System i

Biztonság
System i és Internet biztonság

Version 6 Release 1

System i

Biztonság
System i és Internet biztonság

Version 6 Release 1

Megjegyzés

Jelen leírás és a tárgyalt termék használatba vétele előtt feltétlenül olvassa el a “Nyilatkozatok”, oldalszám: 27 részben leírtakat.

Ez a kiadás az IBM i5/OS (termékszám: 5761-SS1) V6R1M0 változatára, és minden ezt követő kiadásra és módosításra vonatkozik mindaddig, amíg az újabb kiadások ezt másként nem jelzik. Ez a változat nem fut minden csökkentett utasításkészletű (RISC) rendszeren illetve a CISC modelleken.

Tartalom

System i és Internet biztonság

Az Internet elérése a helyi hálózatról (LAN) szükségessé teszi a biztonsági követelmények újragondolását.

Az IBM System i termék szoftver megoldásai és biztonsági architektúrája lehetővé teszi, hogy erős védelmet építsen a potenciális internetes biztonsági csapdák és behatolók ellen. Ezeknek a biztonsági ajánlásoknak a használata biztosítja, hogy az ügyfelei, alkalmazottai és üzleti partnerei biztonságos környezetben kérdezhessék le a számukra szükséges információkat.

Ez a témakörgyűjtemény elmagyarázza a jól ismert biztonsági fenyegetéseket, és hogy azok hogyan viszonyulnak az internetes és e-business céljaihoz. A gyűjtemény arról is szól, hogy hogyan mérheti fel a kockázatokat, összevetve őket a különféle biztonsági beállítások használatából eredő előnyökkel, amelyet a rendszer nyújt az ilyen kockázatok kezelésére. Meghatározhatja azt is, hogyan lehet felhasználni ezeket az információkat a hálózatbiztonsági terv elkészítéséhez, amely eleget tesz az üzleti igényeknek.

System i és Internet biztonság, PDF fájl

Ezeket az információkat egy PDF fájlként is megjelenítheti és kinyomtathatja.

A dokumentum PDF változatának megjelenítéséhez vagy letöltéséhez válassza a System i és Internet biztonság kiadványt (kb. 456 KB).

Az alábbi kapcsolódó témaköröket is megtekintheti vagy letöltheti:

- Behatolás észlelés (kb 285 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. 1954 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.
- Egyszeri bejelentkezés (kb 1203 KB). Az egyszeri bejelentkezés megoldással a felhasználónak kevesebb alkalommal kell bejelentkezést végrehajtani, valamint kevesebb jelszót kell használni az alkalmazások és a rendszerek eléréséhez.
- A rendszer biztonságának tervezése és beállítása (kb. 3992 KB). A rendszer biztonságának tervezése és beállítása arról szól, hogyan kell hatékonyan és szisztematikusan megtervezni és beállítani a rendszerszintű biztonságot.

PDF fájlok mentése

A PDF fájl munkaállomáson történő mentése megjelenítés vagy nyomtatás céljából:

1. Kattintson a jobb egérgombbal a böngészőben a PDF 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 fájlok megtekintéséhez vagy nyomtatásához telepített Adobe Reader szükséges. Letöltheti egy ingyenes példányát az Adobe honlapról (www.adobe.com/products/acrobat/readstep.html)  .

Kapcsolódó fogalmak

Behatolás felismerés

Vállalati azonosság leképezés (EIM)

Egyszeri bejelentkezés

A rendszerbiztonság tervezése és beállítása

System i és Internet biztonság megfontolások

Az Internethez kapcsolódó biztonsági kérdések igen jelentősek. Ez a fejezet bemutatja a i5/OS biztonsági erősségeit és ajánlatait.

Amikor a System i platformot az Internethez csatlakoztatja, akkor általában az első kérdés a következő: ″Mit kell tudnom a biztonságról és az Internetről?″ Ez a fejezet segít megválaszolni ezt a kérdést.

A tudnivalók függnek attól, hogyan akarja használni az Internetet. 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.

Megjegyzés: Ha számára ismeretlenek a biztonsággal és az Internettel kapcsolatos kifejezések, nézze át a Biztonsági szakkifejezések című részt, amikor ezt a könyvet használja.

Miután megértette, 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 befolyásolja 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 i5/OS biztonsági jellemzői

A számos egyedi biztonsági ajánlaton (amelyek az Internethez csatlakozó rendszer védelmére hivatottak) túlmenően az i5/OS operációs rendszer a következő biztonsági jellemzőkkel rendelkezik:

- 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 i5/OS operációs rendszeren egy fájl nem keltheti azt a látszatot, mintha program lenne, és egy adott program sem tud megváltoztatni egy másik programot. Az i5/OS 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. A Biztonságtervező segítségével meghatározhatja, hogy mely biztonsági javaslatok illeszkednek biztonsági igényeihez.

Az i5/OS fejlett biztonsági ajánlatai

Az i5/OS operációs rendszernek van néhány különleges biztonsági ajánlata, amelyeket kiválasztva fokozhatja rendszerének biztonságát, amikor az Internethez csatlakozik. Az Internet használat módjától függően, szándékában állhat az alábbi ajánlatokból egy vagy több ajánlat előnyét kihasználni:

- Virtuális magánhálózat (VPN), amely a vállalati magán intranet hálózat kiterjesztése 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 operációs rendszer beépített szolgáltatása, amely az System i Navigator felületén érhető el.

- A csomagszabály az i5/OS operációs rendszer beépített szolgáltatása, amely az System i Navigator felületén érhető el. Ez a kiegészítő lehetővé teszi az IP csomagszűrő és a hálózaticím-fordítás (NAT) szabályainak konfigurálását, amely révén vezérelni tudja a rendszerre bemenő és onnan kimenő TCP/IP forgalmat.
- A Védett socket réteg (SSL) protokoll segítségével úgy állíthatja be az alkalmazásokat, hogy SSL használatával védett kapcsolatok jöjjenek létre a szerver alkalmazások és a kliensek között. Az SSL-t eredetileg a Web böngészők és a szerver alkalmazások védelmére fejlesztették ki, de más alkalmazásoknál is engedélyezhető a használata. Számos alkalmazáshoz engedélyezett már az SSL használata, például: IBM HTTP Server for i5/OS, System i Access for Windows, Fájlátviteli protokoll (FTP), Telnet stb.

  Kapcsolódó fogalmak

  “Biztonsági irányelvek és célok” oldalszám: 6
  A biztonság irányelv meghatározza, hogy mit akar védeni, és milyen biztonsági célokat vár el a felhasználóktól.

  “Virtuális magánhálózatok a biztonságos magán kommunikációhoz” oldalszám: 25
  A virtuális magánhálózat (VPN), amely a cég intranet hálózatának kiterjesztése egy nyilvános vagy privát hálózat meglévő keretrendszerén keresztül, lehetővé teszi a privát és biztonságos kommunikációt a szervezeten belül.

  “Forgatókönyv: JKL Toy Company e-business tervek” oldalszám: 7
  Tipikus példahelyzet a JKL Toy Company cég, amely elhatározta, hogy az Internet használatával kibővíti üzleti céljait; ez a példa segítséget nyújthat a saját e-business terveinek létrehozásában.

  Kapcsolódó tájékoztatás

  Csatlakozás az Internethez

  eServer biztonságtervező

  IP szűrés és hálózaticím-fordítás

  Védett socket réteg

  AS/400 Internet Security: Protecting Your AS/400 from HARM on the Internet

Az Internet biztonság tervezése

Amikor az Internet használati tervet készíti, akkor meg kell tervezni az Internettel kapcsolatos biztonsági igényeket is.

Részletesen tájékozódni kell az Internet használati tervekről, és dokumentálni kell a belső hálózat konfigurációját. A begyűjtött információk alapján pontosan kiértékelheti biztonsági igényeket.

Például a következő információkat kell dokumentálni és leírni:

- A hálózat aktuális konfigurációját.
- A tartománynév rendszer (DNS) és az e-mail szerver konfigurációs információit.
- 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; lehet azonban néhány szempontja a bizalmas adatokra vonatkozóan, amelyek védtelenül haladnak át az Interneten. Ha a versenytársak elfogják és használják 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 (például védett socket réteg (SSL) engedélyezése).

A réteges védelem elve a biztonságért

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

A biztonsági irányelv 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 i5/OS rendszerek vele született biztonsági szolgáltatásai a megfelelő beállítás esetén lehetővé teszik több kockázat minimálisra csökkentését is. A rendszer Internetre csatlakoztatása esetén azonban a belső hálózat biztonsága érdekében további biztonsági szempontokat is figyelembe kell venni.

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 támadások**

  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 támadások**

  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 egy erős alapszintű biztonságot kell beállítani a rendszeren.

Hálózati szintű biztonság

A hálózatbiztonsági intézkedések vezérlik a hozzáférést az i5/OS operációs rendszerhez és a többi hálózati rendszerhez. 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 lehet 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 rendszerhez (DNS).

Alkalmazás szintű biztonság

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. Különleges figyelmet kell azonban 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.

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 rendszeren 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.

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
Mielőtt csatlakozna az Internethez, el kell döntenie, milyen biztonsági szintre van szüksége a rendszer megóvásához.

“Hálózatbiztonsági beállítások” oldalszám: 11
A belső erőforrások megvédéséhez válassza ki a megfelelő hálózatszintű biztonsági intézkedéseket.

“Alkalmazásbiztonsági beállítások” oldalszám: 16
Lehetősége van számos népszerű Internetes alkalmazás és szolgáltatás biztonsági kockázatainak kezelésére.

“Átvitelbiztonsági beállítások” oldalszám: 22
Ahhoz, hogy megvédje az adatait, miközben azok keresztül mennek egy olyan megbízhatatlan hálózaton, mint az Internet, hatályba kell helyezni a megfelelő biztonsági intézkedéseket. Ezek az intézkedés a következők: Védett socket réteg (SSL), System i Access for Windows, és virtuális magánhálózat (VPN) kapcsolatok.

“Biztonsági irányelvek és célok” oldalszám: 6
A biztonság irányelv meghatározza, hogy mit akar védeni, és milyen biztonsági célokat vár el a felhasználóktól.

“E-mail biztonság” oldalszám: 19
Az Interneten vagy más nem megbízható hálózaton keresztül küldött e-mail biztonsági kockázatot jelent, még akkor is, ha a rendszer egy tűzfal védelme alatt áll.

Kapcsolódó hivatkozás


System i biztonsági kézikönyv IBM i5/OS V5R4 rendszerhez

Biztonsági irányelvek és célok

A biztonság irányelv meghatározza, hogy mit akar védeni, és milyen biztonsági célokat vár el a felhasználóktól.

Biztonsági irányelvek

Minden egyes biztosított Internet szolgáltatás potenciális veszélyt hordoz magával a rendszerrel, és a hozzá kapcsolódó hálózattal szemben. 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 megállapíthatja, 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 hozhatnak magukkal.

Biztonsági célok

Amikor létrehozza és végrehajtja a biztonsági irányelveket, világos célokkal kell rendelkezni. A biztonsági célok az alábbi kategóriákba 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 a System i 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, 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 i5/OS operációs rendszer esetén a rendszer sértetlensége a biztonság leggyakrabban áttekintett összetevője, mivel ez az i5/OS architektúra alapvető része. Az i5/OS architektúra például különösen nehézzé teszi egy betörő számára, hogy változtatásokat kezdeményezzen az operációs rendszer programjában, amikor a biztonsági szintje 40 vagy 50.

Letagadhatatlanság
Bizonyíték, hogy egy tranzakció megtörtént, vagy hogy elküldött vagy fogadott egy üzenetet. A digitális igazolások és a nyilvános kulcsok titkosításának igénybe vétele a tranzakciók, az üzenetek és a dokumentumok aláírására támogatja ezt a funkciót. A küldő és a fogadó is egyetért abban, hogy az adatcsere 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 a Védett socket réteg (SSL) vagy virtuális magánhálózat (VPN) kapcsolat 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.

Kapcsolódó fogalmak

“System i és Internet biztonság megfontolások” oldalszám: 2
Az Internethez kapcsolódó biztonsági kérdések igen jelentősek. Ez a fejezet bemutatja a i5/OS biztonsági erősségeit és ajánlatait.

“A réteges védelem elve a biztonságért” oldalszám: 3
A biztonsági irányelve meghatározza, hogy mit akar védeni, és mit vár el a rendszer felhasználóitól.

DCM konfigurálása

Védett socket réteg (SSL)

“Forgatókönyv: JKL Toy Company e-business tervek”
Tipikus példahelyzet a JKL Toy Company cég, amely elhatározta, hogy az Internet használatával kibővíti üzleti céljait; ez a példa segítséget nyújthat a saját e-business terveinek létrehozásában.

Forgatókönyv: JKL Toy Company e-business tervek

Tipikus példahelyzet a JKL Toy Company cég, amely elhatározta, hogy az Internet használatával kibővíti üzleti céljait; ez a példa segítséget nyújthat a saját e-business terveinek létrehozásában.

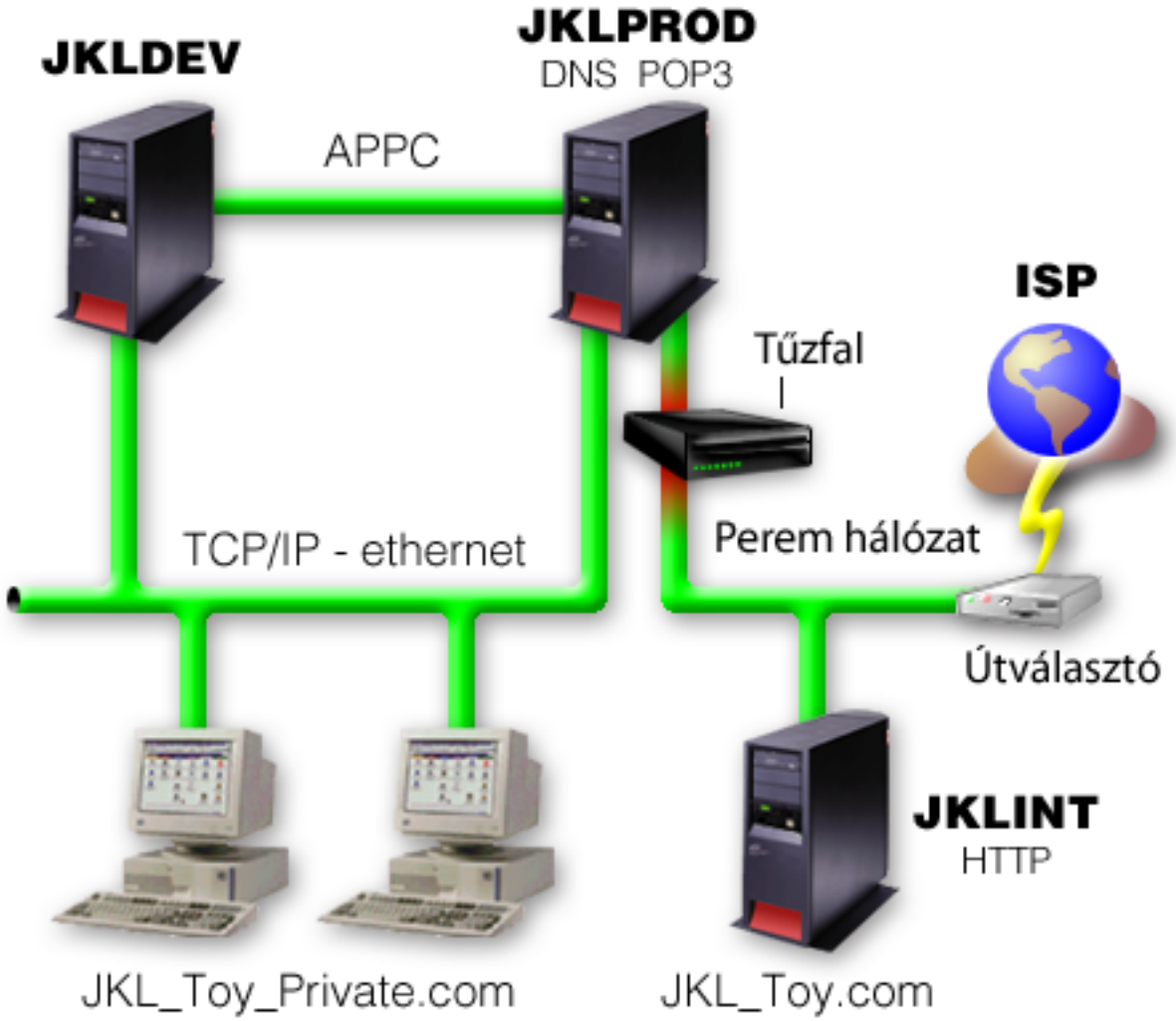
A JKL Toy Company egy kicsi, gyorsan növekvő játékgyár. A cég elnöke elkötelezett híve a vállalkozás gyarapodásának, és azt is látja, hogy az új i5/OS operációs rendszer könnyedén elbírja a növekedés terheit. Safranek Elek a főkönyvelő felelős a rendszer adminisztrálásáért és a rendszerbiztonságért.

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. A vállalat végső célként szeretné lehetővé tenni az ügyfelei számára, hogy online rendeléseiket közvetlenül a webhelyen keresztül végezhessék. 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 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 szerver 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. A következő ábra bemutatja a cég internetes vagy hálózati konfigurációját.



Ahogy az ábrán is látszik, a JKL Toy Company két elsődleges rendszerrel rendelkezik. A vállalat az egyik rendszert alkalmazásfejlesztésre (JKLDEV), a másikat pedig éles alkalmazásokhoz (JKLPROD) használja. Mindkét rendszer életbevágó adatokat és alkalmazásokat kezel. Következésképpen, nem lenne kényelmes az Internet alkalmazásokat ezeken a rendszereken futtatni. Úgy döntöttek, hogy egy új rendszeren (JKLINT) futtatják ezeket az alkalmazásokat.

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. Mivel az új rendszer kizárólag Internet szerverként működik, így a vállalat a hálózati biztonság kezelésének összetettségét is korlátozza.

A vállalat nem fog üzleti szempontból kritikus alkalmazásokat futtatni az új rendszeren. Az e-business terveknek ennél az állomásánál az új rendszer csak egy statikus nyilvános webhelyet szolgáltat. 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 hálózaticím-fordítási (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 biztonság irányelv meghatározza, hogy mit akar védeni, és milyen biztonsági célokat vár el a felhasználóktól.

“System i és Internet biztonság megfontolások” oldalszám: 2
Az Internethez kapcsolódó biztonsági kérdések igen jelentősek. Ez a fejezet bemutatja a i5/OS biztonsági erősségeit és ajánlatait.

“Hálózatbiztonsági beállítások” oldalszám: 11
A belső erőforrások megvédéséhez válassza ki a megfelelő hálózatszintű biztonsági intézkedéseket.

“Átvitelbiztonsági beállítások” oldalszám: 22
Ahhoz, hogy megvédje az adatait, miközben azok keresztül mennek egy olyan megbízhatatlan hálózaton, mint az Internet, hatályba kell helyezni a megfelelő biztonsági intézkedéseket. Ezek az intézkedés a következők: Védett socket réteg (SSL), System i Access for Windows, és virtuális magánhálózat (VPN) kapcsolatok.

Biztonsági szintek az alapszintű Internet eléréshez

Mielőtt csatlakozna az Internethez, el kell döntenie, milyen biztonsági szintre van szüksége a rendszer megóvásához.

A rendszer biztonsági intézkedések az Internet alapú biztonsági problémákkal szembeni védekezés legalsó szintjét képviselik. 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 javasolt a rendszer védelméhez olyan magas kockázati tényezőjű környezetben, mint az Internet.

  Megjegyzés: Ha pillanatnyilag az 50-esnél alacsonyabb biztonsági szinten dolgozik, szükségessé válhat a működési eljárások vagy az alkalmazások frissítése. Tekintse át a System i biztonsági kézikönyvet. a magasabb biztonsági szintre történő váltás előtt.
- A biztonsággal kapcsolatos rendszerváltozókat legalább korlátozó állapotba állítsa az ajánlott értékekhez képest. A System i Navigator biztonsági varázsló segítségével beállíthatja a javasolt biztonsági beállításokat.
- 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 rendszer minimális biztonsági követelményeit a következő eszközökkel állíthatja be: eServer Biztonsági tervező, vagy a Biztonság varázsló, amely az System i Navigator felületéről érhető el. 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 tervezővel szemben, a varázsló a javasolt beállítások használatával konfigurálja a rendszer biztonságát.

Az i5/OS rendszerben rejlő biztonsági szolgáltatások számos kockázatot tudnak minimalizálni, ha helyesen vannak beállítva és kezelve. A rendszer Internetre csatlakoztatása esetén azonban a belső hálózat biztonsága érdekében további biztonsági szempontokat is figyelembe kell venni. Miután meggyőződött róla, hogy a rendszer rendelkezik az általános biztonsági beállításokkal, további biztonsági intézkedéseket állíthat be az Internet használat átfogó biztonsági tervének részeként.

Kapcsolódó fogalmak

“A réteges védelem elve a biztonságért” oldalszám: 3
A biztonsági irányelve meghatározza, hogy mit akar védeni, és mit vár el a rendszer felhasználóitól.

Kapcsolódó hivatkozás

Biztonsági szint rendszerváltozó

Biztonsági kézikönyv

Hálózatbiztonsági beállítások

A belső erőforrások megvédéséhez válassza ki a megfelelő hálózatszintű biztonsági intézkedéseket.

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 lehet 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 rendszerhez (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.

Fő védelmi vonalként fontolja meg egy tűzfal használatát, ha a rendszert, vagy a belső hálózatot az Internethez csatlakoztatja. Bár az IBM Firewall for the i5/OS termék, és a hozzá tartozó támogatás már nem vásárolható meg, számos másik terméket használhat helyette.

Mivel a kereskedelmi forgalomban lévő tűzfal termékek a hálózati biztonságot adó technológiák teljes körét biztosítják, a JKL Toy Company kiválasztja az egyiket a saját hálózata védelméhez. Mivel az általuk választott tűzfal nem védi meg az operációs rendszerüket, az i5/OS csomag szabályokból származó kiegészítő biztonsági szolgáltatást is használják. Ez lehetővé teszi a szűrő és NAT szabályok létrehozását, amelyek az internetes szerver forgalmát szabályozzák.

Kapcsolódó fogalmak

“A réteges védelem elve a biztonságért” oldalszám: 3
A biztonsági irányelve meghatározza, hogy mit akar védeni, és mit vár el a rendszer felhasználóitól.

“Forgatókönyv: JKL Toy Company e-business tervek” oldalszám: 7
Tipikus példahelyzet a JKL Toy Company cég, amely elhatározta, hogy az Internet használatával kibővíti üzleti céljait; ez a példa segítséget nyújthat a saját e-business terveinek létrehozásában.

Behatolás felismerés

Kapcsolódó tájékoztatás

Redbook: 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 a következő funkciókkal rendelkezik:

- 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 csökkenti a kockázatot a belső hálózaton. 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
  - Hálózaticím-fordítás (NAT) szolgáltatások
  - SOCKS szerver
  - Proxy szerverek különféle szolgáltatásokkal, például HTTP, Telnet, FTP, és így tovább
  - Levéltovábbítási szolgáltatás
  - Osztott tartománynév rendszer (DNS)
  - Naplózás
  - Valós idejű megfigyelés

  Megjegyzés: Egyes tűzfal termékek virtuális saját hálózat (VPN) szolgáltatást nyújtanak, amely lehetővé teszi titkosított szekciók beállítását a tűzfal és más kompatibilis 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 rendszer 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 korlátozhatja a hálózati belépési pontok számát. 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 Hálózaticím-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, 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 Egyszerű levéltovábbítási protokoll (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.

i5/OS csomagszabályok

Az i5/OS csomagszabályok segítségével megvédheti rendszerét. A csomagszabályok az i5/OS operációs rendszer funkciói, és az System i Navigator felületről érhetők el.

A csomagszabályok segítségével két alapvető hálózati biztonsági technológiát állíthat be, amelyek a TCP/IP forgalmat vezérlik:

- Hálózaticím-fordítás (NAT)
- IP csomagszűrés

Mivel a NAT és az IP szűrés az i5/OS operációs rendszer 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: A rendszer biztonságának szempontjait előnyben kell részesíteni a költségekkel szemben. Fontolja meg a tűzfal használatát, ha biztos akar abban lenni, hogy maximális védelmet biztosít a termelési rendszernek.

Hálózaticím-fordítás és IP csomagszűrés

A hálózaticím-fordítás (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 inkompatibilis címzésű hálózatoknak, hogy egymáshoz kapcsolódjanak. Következésképpen, használhatja úgy a NAT szabályokat, hogy az i5/OS operációs 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.

IP csomagszűrés lehetőséget biztosít ahhoz, hogy szelektíven blokkolja vagy védje az IP forgalmat a csomag fejlécben lévő információk alapján. Az System i Navigator 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 csomagok legyenek beengedve a hálózatba, és melyek legyenek tiltva. 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 nem kívánt vagy szükségtelen forgalom elérje a rendszeren lévő alkalmazásokat. Ehhez hasonlóan, megakadályozhatja a forgalom továbbítását más rendszerekhez is. Ez magában foglalja az alacsony szintű Internet vezérlőüzenet protokoll (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. Miután az információk a rendszernaplóba kerültek, a naplóbejegyzést nem lehet módosítani. A napló ideális eszköz a hálózati tevékenység ellenőrzéséhez.

A csomagszűrő szabályokkal 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 lecserél egy nyilvános IP címet egy belső 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 i5/OS csomag szabályok funkció közötti választásról.

Kapcsolódó fogalmak

Hálózaticím-fordítás (NAT)

IP csomagszűrés

Behatolás felismerés

A *Behatolás felismerés* a jogosulatlan hozzáférési kísérletekre és a TCP/IP hálózaton keresztüli támadásokra vonatkozó információk összegyűjtését jelenti. Az átfogó biztonsági házirend rendelkezik egy behatolás felismerésnek szentelt résszel.

A *behatolás felismerés* kifejezés két módon kerül felhasználásra az i5/OS dokumentációban. Az első értelemben a behatolás felismerés a biztonsági veszélyforrások felismerését és megelőzését jelenti. Egy betörő például érvénytelen felhasználói azonosító segítségével megpróbálhat behatolni a rendszerbe, vagy egy túl sok jogosultsággal rendelkező gyakorlatlan felhasználó fontos objektumokat változtathat meg a rendszerkönyvtárakban.

A másik értelemben a behatolás felismerés az új behatolás felismerő funkcióra vonatkozik, amely házirendek segítségével figyeli meg a rendszeren végbemenő kártékony forgalmat. Létrehozhat behatolást észlelő szabályzatot, amely megvizsgálja a TCP/IP hálózaton keresztül érkező gyanús behatolási kísérleteket.

i5/OS hálózatbiztonsági beállítások kiválasztása

Válassza ki az internet használati tervének megfelelő hálózatbiztonsági beállításokat.

A jogosulatlan hozzáférés ellen védő hálózatbiztonsági megoldások általában tűzfal technológiákra épülnek. A rendszer megóvásához használhat teljes funkcionalitású tűzfal terméket, vagy az i5/OS TCP/IP megvalósítás részeként érvénybe léptethet specifikus hálózatbiztonsági technológiákat. Ez a megvalósítás a következőkből áll: csomagszabályok (IP szűrés és NAT), és a HTTP for i5/OS proxy szerver licencprogram.

A hálózati környezettől, a hozzáférési követelményektől és a biztonsági igényektől függ az, hogy a csomag szabályokat választja vagy egy tűzfal terméket. Fő védelmi vonalként fontolja meg egy tűzfal használatát, ha a rendszert, vagy a belső hálózatot az Internethez, vagy más 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.

Megjegyzés: Együtt is használhatja a tűzfalat és az integrált i5/OS hálózatbiztonsági technológiákat. Így megóvhatja a rendszert a külső támadóktól (a tűzfal mögül), valamint az összes olyan támadástól, amely rossz konfiguráció, vagy egyéb dolog miatt átjut a tűzfalon.

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 rendszeren, potenciálisan elérheti a különféle hasznos alkalmazásokat, szolgáltatásokat és adatokat. A támadó ezek segítségével megsemmisítheti magát a rendszert, vagy hozzáférhet a belső hálózat más rendszereihez.

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 i5/OS rendszernek, mint például egy nyilvános webszervernek vagy egy érzékeny adatokkal rendelkező intranet rendszernek. • A vállalati intranet egyik alhálózatát védi, amikor az i5/OS rendszer átjáróként szerepel (alkalmi útválasztóként) a hálózat többi része számára. • A kommunikációt vezérli, ami egy némiképp megbízható partnerrel folyik magán hálózaton vagy extraneten keresztül, ahol az i5/OS rendszer 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.

Biztonsági technológia	Legjobb az i5/OS TCP/IP technológia használata	Legjobb a teljes funkciójú tűzfal használata
Hálózaticím-fordítás (NAT)	• Kapcsolatot engedélyez két magánhálózat között, amelyek inkompatibilis 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.

Kapcsolódó hivatkozás

IP szűrés és hálózaticím-fordítás

HTTP Server for i5/OS

Kapcsolódó tájékoztatás

AS/400 Internet Scenarios: A Practical Approach

Alkalmazásbiztonsági beállítások

Lehetősége van számos népszerű Internetes alkalmazás és szolgáltatás biztonsági kockázatainak kezelésére.

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 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. A biztonsági intézkedéseknek le kell fedni a szerver- és a kliens oldali biztonsági kockázatokat.

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

Kapcsolódó fogalmak

“A réteges védelem elve a biztonságért” oldalszám: 3
A biztonsági irányelve meghatározza, hogy mit akar védeni, és mit vár el a rendszer felhasználóitól.

Web szolgáltatás biztonsága

Amikor hozzáférést biztosít a látogatóknak a saját webhelyéhez, akkor nem tájékoztatja őket arról, hogyan állította be a helyet, és milyen kód állítja elő a lapot. A látogatásnak könnyűnek, gyorsnak és simának kell lenni, a munkának pedig a színfalak mögött kell végbemenni.

Adminisztrátorként biztosítani kell, hogy biztonsági gyakorlatok ne legyenek negatív hatással a webhelyre, de valósítsák meg a kiválasztott biztonsági modelleket. Ennek eléréséhez választani kell az IBM HTTP Server for i5/OS beépített biztonsági szolgáltatásai közül.

Az Apache alapú IBM HTTP szerver Redbook biztonsági beállításokról szóló fejezete leírja, hogyan lehet a hitelesítés, a hozzáférés felügyelet és a titkosítás segítségével megvalósítani a biztonsági szolgáltatásokat.

A Hiperszöveg átviteli protokoll (HTTP) lehetőséget nyújt az adatbázis fájl adatainak megjelenítésére, de módosításukra nem. Néha azonban szükség van olyan alkalmazások megírására, amelyeknek frissíteni is kell adatbázis

fájlokat. Például, létre akar hozni olyan űrlapokat, amelyeket később a felhasználó tölt ki, és frissíti vele az i5/OS adatbázist. Ehhez általános átjáró illesztő (CGI) programokat használhat.

Egy másik használható biztonsági szolgáltatás a proxy szerver. Fogadja a más szervereknek küldött kéréseket, és teljesíti, továbbítja, átirányítja vagy elutasítja azokat.

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

A CGI programokon kívül használhat Java programokat is a weblapokon. Mielőtt Java programokat használna a webhelyen, meg kell értenie a Java biztonsági szolgáltatásait.

Kapcsolódó fogalmak

"Java Internet biztonság"
A Java programozás egyre szélesebb körben terjed napjaink számítástechnikai környezetében. Fel kell készülnie a Java nyelvhez tartozó biztonsági tényezők kezelésére.

Kapcsolódó tájékoztatás

Proxy szerver típusok és használatuk Apache alapú HTTP szerver esetén

Biztonsági tippek a HTTP szerverhez

Common Gateway Interface

Java Internet biztonság

A Java programozás egyre szélesebb körben terjed napjaink számítástechnikai környezetében. Fel kell készülnie a Java nyelvhez tartozó biztonsági tényezők kezelésére.

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.) A Java például erősen típusos, kivétel nélkül szorosan veszi a típusszabályokat, ezzel biztosítja, hogy a programozó megfelelő módon használja az objektumokat. 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 a rendszeren.

Java kisalkalmazások

A *Java kisalkalmazások* olyan kis Java programok, amelyeket HTML oldalakba ágyazva a kliens oldalon futnak, de potenciálisan hozzáférnek az i5/OS operációs rendszerhez. (A hálózatban lévő PC-n működő Nyílt adatbázis összekapcsolhatóság (ODBC) vagy fejlett program-program kommunikáció (APPC) programok ugyancsak elérhetik az operációs rendszert, amikor például a rendszer alkalmazásokat szolgál ki, vagy webszerverként működik. Általánosságban elmondható, hogy a Java kisalkalmazások csak azzal az i5/OS operációs rendszerrel tudnak szekciót létrehozni, amelyiktől a kisalkalmazás ered. Ezért egy Java kisalkalmazás csak akkor férhet hozzá egy csatlakoztatott PC-ről az i5/OS operációs rendszerhez, ha magáról az i5/OS operációs rendszerről jön.

A kisalkalmazás megpróbálhatja a kapcsolódást a rendszer bármelyik TCP/IP portján. Nem kell egyeztetni a Java nyelven írt szoftver szerverrel. Az IBM Toolbox for Java segítségével írt rendszerek esetében azonban, a kisalkalmazásnak felhasználói azonosítót és jelszót kell szolgáltatni, amikor kapcsolatot létesít vissza a rendszerhez.

Ebben az anyagban a leírt rendszerek mindegyike i5/OS operációs rendszer. (A Java alkalmazásszervernek nincs szüksége az IBM Toolbox for Java használatára.) 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 i5/OS operációs rendszeren, 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 alkalmazás 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 az i5/OS operációs rendszeren; ez azomban nem esik a böngésző biztonsági korlátozásai alá. Ezért 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, és ez alkalmat nyújt a kisalkalmazásnak romboló tevékenység folytatására. 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 a rendszeren, mert azok a PC számára helyi lemezegységekként jelennek meg.

A rendszerről 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 (DCM) 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 Web Enablement for i5/OS része, támogatja a szerver kisalkalmazások használatát az i5/OS operációs rendszereken.

Erőforrás biztonságot kell beállítani azokra a szerver kisalkalmazás objektumokra, amelyeket a rendszer használ. Azonban, az erőforrás biztonság alkalmazása a szerver kisalkalmazásra még jelent elegendő védelmet. Miután 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 vezérlőket és direktívákat is. Ne engedélyezze például, hogy a szerver kisalkalmazások csupán a webszerver profilja alatt fussanak. Használja továbbá a szerver kisalkalmazás fejlesztőeszközei által nyújtott biztonsági funkciókat, mint amilyeneket a WebSphere Application Server for i5/OS tartalmaz.

A Java általános biztonsági rendszabályait az alábbi helyen tanulmányozhatja:

- IBM Developer Kit for Java: Java biztonság.
- IBM Toolbox for Java: Biztonsági osztályok.
- Internet böngészők biztonsági tudnivalói.

Java hitelesítés és jogosultságkezelés az erőforrásokhoz

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 i5/OS rendszeren fut. Ezt követően ellenőrzi az erőforrás biztonságot a hozzárendelt azonosság alatt.

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).

Java alkalmazások biztonságossá tétele SSL használatával

A Védett socket réteg (SSL) segítségével biztonságossá teheti az IBM Developer Kit for Java programmal fejlesztett i5/OS 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 azt.

Kapcsolódó fogalmak

"Web szolgáltatás biztonsága" oldalszám: 16
Amikor hozzáférést biztosít a látogatóknak a saját webhelyéhez, akkor nem tájékoztatja őket arról, hogyan állította be a helyet, és milyen kód állítja elő a lapot. A látogatásnak könnyűnek, gyorsnak és simának kell lenni, a munkának pedig a színfalak mögött kell végbemenni.

DCM konfigurálása

Hitelesítési szolgáltatások

Kapcsolódó tájékoztatás

Java hitelesítés és hitelesítési szolgáltatás

Védett socket réteg (SSL)

E-mail biztonság

Az Interneten vagy más nem megbízható hálózaton keresztül küldött e-mail biztonsági kockázatot jelent, még akkor is, ha a rendszer egy tűzfal védelme alatt áll.

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. Fontos, hogy igen meggondolt legyen, mielőtt bármilyen bizalmas információt elküldene e-mail formájában. Mivel az e-mail sok rendszeren 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 szolgáltatás megbénítását tapasztalhatja, mivel a szerver tároló lemeze megtelik haszontalan üzenetekkel. Akkor is leállhat a rendszer válaszadása, ha az összes rendszererőforrás a támadásból származó levelek feldolgozásával van elfoglalva.
- 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 rendszeren áthalad, mielőtt megérkezik a címzetthez. Ha nem titkosítja az üzenetet, a hacker elkaphatja 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.

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 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 rendszer segítségével különböző VPN kapcsolatokat állíthat be, beleértve a távoli kliensek és a rendszer közti kapcsolatokat is. Amikor VPN kapcsolatot használ, a kommunikációs végpontok között folyó teljes forgalom titkosítva van, ami biztosítja az adatok titkosságát és sérthetetlenségét.

Kapcsolódó fogalmak

“FTP biztonság” oldalszám: 21
A fájlátviteli protokoll (FTP) fájlátviteli képességet biztosít egy kliens (egy felhasználó egy másik rendszeren) és a szerver között. Ahhoz, hogy meggyőződjön róla, hogy biztonsági irányelvek hogyan minimalizálják a kockázatokat, meg kell értenie azokat a biztonsági kockázatokat, amelyekkel az FTP használata esetén számolhat.

“A réteges védelem elve a biztonságért” oldalszám: 3
A biztonsági irányelve meghatározza, hogy mit akar védeni, és mit vár el a rendszer felhasználóitól.

Virtuális magánhálózat (VPN)

Kapcsolódó hivatkozás

Biztonsági szakkifejezések

Kapcsolódó tájékoztatás

Lotus Domino referencia könyvtár

Lotus dokumentáció

Lotus Notes and Domino R5.0 Security Infrastructure Revealed Redbook

Lotus Domino for AS/400 Internet Mail and More Redbook

FTP biztonság

A fájlátviteli protokoll (FTP) fájlátviteli képességet biztosít egy kliens (egy felhasználó egy másik rendszeren) és a szerver között. Ahhoz, hogy meggyőződjön róla, hogy biztonsági irányelvek hogyan minimalizálják a kockázatokat, meg kell értenie azokat a biztonsági kockázatokat, amelyekkel az FTP használata esetén számolhat.

A távoli parancs segítségével elküldhet parancsokat a szervernek. Következésképpen, az FTP 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. Ezeknek a kockázatoknak a megértése segít a rendszer biztonságossá tételében.

- 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 i5/OS teljes objektum biztonságát a rendszeren (másszóval, változtassa meg a rendszer biztonsági modelljét menü biztonságról objektum biztonságra. Ez a legjobb, és legbiztonságosabb lehetőség).
  – 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. Lehetséges, hogy még jobban szeretné korlátozni az FTP hozzáférés vezérlést. Ez a beállítás csak az FTP funkcióra vonatkozik, más illesztőfelületekre, mint például a nyílt adatbázis összekapcsolhatóság (ODBC), az osztott adatkezelés (DDM) vagy az osztott relációs adatbázis architektúra (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 megbénítást 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 megbénítása 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, mérlegelje a biztonsági kockázatokat, gondolkodjon el azon, hogy kilépési programokkal védje az FTP szervert.

Kapcsolódó fogalmak

“E-mail biztonság” oldalszám: 19
Az Interneten vagy más nem megbízható hálózaton keresztül küldött e-mail biztonsági kockázatot jelent, még akkor is, ha a rendszer egy tűzfal védelme alatt áll.

Kapcsolódó feladatok

Anonymous Fájlátviteli protokoll konfigurálása

Hozzáférés-kezelés Fájlátviteli protokoll végprogramok használatával

Kapcsolódó tájékoztatás

Az FTP biztonságossá tétele

Az FTP szerver biztonságossá tétele SSL használatával

Átvitelbiztonsági beállítások

Ahhoz, hogy megvédje az adatait, miközben azok keresztül mennek egy olyan megbízhatatlan hálózaton, mint az Internet, hatályba kell helyezni a megfelelő biztonsági intézkedéseket. Ezek az intézkedés a következők: Védett socket réteg (SSL), System i Access for Windows, és virtuális magánhálózat (VPN) kapcsolatok.

Emlékezzen rá, hogy a JKL Toy Company forgatókönyve két elsődleges rendszerrel rendelkezik. Ebből az egyiket fejlesztésre használják, míg a másikat a termelési alkalmazásokra. Mindkét rendszer életbevágó adatokat és alkalmazásokat kezel. Következésképpen, az új 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 a szétválasztás csökkenti a belső rendszer potenciális, az Internetről jelentkező kockázatait. Mivel az új rendszer kizárólag Internet szerverként működik, így a vállalat a hálózati biztonság kezelésének összetettségét is korlátozza.

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 a gyakorlatban kell megvalósítani a biztonsági intézkedéseket, hogy megvédje az adatok átvitelét, miközben azok az Interneten keresztül haladnak.

A nem megbízható rendszereken áthaladó információkhoz tartozó kockázatokat minimalizálhatja két, sajátos átviteli szintű i5/OS operációs rendszer funkcióval: SSL biztonságos kommunikáció és VPN kapcsolatok.

Az SSL protokoll egy ipari szabvány, amely a kliens és szerver közti kommunikációt teszi biztonságossá. Az SSL protokollt eredetileg Web böngésző alkalmazások számára fejlesztették ki, de egyre több egyéb alkalmazás is képes az SSL használatára. Az i5/OS operációs rendszer esetén a következők tartalmazzák:

- IBM HTTP Server for i5/OS (Apache alapú)
- FTP szerver
- Telnet szerver
- Osztott relációs adatbázis architektúra (DRDA) és Osztott adatkezelés (DDM) szerver
- Az System i Navigator Kezelőközpontja
- Címtár szolgáltatások szerver (LDAP)
- System i Access for Windows alkalmazások, beleértve a következőket: System i Navigator, és azok az alkalmazások, amelyek a System i Access for Windows alkalmazás programozási felületekhez (API) készültek
- 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.

Virtuális magánhálózat

A VPN kapcsolatot két végpont közötti biztonságos kommunikációs csatona létrehozásához használhatja. 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.

Melyik módszert használja?

Az SSL és a VPN egyaránt garantálja a biztonságos hitelesítést, az adatok bizalmas voltát és sérthetetlenségét. Számos tényezőtől függ, hogy melyik módszert kell használni. Megfontolandó, 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 nem tudja kihasználni az SSL előnyeit, számos más, mint a Telnet és az System i Access for Windows 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. Ha azonban 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 létrehozhat egy átjáró-átjáró VPN kapcsolatot a hálózat adott részére. Ez biztonságossá teheti 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: 3
A biztonsági irányelve meghatározza, hogy mit akar védeni, és mit vár el a rendszer felhasználóitól.

“Forgatókönyv: JKL Toy Company e-business tervek” oldalszám: 7
Tipikus példahelyzet a JKL Toy Company cég, amely elhatározta, hogy az Internet használatával kibővíti üzleti céljait; ez a példa segítséget nyújthat a saját e-business terveinek létrehozásában.

Kapcsolódó hivatkozás

Védett socket API-k

Kapcsolódó tájékoztatás

Védett socket réteg (SSL)

Virtuális magánhálózat (VPN)

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 i5/OS rendszeren 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 i5/OS 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 meghatározza, hogy milyen azonosítási információkat igényel az igazolás kiadása céljából. Egyes Internet CA-k lehet, hogy kevés információt igényelnek, mint például megkülönböztető nevet csak. Ez a személynek vagy a rendszernek 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.

Annak ellenére, hogy sok alkalmazás nem tudja kihasználni az SSL előnyeit, számos más, mint a Telnet és az System i Access for Windows rendelkeznek SSL képességgel.

Kapcsolódó fogalmak

DCM konfigurálása

Védett socket réteg (SSL)

Kapcsolódó hivatkozás

Biztonsági szakkifejezések

Védett socket réteg a Telnet elérés titkosításához

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 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 Telnet szekciók SSL használatát a Telnet attribútumok módosítása (CHGTELNA) parancs Védett socket réteg engedélyezése (ALWSSL) paraméterével vezérelheti. A TCP/IP portkorlátozás hozzáadása (ADDTCPPORT) parancs segítségével biztosíthatja, hogy az alkalmazások a megfelelő SSL vagy nem SSL portokat használják.

Ha meg szeretné ismerni a Telnet funkciót és az ezzel kapcsolatos biztonsági tippeket (SSL használatával és anélkül), akkor olvassa el az IBM Systems Szoftver információs központ Telnet-tel foglalkozó témakörét, amely információkat nyújt a Telnet i5/OS operációs rendszeren történő használatáról.

Kapcsolódó fogalmak

Telnet példahelyzet: a Telnet biztonságossá tétele SSL segítségével

DCM tervezése

Kapcsolódó tájékoztatás

Telnet

Védett socket réteg a System i Access for Windows biztonságossá tételéhez

A System i Access for Windows kommunikációs szekciók biztonságossá tételéhez beállíthatja, hogy a System i Access for Windows Védett socket réteget (SSL) használjon.

Az SSL használata biztosítja, hogy a System i Access for Windows szekciók teljes forgalma titkosított legyen. Ez megakadályozza azt, hogy az adatokat valaki elolvassa, míg azok a helyi és a távoli gazdagépek között mozognak.

Kapcsolódó tájékoztatás

Védett socket réteg adminisztráció

Java biztonság

Biztonsági osztályok

Virtuális magánhálózatok a biztonságos magán kommunikációhoz

A virtuális magánhálózat (VPN), amely a cég intranet hálózatának kiterjesztése egy nyilvános vagy privát hálózat meglévő keretrendszerén keresztül, lehetővé teszi a privát és biztonságos kommunikációt a szervezeten belül.

A 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 i5/OS operációs rendszert használ, és VPN kapcsolat biztosítja a szükséges védett kommunikációt a két hálózat között. Egy VPN létrehozása sokkal költséghatékonyabb megoldás, mint a hagyományos nem kapcsolt vonalak használata.

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 weboldalak frissítésére használ. Meg akarja engedni 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. 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 azon 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 i5/OS operációs rendszer 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.

Kapcsolódó fogalmak

“System i és Internet biztonság megfontolások” oldalszám: 2
Az Internethez kapcsolódó biztonsági kérdések igen jelentősek. Ez a fejezet bemutatja a i5/OS biztonsági erősségeit és ajánlatait.

Virtuális magánhálózatok (VPN)

. 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 IBM Vásárlói megállapodás, IBM Nemzetközi programlicenc szerződés, 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 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 körülmények között 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. © Szerői jog: 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.

Programozási felületre vonatkozó információk

A System i és Internet biztonság kiadvány leír olyan programozási csatolókat, amelyek révén a felhasználó írhat programokat az IBM i5/OS kiszolgálásához.

Védjegyek

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

Domino
Distributed Relational Database Architecture (DRDA)
i5/OS
IBM
IBM (logó)
Lotus Notes
Notes
System i
WebSphere

Az Adobe, az Adobe logó, a PostScript és a PostScript logó az Adobe Systems Incorporated védjegyei vagy bejegyzett 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.

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