származó információkat anélkül, hogy a felhasználó felé ebből bármilyen kötelezettsége származna.

A programlicenc azon birtokosainak, akik információkat kívánnak szerezni a programról (i) a függetlenül létrehozott programok vagy más programok (beleértve ezt a programot is) közti információcseréhez, illetve (ii) a kicserélt információk kölcsönös használatához, fel kell venniük a kapcsolatot az alábbi címmel:

| IBM Corporation

Software Interoperability Coordinator, Department YBWA
3605 Highway 52 N
Rochester, MN 55901
U.S.A.

Az ilyen információk bizonyos feltételek és kikötések mellett állnak rendelkezésre, ideértve azokat az eseteket is, amikor ez díjfizetéssel jár.

A dokumentumban tárgyalt licencprogramokat és a hozzájuk tartozó licenc anyagokat az IBM az IBM Vásárlói megállapodás, az IBM Nemzetközi programlicenc szerződés, az IBM Gépi kódra vonatkozó licencszerződés vagy a felek azonos tartalmú megállapodása alapján biztosítja.

A dokumentumban található teljesítményadatok ellenőrzött környezetben kerültek meghatározásra. Ennek következtében a más működési körülmények között kapott adatok jelentősen különbözhetnek a dokumentumban megadottaktól. Egyes mérések fejlesztői szintű rendszereken kerültek végrehajtásra, így nincs garancia arra, hogy ezek a mérések azonosak az általánosan hozzáférhető rendszerek esetében is. Továbbá bizonyos mérések következtetés útján kerültek becslésre. A tényleges értékek eltérhetnek. A dokumentum felhasználóinak ellenőrizni kell az adatok alkalmazhatóságát az adott környezetben.

A nem IBM termékekre vonatkozó információkat az IBM a termékek szállítóitól, az általuk közzétett bejelentésekből, illetve egyéb nyilvánosan elérhető forrásokból szerezte be. Az IBM nem vizsgálta ezeket a termékeket, és nem tudja megerősíteni a nem IBM termékekre vonatkozó teljesítményadatok pontosságát, a kompatibilitást és egyéb követelményeket. A nem IBM termékekkel kapcsolatos kérdéseivel forduljon az adott termék szállítóihoz.

Az IBM jövőbeli tevékenységére vagy szándékaira vonatkozó állításokat az IBM mindennemű értesítés nélkül módosíthatja, azok csak célokat jelentenek.

Az IBM által ajánlott kereskedelmi árként megjelenő összes IBM ár csak az adott pillanatra érvényes, értesítés nélkül változhat. A forgalmazói árak ettől eltérők lehetnek.

Az itt leírt információk csak tervezési célokat szolgálnak. Így az itt található információk módosulhatnak, mielőtt a leírt termékek beszerezhetők lennének.

Az információk között példaként napi üzleti tevékenységekhez kapcsolódó jelentések és adatok lehetnek. A valóságot a lehető legjobban megközelítő illusztráláshoz a példákban egyének, vállalatok, márkák és termékek nevei szerepelnek. Minden ilyen név a képzelet szüleménye, és valódi üzleti vállalkozások neveivel és címeivel való bármilyen hasonlóságuk teljes egészében a véletlen műve.

Szerzői jogi licenc:

Jelen dokumentáció forrásnyelvű példa alkalmazásokat tartalmazhat, amelyek a programozási technikák bemutatására szolgálnak a különböző működési környezetekben. A példaprogramokat tetszőleges formában, az IBM-nek való díjfizetés nélkül másolhatja, módosíthatja és terjesztheti fejlesztési, használati, marketing célból, illetve olyan alkalmazási programok terjesztése céljából, amelyek megfelelnek azon operációs rendszer alkalmazásprogram illesztőjének, ahol a példaprogramot írta. Ezek a példák nem kerültek minden állapotban tesztelésre. Az IBM így nem tudja garantálni a megbízhatóságukat, szervizelhetőségüket, de még a programok funkcióit sem.

A példaprogramok minden példányának, illetve a belőlük készített összes származtatott munkának tartalmaznia kell az alábbi szerzői jogi nyilatkozatot:

© (cégnév) (évszám). A kód bizonyos részei az IBM Corp. példaprogramjaiból származnak. © Copyright IBM Corp. (évszám vagy évszámok). Minden jog fenntartva.

Ha az információkat elektronikus formában tekinti meg, akkor elképzelhető, hogy a fotók és színes ábrák nem jelennek meg.

Védjegyek

A következő kifejezések az International Business Machines Corporation védjegyei az Egyesült Államokban és/vagy más országokban:

| AIX
| AIX 5L
| e(logó)server
| eServer
| i5/OS
| IBM
| iSeries
| pSeries
| xSeries
| zSeries

| Az Intel, az Intel Inside (logók), az MMX és a Pentium az Intel Corporation védjegyei az Egyesült Államokban és/vagy
| más országokban.

A Microsoft, a Windows, a Windows NT és a Windows embléma a Microsoft Corporation védjegye az Egyesült Államokban és/vagy más országokban.

A Java, valamint minden Java alapú védjegy a Sun Microsystems, Inc. védjegye az Egyesült Államokban és/vagy más országokban.

| A Linux a Linus Torvalds védjegye az Egyesült Államokban és/vagy más országokban.

A UNIX az Open Group bejegyzett védjegye az Egyesült Államokban és más országokban.

Egyéb cég-, termék- és szolgáltatásnevek mások áru-, vagy szolgáltatási védjegyei lehetnek.

Feltételek

A kiadványok használata az alábbi feltételek és kikötések alapján lehetséges.

Személyes használat: A kiadványok másolhatók személyes, nem kereskedelmi célú használatra, de valamennyi tulajdonosi feljegyzést meg kell tartani. Az IBM kifejezett engedélye nélkül nem szabad a kiadványokat vagy azok részeit terjeszteni, megjeleníteni, illetve belőlük származó munkát készíteni.

Kereskedelmi használat: A kiadványok másolhatók, terjeszthetők és megjeleníthetők, de kizárólag a vállalaton belül, és csak az összes tulajdonosi feljegyzés megtartásával. Az IBM kifejezett hozzájárulása nélkül nem készíthetők olyan munkák, amelyek a kiadványokból származnak, továbbá nem másolhatók, nem terjeszthetők és nem jeleníthetők meg, még részben sem, a vállalaton kívül.

A jelen engedélyben foglalt, kifejezetten megadott hozzájáruláson túlmenően a kiadványokra, illetve a bennük található információkra, adatokra, szoftverekre vagy egyéb szellemi tulajdonra semmilyen más kifejezett vagy vélelmezett engedély nem vonatkozik.

Az IBM fenntartja magának a jogot, hogy jelen engedélyeket saját belátása szerint bármikor visszavonja, ha úgy ítéli meg, hogy a kiadványokat az IBM érdekeit sértő módon használják fel, vagy a fenti útmutatásokat nem megfelelően követik.

Jelen információk kizárólag valamennyi vonatkozó törvény és előírás betartásával tölthetők le, exportálhatók és reexportálhatók, beleértve az Egyesült Államok exportra vonatkozó törvényeit és előírásait is.

AZ IBM A KIADVÁNYOK TARTALMÁRA VONATKOZÓAN SEMMIFÉLE GARANCIÁT NEM NYÚJT. A KIADVÁNYOK ″ÖNMAGUKBAN″, BÁRMIFÉLE KIFEJEZETT VAGY VÉLELMEZETT GARANCIA VÁLLALÁSA NÉLKÜL KERÜLNEK KÖZREADÁSRA, IDEÉRTVE, DE NEM KIZÁRÓLAG A KERESKEDELMI ÉRTÉKESÍTHETŐSÉGRE, A SZABÁLYOSSÁGRA ÉS AZ ADOTT CÉLRA VALÓ ALKALMASSÁGRA VONATKOZÓ VÉLELMEZETT GARANCIÁKAT IS.

Nyomtatva Dániában