System i

System i a zabezpečení Internetu

Verze 6 vydání 1

System i

System i a zabezpečení Internetu

Verze 6 vydání 1

Poznámka

Dříve než použijete tyto informace a produkt, který podporují, nezapomeňte si přečíst informace uvedené v části “Upozornění”, na stránce 27.

Toto vydání se týká verze 6, vydání 1, modifikace 0 operačního systému IBM i5/OS (5761-SS1) a všech následných vydání a modifikací, dokud nebude v nových vydáních uvedeno jinak. Tato verze nefunguje na všech modelech počítačů RISC (reduced instruction set computer) ani na modelech CISC.

Obsah

System i a zabezpečení Internetu

Přístup k Internetu z Vaší lokální sítě (LAN) vyžaduje, abyste přehodnotili své požadavky na zabezpečení.

Integrovaná softwarová řešení a architektura zabezpečení produktu IBM System i Vám umožňuje budovat silnou obranu proti možným bezpečnostním pastem a narušitelům v Internetu. Využívání těchto nabídek zabezpečení zajišťuje, že Vaši zákazníci, zaměstnanci a obchodní partneři získají potřebné informace v bezpečném prostředí.

Tato kolekce témat vysvětluje tato dobře známá ohrožení zabezpečení a způsob, jak tato ohrožení souvisejí s Vašimi cíli v oblastiInternetu a elektronického obchodování. Tato kolekce témat rovněž popisuje, jak zhodnotit rizika v porovnání s výhodami používání různých možností zabezpečení, která systém obsahuje proti těmto rizikům. Můžete se rozhodnout, jak použít tyto informace k rozvoji plánu zabezpečení sítě, který bude nejlépe vyhovovat Vašim obchodním potřebám.

Soubor PDF pro System i a zabezpečení Internetu

Můžete si prohlédnout a vytisknout soubor PDF s těmito informacemi.

Chcete-li zobrazit nebo stáhnout tento dokument ve formátu PDF, vyberte téma System i a zabezpečení Internetu (přibližně 456 kB).

Zobrazovat nebo stahovat můžete také tato související témata:

- Detekce vniknutí (přibližně 285 kB). Můžete nastavit zásady detekce vniknutí, které budou monitorovat události podezřelých vniknutí, která byla provedena prostřednictvím TCP/IP sítě, jako např. nesprávně vytvořené IP pakety. Můžete také napsat aplikaci, která bude analyzovat data monitorování a hlásit administrátorovi zabezpečení každé případné probíhající TCP/IP vniknutí.
- EIM (Enterprise Identity Mapping) (přibližně 1954 kB). EIM (Enterprise Identity Mapping) je mechanismus mapování osoby nebo entity (jako např. služby) na odpovídající totožnosti uživatelů v různých registrech uživatelů v celém podniku.
- Jednotné přihlášení (přibližně 1203 kB). Řešení pro jednotné přihlášení snižuje počet přihlášení, které musí uživatel provést, stejně jako počet hesel, která uživatel potřebuje k přístupu k více aplikacím a serverům.
- Plánování a nastavení zabezpečení systému (přibližně 3992 kB). Plánování a nastavení zabezpečení systému poskytuje informace o tom, jak efektivně a systematicky plánovat a konfigurovat zabezpečení na úrovni systému.

Uložení souborů ve formátu PDF

Jak uložit soubory ve formátu PDF na pracovní stanici za účelem prohlížení nebo tisku:

1. Klepněte pravým tlačítkem na odkaz PDF ve svém prohlížeči.
2. Klepněte na volbu, která soubor PDF uloží lokálně.
3. Přejděte do adresáře, do kterého chcete uložit soubor PDF.
4. Klepněte na **Save** (Uložit).

Stažení aplikace Adobe Reader

Abyste mohli zobrazit či tisknout tyto soubory ve formátu PDF, musíte mít na svém systému naintalován produkt Adobe Reader. Zde si můžete stáhnout zdarma jeho kopii: Adobe Web site (www.adobe.com/products/acrobat/readstep.html) .

Související pojmy

Detekce vniknutí

Enterprise Identity Mapping (EIM)

Jednotné přihlášení

Plánování a nastavení zabezpeční systému

Produkt System i a otázky zabezpečení Internetu

Bezpečnostní otázky spojené s Internetem jsou významné. Toto téma nabízí přehled silných stránek zabezpečení a možností zabezpečení operačního systému i5/OS.

Když připojíte svou platformu System i k Internetu, jedna z Vašich prvních otázek typicky bude ″Co bych měl vědět o zabezpečení a Internetu?″ Toto téma Vám může pomoci zodpovědět tuto otázku.

To, co potřebujete vědět, závisí na tom, k čemu chcete Internet využívat. Vaší první akcí v Internetu bude poskytnout uživatelům Vaší interní sítě přístup k webu a k elektronické poště. Možná budete potřebovat také schopnost přenášet citlivé informace z jednoho serveru do druhého. A konečně můžete plánovat použití Internetu pro elektronický obchod nebo pro vytvoření sítě typu extranet mezi vaší společností a obchodními partnery a dodavateli.

Dříve než s Internetem začnete, měli byste si promyslet, co chcete dělat a jakým způsobem to chcete dělat. Rozhodování ve věci využití Internetu a zabezpečení dat na Internetu může být složité.

Poznámka: Jestliže nejste obeznámeni s terminologií týkající se zabezpečení dat a Internetu, můžete se při práci s tímto materiálem podívat na všeobecnou Terminologii zabezpečení.

Jakmile si ujasníte, jak chcete používat Internet pro elektronické podnikání a také jaké jsou problémy zabezpečení a dostupné nástroje, funkce a nabídky zabezpečení, můžete vyvinout vlastní strategii a cíle zabezpečení. Vaše volby při vyvíjení strategie zabezpečení bude ovlivňovat řada faktorů. Když se svou organizací pronikáte na Internet, představuje strategie zabezpečení ochrany dat rozhodující faktor pro zajištění bezpečnosti vašich systémů a prostředků.

Charakteristiky zabezpečení operačního systému i5/OS

Kromě velké nabídky specifických produktů sloužících k zabezpečení vašeho systému v síti Internet má operační systém i5/OS následující charakteristiky zabezpečení:

- Integrované zabezpečení dat, které se nesmírně obtížně obchází ve srovnání s přídavnými softwarovými balíky nabízenými v jiných systémech.
- Objektová architektura, která technicky ztěžuje vytvoření a rozšíření viru. V operačním systému i5/OS nemůže soubor předstírat, že je program, a program nemůže změnit jiný program. Vlastnosti integrity operačního systému i5/OS vyžadují, abyste při přístupu k objektům použili systémem dodávaná rozhraní. K objektu nemůžete přistupovat přímo podle jeho adresy v systému. Nelze vzít offset a změnit jej na ukazatel nebo z něj ukazatel ″vyrobit″. Manipulace s ukazateli je oblíbená technika vetřelců v architektuře jiných systémů.
- Flexibilita, která vám umožňuje nastavit zabezpečení systému tak, aby vyhovovalo vašim specifickým požadavkům. Můžete využít Plánovač zabezpečení, který doporučí zabezpečení ochrany dat odpovídající Vašim potřebám zabezpečení.

Rozšířená nabídka zabezpečení operačního systému i5/OS

Operační systém i5/OS rovněž nabízí několik specifických produktů, které můžete použít k rozšíření zabezpečení systému, když se připojujete k síti Internet. Podle toho, jak Internet používáte, budete se rozhodovat pro využití některých z těchto nabízených produktů:

- VPN (Virtual private network) je rozšířením soukromé vnitropodnikové sítě do veřejné sítě, jakou je například Internet. VPN můžete použít k vytvoření zabezpečeného soukromého připojení, v podstatě vytvořením soukromého tunelu přes veřejnou síť. VPN je integrovaná funkce operačního systému i5/OS dostupná z rozhraní produktu System i Navigator.

- Pravidla paketů jsou integrovaná funkce operačního systému i5/OS přístupná z rozhraní produktu System i Navigator. Tato funkce vám umožňuje konfigurovat pravidla pro filtrování IP paketů a pro NAT (převod síťových adres) pro řízení postupu provozu TCP/IP do a z Vašeho systému.
- S prrotokoly SSL (Secure Sockets Layer) můžete konfigurovat aplikace tak, aby používaly SSL k vytvoření zabezpečeného připojení mezi aplikacemi serveru a jejich klienty. Protokol SSL byl původně vyvinut k zabezpečení webového prohlížeče a aplikací serverů, ale ostatním aplikacím může být jeho používání umožněno. Mnohým aplikacím je nyní povoleno použití protokolu SSL, včetně produktů IBM HTTP Server for i5/OS, System i Access for Windows, File Transfer Protocol (FTP), Telnet, a tak dále.

  Související pojmy

  “Strategie a cíle zabezpečení ochrany dat” na stránce 5
  Vaše strategie zabezpečení definuje, co chcete chránit, a cíle zabezpečení jsou to, co očekáváte od uživatelů.

  “VPN pro zabezpečení soukromých komunikací” na stránce 24
  VPN (Virtual private network), rozšíření intranetu společnosti přes existující rámec buď veřejné nebo soukromé sítě, Vám může pomoci bezpečně a soukromě komunikovat uvnitř Vaší organizace.

  “Scénář: Plán elektronického podnikání společnosti JKL Toy Company” na stránce 7
  Typický scénář pro společnost JKL Toy, která se rozhodla rozšířit cíle svého podnikání pomocí využívání Internetu, Vám může pomoci při nastavení Vašeho vlastního plánu na elektronické obchodování.

  Související informace

  připojení k Internetu

  Plánovač zbezpečení eServeru

  Filtrování IP a převod síťové adresy

  SSL (Secure Sockets Layer)

  Zabezpečení Internetu AS/400: Jak chránit Váš AS/400 před poškozením na Internetu

Plánování zabezpečení Internetu

Při vývoji plánů na použití sítě Internet musíte pečlivě naplánovat i potřeby jeho zabezpečení.

Měli byste shromáždit podrobné informace o plánovaném využití Internetu a zdokumentovat konfiguraci vaší interní sítě. Na základě takto shromážděných informací můžete dospět k přesnému ohodnocení požadavků na zabezpečení ochrany dat.

Potřebujete například zdokumentovat a popsat následující informace:

- Aktuální konfiguraci vaší sítě.
- Informace o konfiguraci serveru DNS a serveru elektronické pošty.
- Vaše připojení k poskytovateli služeb sítě Internet (ISP).
- Služby, které chcete na Internetu používat.
- Služby, které chcete poskytovat uživatelům Internetu.

Zdokumentování tohoto typu informací vám pomůže určit, kde jsou bezpečnostní rizika a jaká bezpečnostní opatření musíte použít, abyste tato rizika minimalizovali.

Například se rozhodnete, že chcete interním uživatelům dovolit používat Telnet, budou-li se chtít připojit ke speciálnímu zdroji za účelem výzkumu. Vaši interní uživatelé tuto službu potřebují při vývoji nových produktů v podniku; máte však jisté obavy o důvěrná data, která by nechráněná procházela sítí Internet. Kdyby se konkurence k těmto datům dostala a zneužila jich, mohlo by to pro vaši společnost představovat finanční riziko. Když určíte potřeby vašeho využití (Telnet) a s ním spojené riziko (ohrožení důvěrných informací), můžete stanovit, jaká další bezpečnostní opatření byste měli přijmout pro zajištění utajení dat při tomto využití (jako například aktivace SSL (Secure Sockets Layer)).

Metoda zabezpečení ochrany dat pomocí vrstvené obrany

Vaše strategie zabezpečení definuje, co chcete chránit a co očekáváte od uživatelů Vašeho systému.

Vaše strategie zabezpečení je základem pro plánování zabezpečení při navrhování nových aplikací nebo rozšiřování Vaší současné sítě. Popisuje odpovědnost uživatelů, jako například ochranu důvěrných informací a vytváření složitých hesel.

Poznámka: Ve své organizaci musíte vytvořit a prosadit strategii zabezpečení ochrany dat, která minimalizuje riziko pro vaši interní síť. Inherentní funkce zabezpečení operačního systému i5/OS, pokud jsou správně nakonfigurovány, Vám umožní minimalizovat mnohá rizika. Avšak když připojíte svůj systém k Internetu, budete muset přijmout dodatečná bezpečnostní opatření k zajištění bezpečnosti své interní sítě.

Mnohá rizika jsou spojena s používáním přístupu k Internetu k provádění obchodní činnosti. Kdykoli budete vytvářet strategii zabezpečení ochrany dat, musíte vytvořit rovnováhu mezi poskytováním služeb a řízením přístupu k funkcím a datům. U počítačů zapojených do sítí je zabezpečení mnohem obtížnější, protože útoku je vystaven samotný komunikační kanál.

Některé internetové služby jsou zranitelnější vůči jistým typům napadení než jiné. Je proto rozhodující, abyste pochopili rizika spojená s jednotlivými službami, které máte v úmyslu použít nebo poskytovat. Mimoto, když pochopíte možná bezpečnostní rizika, budete moci jasně určit cíle zabezpečení dat.

Internet hostí mnoho jedinců, kteří představují ohrožení pro komunikaci v této síti. Následující seznam popisuje některá z typických bezpečnostních rizik, s nimiž byste se mohli setkat:

- **Pasivní napadení**

  Při pasivním napadení vetřelec sleduje provoz ve vaší síti a pokouší se odhalit utajované skutečnosti. Taková napadení mohou být buď v síti (vystopování komunikační linky), nebo v systému (nahrazení systémové komponenty programem typu trojský kůň, který záludně krade data). Pasivní napadení se odhaluje nejobtížněji. Musíte proto předpokládat, že někdo sleduje všechno, co po Internetu posíláte.
- **Aktivní napadení**

  Při aktivním napadení se vetřelec pokouší porušit vaši obranu a proniknout do systémů vašich sítí. Existuje několik typů aktivního napadení:
  - Při **pokusech o přístup do systému** se vetřelec pokouší využít nedostatky v zabezpečení, aby získal přístup k systému klienta nebo serveru a ovládl je.
  - Při napadení typu **spoofing** se vetřelec pokouší překonat vaši obranu předstíráním, že jde o důvěryhodný systém, nebo vás nějaký uživatel přesvědčí, abyste mu poslali utajované informace.
  - Při **útocích s následkem přerušení síťových služeb** se vetřelc pokouší zasahovat do Vašich operací nebo je ukončit pomocí přesměrování provozu nebo zahlcením systému nevyžádanými daty.
  - Při **šifrovacích napadeních** se vetřelec pokouší uhodnout či ukrást Vaše hesla nebo použije specializované nástroje k pokusu o dešifrování šifrovaných dat.

Mnohovrstvá obrana

Protože se potenciální rizika zabezpečení Internetu mohou vyskytnout na nejrůznějších úrovních, musíte podniknout taková bezpečnostní opatření, která zabezpečí proti riziku více obranných vrstev. Obecně by vás po připojení k Internetu nemělo překvapit, jestliže zaznamenáte pokusy o vniknutí do systému nebo útoky s následkem přerušení síťových služeb. Měli byste spíše předpokládat, že dojde k problému se zabezpečením. V důsledku toho se jako nejlepší obrana jeví promyšlený, předvídavý útok. Použití vrstveného přístupu při plánování strategie zabezpečení Internetu zajistí, že jestliže vetřelec pronikne jednou obrannou vrstvou, bude zastaven vrstvou následující.

Vaše strategie zabezpečení ochrany dat by měla zahrnovat opatření, která poskytují ochranu přes následující vrstvy modelu tradičního síťového počítačového zpracování. Obecně řečeno byste měli plánovat zabezpečení dat od těch nejzákladnějších (zabezpečení na úrovni systému) až po ta nejsložitější (zabezpečení na úrovni transakce).

Zabezpečení na úrovni systému

Opatření pro zabezpečení systému představují poslední obrannou linii proti problémům s bezpečností v síti Internet. V důsledku toho musí být vaším prvním krokem v celkové strategii zabezpečení Internetu řádná konfigurace základních nastavení zabezpečení systému.

Zabezpečení na úrovni sítě

Opatření pro zabezpečení sítě kontrolují přístup k Vašemu operačnímu systému i5/OS a k ostatním síťovým systémům. Když připojíte síť k Internetu, měli byste se ujistit, že máte odpovídající opatření pro zabezpečení na úrovni sítě k ochraně vašich interních prostředků v síti před neoprávněným přístupem a vniknutím. Nejběžnějším prostředkem pro zajištění bezpečnosti sítě je ochranná bariéra. Poskytovatel služeb sítě Internet (ISP) může představovat důležitý prvek v plánu zabezpečení vaší sítě. Vaše schéma zabezpečení sítě by mělo vymezit, jaká bezpečnostní opatření Váš poskytovatel služeb sítě Internet (ISP) poskytuje, například pravidla filtrování pro směrovač ISP a opatření pro služby jmen domény (DNS).

Zabezpečení na úrovni aplikace

Opatření pro zabezpečení na úrovni aplikace řídí, jak mohou uživatelé se specifickými aplikacemi zacházet. Obecně byste měli konfigurovat nastavení zabezpečení u každé aplikace, kterou používáte. Zvláštní péči byste však měli věnovat nastavení zabezpečení dat u těch aplikací a služeb, které budete na Internetu využívat nebo do něj poskytovat. Takové aplikace a služby jsou citlivé na zneužití ze strany neoprávněných uživatelů hledajících způsob, jak získat přístup do systémů vaší sítě. Opatření pro zabezpečení dat, která se rozhodnete použít, musí pokrýt ohrožení na straně serveru i na straně klienta.

Zabezpečení na úrovni přenosu

Opatření zabezpečení na úrovni přenosu ochraňuje datové komunikace uvnitř sítě a mezi sítěmi. Při komunikaci v nedůvěryhodné síti, jakou je Internet, nemůžete ovládat postup provozu ze zdroje na místo určení. Váš provoz a přenášená data postupují přes mnoho různých serverů, které nemůžete ovládat. Pokud nenastavíte opatření pro zabezpečení dat, jako například konfigurování vlastních aplikací tak, aby používaly SSL (Secure Sockets Layer), bude si vaše směrovaná data moci kdokoliv prohlédnout a použít. Opatření pro zabezpečení dat na úrovni přenosu chrání vaše data, když procházejí mezi hranicemi další úrovně zabezpečení.

Při vývoji celkové strategie zabezpečení ochrany dat v síti Internet byste měli vyvinout strategii pro každou vrstvu jednotlivě. A kromě toho byste měli popsat, jaká bude interakce jedné strategické sady s ostatními, aby poskytovala úplnou bezpečnostní síť pro vaše podnikání.

Související pojmy

“Úrovně zabezpečení systému v rámci základní přípravy na připojení k Internetu” na stránce 9
Než se připojíte k Internetu, měli byste se rozhodnout, jakou úroveň zabezpečení potřebujete pro ochranu Vašeho systému.

“Volby zabezpečení sítě” na stránce 10
Zvolte si opatření odpovídající úrovně zabezpečení k ochraně svých interních prostředků.

“Volby zabezpečení aplikací” na stránce 15
Máte několik možností, jak zvládat rizika zabezpečení pro mnoho oblíbených aplikací a služeb Internetu.

“Volby zabezpečení přenosu dat” na stránce 21
Chcete-li chránit svá data při jejich přenosu přes nedůvěryhodnou síť, měli byste přijmout náležitá bezpečnostní opatření. Tato opatření zahrnují připojení pomocí SSL, produkt System i Access for Windows a připojení VPN.

“Strategie a cíle zabezpečení ochrany dat”
Vaše strategie zabezpečení definuje, co chcete chránit, a cíle zabezpečení jsou to, co očekáváte od uživatelů.

“Zabezpečení elektronické pošty” na stránce 18
Použití elektronické pošty v síti Internet nebo v jiné nedůvěryhodné síti představuje bezpečnostní riziko pro Váš systém, a to i pokud je chráněn ochrannou bariérou.

Související odkazy


Příručka zabezpečení produktu System i operačního systému IBM i5/OS verze 5 vydání 4

Strategie a cíle zabezpečení ochrany dat

Vaše strategie zabezpečení definuje, co chcete chránit, a cíle zabezpečení jsou to, co očekáváte od uživatelů.

Vaše strategie zabezpečení ochrany dat

Každá služba Internetu, kterou používáte nebo poskytujete, znamená riziko pro Váš systém a pro síť, k níž je připojen. Strategie zabezpečení ochrany dat je sada pravidel, která se používají u činností týkajících se počítačových a komunikačních prostředků organizace. Tato pravidla se týkají oblastí, jako je například fyzické zabezpečení, zabezpečení dat zaměstnanců, zabezpečení administrativních dat a zabezpečení sítě.

Vaše strategie zabezpečení definuje, co chcete chránit a co očekáváte od uživatelů Vašeho systému. Je základem plánu pro zabezpečení ochrany dat při navrhování nových aplikací nebo rozšiřování vaší stávající sítě. Popisuje odpovědnost uživatelů, jako například ochranu důvěrných informací a vytváření složitých hesel. Vaše strategie zabezpečení ochrany dat by měla také popsat, jak budete efektivitu bezpečnostních opatření monitorovat. Takové monitorování Vám pomůže určit, zda by se někdo mohl pokusit obejít Vaše bezpečnostní opatření.

Při vyvíjení strategie zabezpečení ochrany dat musíte jasně definovat její cíle. Poté, co vytvoříte strategii zabezpečení, je třeba podniknout kroky, jimiž se pravidla v ní obsažená budou realizovat.Mezi ně patří školení zaměstnanců a dodání softwaru a hardwaru, s jejichž pomocí se pravidla uplatní. Když provádíte změny v počítačovém prostředí, měli byste také aktualizovat strategii zabezpečení ochrany dat. Tím zajistíte, že postihnete veškerá nová rizika, která z těchto změn mohou vyplynout.

Úkoly vašeho zabezpečení ochrany dat

Když vytváříte a realizujete strategii zabezpečení ochrany dat, musíte mít jasný cíl. Cíle zabezpečení spadají do jedné či více z následujících kategorií:

ochrana prostředků
: Plán ochrany prostředků zajistí, aby přístup k objektům v systému měli pouze oprávnění uživatelé. Síla produktu System i spočívá ve schopnosti zabezpečit všechny typy systémových prostředků. Měli byste pečlivě definovat různé kategorie uživatelů, kteří mohou mít přístup do vašeho systému. Rovněž byste měli definovat, jaká přístupová oprávnění chcete dát těmto skupinám uživatelů jako součást strategie zabezpečení ochrany dat.

autentizace
: Zabezpečení nebo ověření, že prostředek (člověk nebo systém) na druhém konci relace je skutečně tím, zač se vydává. Plné prokázání pravosti brání systém proti riziku, kdy se odesílatel nebo přijímající vydává za někoho jiného a používá falešnou identitu, aby získal přístup k systému. Tradičně používaly systémy pro autentizaci heslo a jméno uživatele; digitální certifikáty mohou nabídnout bezpečnější metodu autentizace a přitom poskytují pro zabezpečení ještě další výhody. Když připojíte systém k veřejné síti jakou je Internet, nabývá autentizace uživatele nových rozměrů. Důležitý rozdíl Internetem a vnitropodnikovou sítí (intranet) je vaše schopnost důvěřovat identitě uživatele, který se do systému přihlásí. V důsledku toho byste měli vážně uvažovat o použití účinnějších metod autentizace, než nabízejí tradiční procedury přihlášení pomocí hesla a jména uživatele. Ověření uživatelé mohou mít různé typy povolení v závislosti na úrovni jejich oprávnění.

oprávnění
: Zabezpečení, aby osoba nebo počítač na druhém konci relace měla povolení provést požadavek. Oprávnění je proces určení, kdo nebo co může mít přístup k systémovým prostředkům nebo provádět v systému jisté činnosti. Kontrola oprávnění se obvykle provádí v kontextu autentizace.

integrita
: Zabezpečení toho, aby přicházející informace byly stejné jako odesílané. Chcete-li pochopit integritu, musíte porozumět pojmům integrita dat a integrita systému.

- **Integrita dat**: Data jsou chráněna před neoprávněnými změnami nebo zfalšováním. Integrita dat chrání před bezpečnostním rizikem manipulace, kdy někdo zachytí a změní informace, ke kterým nemá oprávnění. Kromě ochrany dat, která jsou uložena ve Vaší síti, budete možná potřebovat dodatečné zabezpečení k zachování integrity dat vstupujících do Vašeho systému z nedůvěryhodných zdrojů. Pokud data vstupující do Vašeho systému pocházejí z veřejné sítě, potřebujete metody zabezpečnení, abyste mohli provést následující úkoly:
  - Ochránit data před ″čmuchánim″ a interpretací, nejčastěji pomocí jejich zašifrování.
  - Zajistit, aby přenos nebyl pozměněn (integrita dat).

– Prokázat, že k přenosu došlo (neodmítání). V budoucnosti budete možná potřebovat elektronický ekvivalent doporučené nebo úředně kontrolované pošty.

- **Integrita systému**: Váš systém poskytuje konzistentní a očekávané výsledky a očekávaný výkon. V operačním systému i5/OS je integrita systému nejčastěji přehlíženou komponentou zabezpečení ochrany dat, protože je základní součástí architektury operačního systému i5/OS. Architektura operačního systému i5/OS například vetřelcům nesmírně ztěžuje napodobení nebo změnu programu operačního systému, pokud používáte úroveň zabezpečení 40 nebo 50.

Neodmítání

Důkaz toho, že transakce proběhla nebo že jste odeslali nebo přijali zprávu. Použití digitálních certifikátů a šifrování pomocí veřejného klíče k podpisu transakcí, zpráv a dokumentů podporuje neodmítání. Odesílatel i příjemce souhlasí, že k výměně došlo. Digitální podpis u dat poskytuje nezbytný důkaz.

Důvěrnost

Zabezpečení, aby citlivé informace zůstaly soukromé a nebyly viditelné slídilům. Důvěrnost je nanejvýš důležitá pro celkové zabezpečení dat. Zašifrování dat pomocí digitálních certifikátů a protokolu SSL (Secure Sockets Layer) nebo připojení virtuální privátní sítě (VPN) pomáhá zajistit důvěrnost při přenosu dat přes nedůvěryhodné sítě. Strategie zabezpečení ochrany dat by se měla zabývat tím, jak zajistit důvěrnost informací nejen ve vaší síti, ale také v okamžiku, kdy vaši síť opustí.

Prověřování aktivit zabezpečení

Monitorování událostí důležitých pro zabezpečení do protokolu úspěšných i neúspěšných (odepřených) přístupů. Záznamy o úspěšném přístupu vám řeknou, kdo co ve vašich systémech dělá. Záznamy o neúspěšném přístupu vám řeknou buď to, že se někdo pokouší porušit vaše zabezpečení dat, nebo že má někdo potíže s přístupem do vašeho systému.

Související pojmy

“Produkt System i a otázky zabezpečení Internetu” na stránce 2
Bezpečnostní otázky spojené s Internetem jsou významné. Toto téma nabízí přehled silných stránek zabezpečení a možností zabezpečení operačního systému i5/OS.

“Metoda zabezpečení ochrany dat pomocí vrstvené obrany” na stránce 4
Vaše strategie zabezpečení definuje, co chcete chránit a co očekáváte od uživatelů Vašeho systému.

Konfigurace DCM

Secure Socket Layer (SSL)

“Scénář: Plán elektronického podnikání společnosti JKL Toy Company”
Typický scénář pro společnost JKL Toy, která se rozhodla rozšířit cíle svého podnikání pomocí využívání Internetu, Vám může pomoci při nastavení Vašeho vlastního plánu na elektronické obchodování.

Scénář: Plán elektronického podnikání společnosti JKL Toy Company

Typický scénář pro společnost JKL Toy, která se rozhodla rozšířit cíle svého podnikání pomocí využívání Internetu, Vám může pomoci při nastavení Vašeho vlastního plánu na elektronické obchodování.

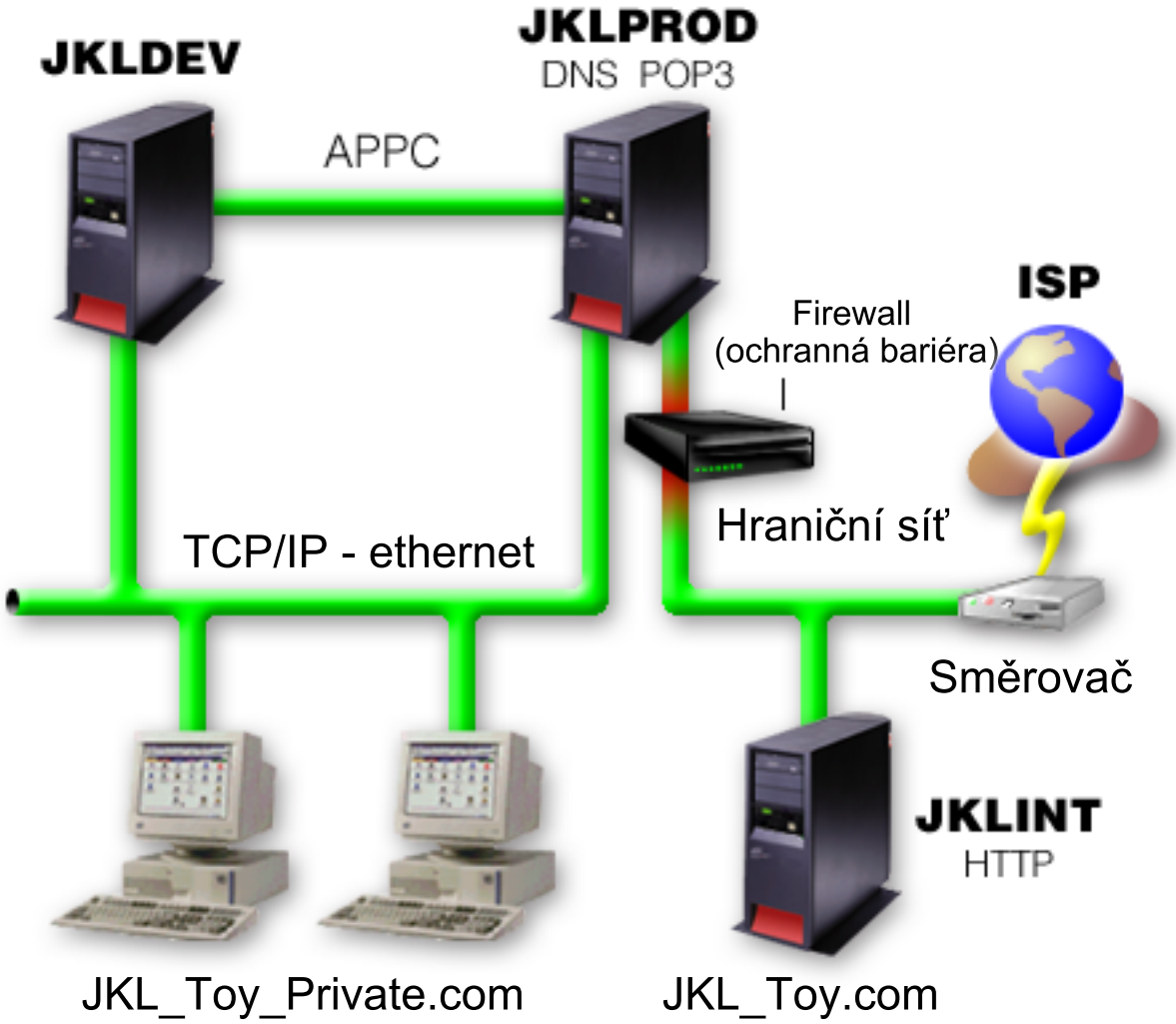
Společnost JKL Toy Company je malý, ale rychle se rozvíjející výrobce hraček. Ředitel společnosti je nadšen nárůstem obchodů a tím, jak jejich nový operační systém i5/OS snižuje zátěž spojenou s tímto růstem. Sharon Jonesová, účetní manažerka, je zodpovědná za správu a zabezpečení systému.

Firma JKL Toy úspěšně používá svou strategii zabezpečení ochrany dat interních aplikaci již více než rok. Nyní má v plánu instalovat intranet (vnitropodnikovou síť) s cílem efektivnějšího sdílení interních informací. Firma má také v plánu začít s využitím sítě Internet na podporu svých obchodních cílů. Patří mezi ně plány na vytvoření společné marketingové účasti v síti Internet, včetně online katalogu. Chtějí také používat Internet k přenosu citlivých informací ze vzdálených počítačů do společné kanceláře. Kromě toho chce společnost umožnit zaměstnancům ve vývojové laboratoři přístup k síti Internet za účelem výzkumu a vývoje. Nakonec chce společnost umožnit zákazníkům používání svých webových stránek k přímému nákupu po síti. Sharon pracuje na zprávě o specifických potenciálních rizicích těchto aktivit a o tom, jaká bezpečnostní opatření by měla společnost podniknout, aby tato rizika minimalizovala. Sharon je zodpovědná za aktualizaci strategie zabezpečení společnosti a za implementaci bezpečnostních opatření, která se společnost rozhodne využívat.

Zvýšená přítomnost v síti Internet má tyto cíle:

- Propagovat obecný obraz a přítomnost společnosti jako součást marketingové kampaně.
- Poskytnout zákazníkům a pracovníkům prodeje online katalog produktů.
- Zlepšit služby zákazníkům.
- Poskytnout zaměstnancům elektronickou poštu a přístup do sítě World Wide Web.

Jakmile společnost JKL Toy zajistila silné základní zabezpečení svého systému, rozhodla se zakoupit a používat produkt ochranné bariéry k zajištění zabezpečení na úrovni sítě. Ochranná bariéra ochrání její interní síť před rizikem spojeným s používáním sítě Internet. Následující obrázek ukazuje konfiguraci Internetu nebo sítě této společnosti.



Jak je vidět z obrázku, společnost JKL Toy má dva primární systémy. Jeden systém používá pro aplikace vývoje (JKLDEV) a druhý pro výrobní aplikace (JKLPROD). Oba systémy pracují s životně důležitými daty a aplikacemi. V důsledku toho společnosti příliš nevyhovuje spouštět v těchto systémech internetové aplikace. Společnost se proto rozhodla přidat další systém (JKLINT) pro provoz těchto aplikací.

Společnost umístila nový systém do hraniční sítě a používá ochrannou bariéru mezi ní a svou hlavní interní sítí, aby zajistila lepší oddělování mezi vlastní sítí a sítí Internet. Takové oddělení snižuje riziko plynoucí z používání Internetu, vůči kterému jsou interní systémy zranitelné. Vymezením nového systému jako výlučně internetového serveru společnost rovněž zjednodušila správu svého zabezpečení sítě.

Společnost v tuto chvíli nebude na novém systému provozovat žádné životně důležité aplikace. V této etapě plánování elektronického podnikání bude systém poskytovat pouze statickou veřejnou webovou stránku. Společnost však chce implementovat bezpečnostní opatření na ochranu systému a veřejných webových stránek, které provozuje, aby zabránila přerušení služeb a jiným možným útokům. V důsledku toho bude společnost chránit systém pravidly pro filtrování paketu a pro převod síťových adres (NAT), stejně jako výraznými základními bezpečnostními opatřeními.

Až společnost vyvine pokročilejší veřejné aplikace (jako například webovou stránku pro elektronický obchod nebo pro přístup k síti extranet), bude implementovat i rozsáhlejší bezpečnostní opatření.

Související pojmy

"Strategie a cíle zabezpečení ochrany dat" na stránce 5
Vaše strategie zabezpečení definuje, co chcete chránit, a cíle zabezpečení jsou to, co očekáváte od uživatelů.

"Produkt System i a otázky zabezpečení Internetu" na stránce 2
Bezpečnostní otázky spojené s Internetem jsou významné. Toto téma nabízí přehled silných stránek zabezpečení a možností zabezpečení operačního systému i5/OS.

"Volby zabezpečení sítě" na stránce 10
Zvolte si opatření odpovídající úrovně zabezpečení k ochraně svých interních prostředků.

"Volby zabezpečení přenosu dat" na stránce 21
Chcete-li chránit svá data při jejich přenosu přes nedůvěryhodnou síť, měli byste přijmout náležitá bezpečnostní opatření. Tato opatření zahrnují připojení pomocí SSL, produkt System i Access for Windows a připojení VPN.

Úrovně zabezpečení systému v rámci základní přípravy na připojení k Internetu

Než se připojíte k Internetu, měli byste se rozhodnout, jakou úroveň zabezpečení potřebujete pro ochranu Vašeho systému.

Opatření pro zabezpečení systému představují poslední obrannou linii proti problémům s bezpečností v síti Internet. Vaším prvním krokem v celkové strategii zabezpečení Internetu musí být správná konfigurace základních bezpečnostních nastavení operačního systému i5/OS. Chcete-li zajistit, aby zabezpečení vašeho systému odpovídalo minimálním požadavkům, postupujte takto:

- Nastavte úroveň zabezpečení (systémová hodnota QSECURITY) na 50. Úroveň zabezpečení 50 poskytuje nejvyšší úroveň ochrany integrity, což se velmi doporučuje pro ochranu systému v prostředí s vysokým rizikem, jakým je například síť Internet.

  Poznámka: Jestliže v současné době pracujete na nižší úrovni zabezpečení než 50, budete muset aktualizovat buď obslužné procedury, nebo vlastní aplikace. Podívejte se na Referenční informace zabezpečení produktu System i, než změníte úroveň zabezpečení na vyšší úroveň.
- Nastavte systémové hodnoty, které jsou důležité pro zabezpečení, aby vyjadřovaly alespoň taková omezení, jako doporučená nastavení. Můžete použít Průvodce zabezpečením System i Navigator ke konfiguraci doporučeného nastavení zabezpečení.
- Zajistěte, aby žádné uživatelské profily, včetně profilů dodaných od IBM, neměly předvolená hesla. Příkazem ANZDFTPWD (Analyze Default Passwords) zkontrolujete, zda máte předvolená hesla.
- K ochraně důležitých systémových prostředků použijte oprávnění k objektu. Použijte restriktivní přístup k vašemu systému. To znamená, standardně omezte všem přístup (PUBLIC *EXCLUDE) k systémovým prostředkům, jako jsou například knihovny a adresáře. Přístup k těmto vyhrazeným prostředkům povolte jen několika uživatelům. Omezení přístupu pomocí menu v prostředí sítě Internet nestačí.
- V systému nastavte oprávnění k objektu.

Konfiguraci těchto minimálních požadavků na zabezpečení systému vám může usnadnit buď program eServer Security Planner nebo Průvodce zabezpečením, který je dostupný v rozhraní produktu System i Navigator. Program Security Planner vám poskytne mnohá doporučení k zabezpečení dat na základě vašich odpovědí na řadu otázek. Tato

doporučení můžete použít při konfiguraci těch nastavení zabezpečení systému, která potřebujete. Na rozdíl od programu Security Planner používá Průvodce zabezpečením doporučení k tomu, aby sám provedl konfiguraci nastavení zabezpečení Vašeho systému.

Inherentní funkce zabezpečení operačního systému i5/OS, pokud jsou správně nakonfigorovány, Vám umožňují minimalizovat mnohá rizika. Avšak když připojíte svůj systém k Internetu, budete muset přijmout dodatečná bezpečnostní opatření k zajištění bezpečnosti své interní sítě. Jakmile zajistíte, že máte vytvořeno všeobecné zabezpečení systému, jste připraveni konfigurovat dodatečná opatření zabezpečení jako součást Vašeho celkového plánu zabezpečení pro používání Internetu.

Související pojmy

"Metoda zabezpečení ochrany dat pomocí vrstvené obrany" na stránce 4
Vaše strategie zabezpečení definuje, co chcete chránit a co očekáváte od uživatelů Vašeho systému.

Související odkazy

Systémová hodnota úrovně zabezpečení

Reference zabezpečení

Volby zabezpečení sítě

Zvolte si opatření odpovídající úrovně zabezpečení k ochraně svých interních prostředků.

Když se připojujete k nedůvěryhodné síti, vaše strategie zabezpečení ochrany dat musí zahrnovat úplné schéma zabezpečení ochrany dat, včetně bezpečnostních opatření, která budete implementovat na úrovni sítě. Instalace ochranné bariéry je nejlepším prostředkem pro rozmístění vyčerpávajících bezpečnostních opatření.

Poskytovatel služeb sítě Internet (ISP) může představovat důležitý prvek v plánu zabezpečení vaší sítě. Schéma zabezpečení sítě by mělo vymezit, jaká bezpečnostní opatření zajistí poskytovatel služeb sítě Internet (ISP), například pravidla pro připojení směrovače ISP a opatření pro služby jmen domény (DNS).

I když ochranná bariéra představuje ve vašem celkovém plánu jednu z hlavních obranných linií, neměla by zůstat jedinou linií obrany. Protože se potenciální rizika zabezpečení Internetu mohou vyskytnout na nejrůznějších úrovních, musíte podniknout taková bezpečnostní opatření, která zabezpečí proti riziku více obranných vrstev.

Zvažte použití některého z produktů ochranné bariéry jako své hlavní obranné linie, kdykoli připojujete svůj systém nebo svou interní síť k Internetu nebo k jiné nedůvěryhodné síti. Ačkoli produkt IBM Firewall for the i5/OS již nelze zakoupit a ani podpora pro tento produkt již není dostupná, existuje mnoho jiných produktů, které můžete používat.

Vzhledem k tomu, že komerční produkty ochranných bariér poskytují celé spektrum technologií pro zabezpečení sítě, společnost JKL Toy si vybrala jednu z nich pro ochranu své sítě. Jelikož ochranná bariéra, kterou si společnost vybrala, nechrání její operační systém, přidala společnost dodatečnou funkci zabezpečení, která vychází z použití pravidel paketů operačního systému i5/OS. To společnosti umožní vytvořit pravidla pro filtrování a NAT k řízení provozu na internetovém serveru.

Související pojmy

"Metoda zabezpečení ochrany dat pomocí vrstvené obrany" na stránce 4
Vaše strategie zabezpečení definuje, co chcete chránit a co očekáváte od uživatelů Vašeho systému.

"Scénář: Plán elektronického podnikání společnosti JKL Toy Company" na stránce 7
Typický scénář pro společnost JKL Toy, která se rozhodla rozšířit cíle svého podnikání pomocí využívání Internetu, Vám může pomoci při nastavení Vašeho vlastního plánu na elektronické obchodování.

Detekce vniknutí

Související informace

Červená kniha: Vše, co potřebujete vědět při migraci z produktu IBM Firewall for AS/400

Ochranná bariéra

Ochranná bariéra je blokáda mezi zabezpečenou sítí a nedůvěryhodnou sítí, jakou je například Internet.

Většina společností používá ochrannou bariéru k bezpečnému připojení interní sítě k Internetu, i když ji lze použít také k zabezpečení jedné interní sítě před druhou.

Ochranná bariéra poskytuje jediný řízený bod kontaktu mezi vaší zabezpečenou interní sítí a nedůvěryhodnou sítí, nazývaný *chokepoint*. Funkce ochranné bariéry jsou následující:

- Dovoluje uživatelům vaší interní sítě používat povolené prostředky nacházející se ve vnější síti.
- Zabraňuje neoprávněným uživatelům z vnější sítě používat prostředky ve vaší interní síti.

Když používáte ochrannou bariéru jako bránu do sítě Internet (nebo do jiné sítě), podstatně snižujete riziko hrozící interní síti. Použití ochranné bariéry usnadňuje i správu zabezpečení sítě, protože její funkce provádějí mnoho direktiv vaší strategie zabezpečení ochrany dat.

Jak pracuje ochranná bariéra

Chcete-li pochopit, jak ochranná bariéra funguje, představte si, že vaše síť je budova a vy řídíte přístup do ní. Budova má halu jako jediný vstupní bod. V této hale jsou recepční, kteří hosty vítají, bezpečnostní služba, která na ně dává pozor, videokamery pro zaznamenání jejich chování a čtecí zařízení pro propustky, a ti všichni prověřují návštěvníky vstupující do budovy.

Tato opatření mohou dobře fungovat při kontrole přístupu do budovy. Když se ale neoprávněné osobě podaří do ní vstoupit, neexistuje způsob, jak budovu před jednáním vetřelce ochránit. Jestliže však budete jeho pohyb monitorovat, máte šanci případné podezřelé jednání vetřelce odhalit.

Komponenty ochranné bariéry

Ochranná bariéra je kolekce hardwaru a softwaru, které, jsou-li použity společně, zabraňují neoprávněnému přístupu do části sítě. Bariéra se skládá z následujících komponent:

- **Hardware**

  Hardware ochranné bariéry obvykle tvoří samostatný počítač nebo zařízení vyhrazené k provádění softwarových funkcí ochranné bariéry.
- **Software**

  Software ochranné bariéry nabízí celou řadu aplikací. V kontextu zabezpečení sítě poskytuje ochranná bariéra prostřednictvím různých technologií tyto bezpečnostní kontroly:
  - IP pakety, filtrování.
  - Služby NAT (převod síťových adres).
  - Server SOCKS.
  - Servery proxy pro nejrůznější služby, jako například HTTP, Telnet, FTP, atd.
  - Služby přenosu pošty.
  - Rozdělení DNS.
  - Protokolování.
  - Monitorování v reálném čase.

  Poznámka: Některé ochranné bariéry poskytují služby VPN tak, že můžete vytvořit zašifrované relace mezi vaší ochrannou bariérou a jinými kompatibilními bariérami.

Použití technologií ochranné bariéry

Pomocí serverů proxy, serveru SOCKS nebo pravidel NAT ochranné bariéry můžete interním uživatelům poskytnout bezpečný přístup k službám sítě Internet. Server proxy a server SOCKS přeruší spojení TCP/IP u ochranné bariéry, aby skryly síťové informace před nedůvěryhodnou sítí. Servery také poskytují další možnosti protokolování.

Pomocí NAT můžete uživatelům Internetu poskytnout snadný přístup k veřejnému serveru za ochrannou bariérou. Ochranná bariéra přesto vaši síť ochrání, protože NAT skryje interní IP adresy.

Ochranná bariéra může také ochránit interní informace tím, že poskytne server DNS, který může sama používat. Ve skutečnosti máte dva servery DNS: jeden používáte pro data o interní síti a druhý je v ochranné bariéře pro data o externích sítích a o samotné bariéře. To vám umožňuje řídit vnější přístup k informacím o vašich interních systémech.

Když definujete strategii vaší ochranné bariéry, můžete se domnívat, že postačí zakázat všechno, co představuje riziko pro organizaci, a všechno ostatní povolit. Počítačoví zločinci však neustále vytvářejí nové metody napadení, a proto musíte předvídat, jak takovým útokům předejít. Jako v příkladu o budově budete také muset sledovat, zda někdo nějakým způsobem nenapadl vaši obranu. Obecně řečeno je mnohem nákladnější zotavit se ze škod z napadení systému, než útoku předejít.

V případě ochranné bariéry je nejlepší strategií povolit pouze ty aplikace, které jste otestovali a kterým důvěřujete. Budete-li se držet této strategie, musíte vyčerpávajícím způsobem definovat seznam služeb, které ochranná bariéra musí poskytovat. Každou službu můžete charakterizovat směrem spojení (zevnitř ven nebo zvenčí dovnitř). Měli byste také vytvořit seznam uživatelů, kterým poskytnete oprávnění k používání jednotlivých služeb a počítače, které mohou zajistit připojení pro tyto služby.

Jak může ochranná bariéra ochránit vaši síť

Ochrannou bariéru instalujete mezi vaši síť a bod připojení k Internetu (nebo jiné nedůvěryhodné síti). Tak můžete omezit vstupní body do vaší sítě. Ochranná bariéra poskytuje jediný styčný bod mezi vaší sítí a sítí Internet, nazývaný chokepoint. Protože máte jediný styčný bod, máte větší kontrolu nad tím, jakému provozu povolíte vstup do sítě a výstup z ní.

Ochranná bariéra se veřejnosti jeví jako jediná adresa. Poskytuje přístup do nedůvěryhodné sítě přes server proxy, server SOCKS nebo službu NAT (převod síťových adres) a přitom skryje interní síťové adresy. V důsledku toho udržuje ochranná bariéra soukromí vaší interní sítě. To, že ochranná bariéra udržuje informace o vaší síti jako soukromé, představuje jeden ze způsobů ochrany, jež činí útok pomocí vydávání se za někoho jiného (tzv. spoofing) méně pravděpodobným.

Ochranná bariéra vám umožňuje řídit provoz do a ze sítě a minimalizovat tak riziko jejího napadení. Bezpečně filtruje veškerý provoz, který vstupuje do vaší sítě tak, že mohou vstoupit jen určité typy provozu pro určitá místa určení. To minimalizuje riziko, že by někdo mohl použít Telnet nebo protokol FTP k získání přístupu k vašim interním systémům.

Co ochranná bariéra pro ochranu vaší sítě nemůže udělat

Ačkoli ochranná bariéra představuje obrovské zabezpečení proti určitým typům napadení, je jen jednou ze součástí celkového řešení vaší bezpečnosti. Ochranná bariéra nemusí například vždy ochránit data, která odesíláte přes Internet pomocí takových aplikací, jako je například pošta SMTP, FTP a Telnet. Pokud se nerozhodnete tato data zašifrovat, může k nim kdokoliv na Internetu získat přístup, když putují na místo určení.

Pravidla paketu operačního systému i5/OS

Můžete používat pravidla paketu operačního systému i5/OS k ochraně svého systému. Pravidla paketu jsou funkce operačního systémui5/OS a jsou přístupná z rozhraní produktu System i Navigator.

Můžete použít pravidla paketu pro konfiguraci dvou základních technologií zabezpečení sítě, abyte mohli řídit provoz protokolu TCP/IP:

- převod síťových adres (NAT)
- filtrování IP paketů

Protože NAT a filtrování IP jsou nedílnými částmi operačního systému i5/OS, poskytují hospodárný způsob zabezpečení systému. V některých případech mohou tyto bezpečnostní technologie obstarat všechno, co potřebujete a nemusíte nic dalšího kupovat. Tyto technologie však nevytvářejí opravdovou funkční ochrannou bariéru. Zabezpečení IP paketů můžete použít samostatně nebo ve spojení s ochrannou bariérou podle požadavků a cílů vaší ochrany.

Poznámka: Zabezpečení vašeho systému by mělo mít přednost před náklady. Chcete-li pro váš provozní systém zajistit maximální možnou ochranu, měli byste uvažovat o použití ochranné bariéry.

Služby NAT (převod síťových adres) a filtrování IP.

Převod síťových adres (NAT) změní zdrojové nebo cílové IP adresy paketů, které procházejí systémem. NAT nabízí transparentnější alternativu serverů proxy a serverů SOCKS ochranné bariéry. NAT také může zjednodušit konfiguraci sítě, protože povoluje vzájemně spojit sítě s nekompatibilním členěním adresování. V důsledku toho můžete použít pravidla NAT tak, aby operační systém i5/OS vystupoval jako brána mezi dvěma sítěmi, které mají konfliktní nebo nekompatibilní schémata adresování. NAT je také možné použít pro ukrytí skutečných IP adres jedné sítě tak, že dynamicky nahradíte jednu nebo více reálných adres. Vzhledem k tomu, že se funkce filtrování IP paketu a NAT vzájemně doplňují, budete je často používat společně za účelem lepšího zabezpečení sítě.

Použití NAT může také zjednodušit provoz veřejného webového serveru za ochrannou bariérou. Veřejné IP adresy pro webový server se převádějí na soukromé interní IP adresy. To snižuje počet registrovaných IP adres, které jsou zapotřebí, a minimalizuje dopad na stávající síť. Poskytuje také mechanismus, aby interní uživatelé měli přístup k Internetu a přitom skryli soukromé interní IP adresy.

Filtrování IP paketů nabízí schopnost selektivně zablokovat nebo ochránit provoz IP na základě informací v záhlaví paketů. K rychlému a snadnému nakonfigurování základních filtrovacích pravidel pro zablokování nežádoucího provozu v síti můžete použít průvodce Internet Setup Wizard v aplikaci System i Navigator.

Filtrování IP paketu můžete použít k těmto účelům:

- Vytvořit sadu filtrovacích pravidel k zadání, kterým IP paketům povolit a kterým odepřít přístup do vaší sítě. Když vytváříte filtrovací pravidla, aplikujete je na fyzické rozhraní (například Token-Ring nebo linku typu Ethernet). Pravidla můžete aplikovat na několik fyzických rozhraní nebo můžete u každého rozhraní použít jiná pravidla.
- Vytvořit pravidla, která buď povolí, nebo zamítnou specifické pakety a která jsou založena na následujících informacích záhlaví:
  - IP adresa místa určení.
  - Protokol IP adresy zdrojového systému (například TCP, UDP a tak dále).
  - Port místa určení (například HTTP má port 80).
  - Port zdroje.
  - Směr IP datagramu (příchozí nebo odchozí).
  - Směrováno nebo lokální.
- Předejít tomu, aby nežádoucí nebo zbytečný provoz dosáhl aplikací v systému. Můžete také zabránit směrování provozu do jiných systémů. To zahrnuje pakety ICMP nižší úrovně (například pakety PING), pro které není zapotřebí žádný specifický aplikační server.
- Specifikovat, zda filtrovací pravidlo vytvoří záznam v protokolu systémového žurnálu o paketech, které pravidlu odpovídají. Jakmile se informace zapíší do systémového žurnálu, nemůžete již záznam v protokolu změnit. Protokol je ideálním nástrojem pro prověřování aktivity sítě.

Pravidla pro filtrování paketu umožňují chránit počítačové systémy odmítnutím nebo přijetím IP paketů podle kritérií, která definujete. Pravidla pro převod síťových adres (NAT) vám umožní skrýt interní systémové informace před externími uživateli nahrazením jedné IP adresy jinou, veřejnou IP adresou. Přestože pravidla pro filtry IP paketu a NAT představují jádro technologií pro zabezpečení sítě, neposkytují stejnou úroveň zabezpečení jako plně funkční ochranná

bariéra (firewall). Při rozhodování mezi kompletním produktem ochranné bariéry a funkcí pravidel paketu operačního systému i5/OS byste měli pečlivě analyzovat požadavky a cíle svého zabezpečení dat.

Související pojmy

Převod síťových adres (NAT)

Filtrování IP paketů

Detekce vniknutí

Detekce vniknutí zahrnuje shromažďování informací o pokusech o neoprávněný přístup a útocích přicházejících přes síť TCP/IP. Vaše celkové zásady zabezpečení budou mít oddělení věnované detekci vniknutí.

Termín *detekce vniknutí* je v dokumentaci operačního systému i5/OS používán ve dvojím smyslu. V prvním smyslu znamená detekce vniknutí prevenci a detekci ohrožení zabezpečení. Vetřelec se například může pokoušet proniknout do systému pomocí neplatného uživatelského ID, nebo může nezkušený uživatel, který má příliš mnoho oprávnění, měnit důležité objekty v knihovnách systému.

Ve druhém smyslu znamená detekce vniknutí novou funkci detekce vniknutí, která využívá zásady k monitorování podezřelého provozu v systému. Můžete nastavit zásady detekce vniknutí, které budou monitorovat události podezřelých vniknutí, která byla provedena prostřednictvím TCP/IP sítě.

Výběr voleb zabezpečení sítě v operačním systému i5/OS

Měli byste provést volbu zabezpečení sítě v souladu se svými plány zabezpečnení Internetu.

Řešení zabezpečení sítě, která chrání před neoprávněným přístupem, obvykle spoléhají na technologie ochranné bariéry. K ochraně svého systému můžete použít produkt plně funkční ochranné bariéry nebo specifické technologie zabezpečení sítě jako součást implementace protokolu TCP/IP v operačním systému i5/OS. Tato implementace sestává z funkce pravidel paketu (což zahrnuje filtrování IP a NAT) a z HTTP pro operační systém i5/OS, což je licencovaný program serveru proxy.

Volba mezi použitím funkce pravidel paketů nebo ochranné bariéry záleží na prostředí vaší sítě, přístupových požadavcích a potřebách zabezpečení. Měli byste uvažovat o použití některého z produktů ochranné bariéry jako své hlavní obranné linie, kdykoli připojujete svůj systém nebo svou interní síť k Internetu nebo k jiné nedůvěryhodné síti.

Ochranná bariéra je v tomto případě vhodnější, protože je to typicky jednoúčelové hardwarové a softwarové zařízení s omezeným počtem rozhraní pro externí přístup. Pokud používáte technologie protokolu TCP/IP pro operační systém i5/OS k ochraně přístupu k Internetu, využíváte obecnou počítačovou platfomu s myriádami rozhraní a aplikací otevřených přístupu zvenčí.

Poznámka: Možná se rozhodnete využívat jak ochrannou bariéru, tak i integrované technologie zabezpečení sítě operačního systému i5/OS. To Vám pomůže chránit systém před vnitřními útoky (z oblasti za ochrannou bariérou) a všemi útoky, které mohou Vaši ochrannou bariéru porušit kvůli špatné konfiguraci nebo z jiných důvodů.

Tento rozdíl je důležitý z mnoha důvodů. Produkt jednoúčelové ochranné bariéry například neposkytuje žádné další funkce ani aplikace mimo ty, které patří k samotné bariéře. Proto i kdyby vetřelec ochrannou bariéru úspěšně obešel a získal k ní přístup, nemohl by toho moc udělat. Naopak pokud by vetřelec obešel funkce zabezpečení TCP/IP na Vašem systému, mohl by potenciálně získat přístup k různým užitečným aplikacím, službám a datům. Vetřelec je pak může využít ke zničení samotného systému nebo ke získání přístupu k dalším systémům ve Vaší interní síti.

Jako u každého rozhodování ve věcech ochrany musíte svá rozhodnutí založit na poměru získaného prospěchu vůči nákladům, které jste ochotni vynaložit. Musíte analyzovat své obchodní cíle a rozhodnout se, která rizika jste ochotni přijmout v poměru k nákladům, které chcete vynaložit na zabezpečení s cílem tato rizika minimalizovat. Následující tabulka nabízí informace o tom, kdy je odpovídající použít funkce zabezpečení dat TCP/IP oproti plně funkčnímu zařízení ochranné bariéry. Tuto tabulku můžete využít k určení, zda potřebujete k zajištění zabezpečení sítě a ochrany systému používat ochrannou bariéru, funkce zabezpečení protokolu TCP/IP nebo kombinaci obojího.

Technologie zabezpečení ochrany dat	Nejlepší použití technologie TCP/IP systému i5/OS	Nejlepší použití plně funkční ochranné bariéry
Filtrování IP paketů	• Poskytnutí dodatečné ochrany pro jediný operační systém i5/OS, jako je například veřejný webový server nebo intranetový systém s citlivými daty. • Chránit dílčí síť společného intranetu, přičemž operační systém i5/OS působí jako brána (příležitostný směrovač) do zbývající části sítě. • Řídit komunikaci s ne zcela důvěryhodným partnerem přes soukromou síť nebo extranet, přičemž operační systém i5/OS působí jako brána.	• Ochrana celé společné sítě proti síti Internet nebo jiné nedůvěryhodné síti, ke které je vaše síť připojena. • Ochrana velké dílčí sítě před hustým provozem ze zbývající části společné sítě.
NAT (převod síťových adres)	• Umožnění spojení dvou soukromých sítí s nekompatibilní strukturou adresování. • Skrytí adres dílčí sítě před méně důvěryhodnou sítí.	• Skrytí adres klientů přistupujících k síti Internet nebo jiné nedůvěryhodné síti. Použití jako alternativy k serverům proxy a SOCKS. • Zpřístupnění služeb určitého systému v soukromé síti klientům v síti Internet.
Server proxy	• Fungovat jako server proxy ve vzdálených systémech ve společné síti, přičemž centrální ochranná bariéra poskytuje přístup k síti Internet.	• Fungování jako server proxy pro celou společnou síť při přístupu k síti Internet.

Související odkazy

Filtrování IP a převod síťové adresy

HTTP Server pro operační systém i5/OS

Související informace

Internetové scénáře AS/400: Praktický přístup

Volby zabezpečení aplikací

Máte několik možností, jak zvládat rizika zabezpečení pro mnoho oblíbených aplikací a služeb Internetu.

Opatření pro zabezpečení na úrovni aplikace řídí, jak mohou uživatelé se specifickými aplikacemi zacházet. Obecně řečeno musíte nakonfigurovat nastavení zabezpečení pro každou aplikaci, kterou používáte. Zvláštní péči byste však měli věnovat nastavení zabezpečení dat u těch aplikací a služeb, které budete na Internetu využívat nebo do něj poskytovat. Takové aplikace a služby jsou citlivé na zneužití ze strany neoprávněných uživatelů hledajících způsob, jak získat přístup do systémů vaší sítě. Opatření pro zabezpečení dat, která se rozhodnete použít, musí pokrýt ohrožení jak na straně serveru, tak i na straně klienta.

I když zabezpečení každé aplikace, kterou používáte, je důležité, bezpečnostní opatření jsou pouze malou částí implementace Vašich celkových zásad zabezpečení.

Související pojmy

“Metoda zabezpečení ochrany dat pomocí vrstvené obrany” na stránce 4

Vaše strategie zabezpečení definuje, co chcete chránit a co očekáváte od uživatelů Vašeho systému.

Zabezpečení webových služeb

Když poskytujete návštěvníkům přístup ke svým webovým stránkám, neodhalujte jim informace o tom, jak jsou vaše stránky nastaveny a jaké kódování je použito k jejich vygenerování. Návštěva Vašich stránek pro ně musí být snadná, rychlá a bezproblémová, přičemž veškerá práce musí být vykonána skrytě.

Jako administrátor musíte zajistit, aby zvolené metody zabezpečení negativně neovlivňovaly vaše webové stránky a aby implementovaly Vámi zvolené modely zabezpečení. Abyste toho dosáhli, musíte zvolit mezi funkcemi zabezpečení vestavěnými v produktu IBM HTTP Server for i5/OS.

Kapitola o implementaci zabezpečení červené knihy k produktu IBM HTTP Server (provozovanému serverem Apache)

 popisuje, jak použít autentizaci, kontrolu přístupu a šifrování k implementaci funkcí zabezpečení.

Protokol HTTP (Hypertext Transfer Protocol) Vám poskytuje schopnost zobrazovat data, ale nikoli měnit data v databázových souborech. Někdy však možná budete potřebovat napsat aplikace, které musí aktualizovat databázový soubor. Například budete potřebovat vytvořit formuláře, které poté, co je uživatelé vyplní, budou aktualizovat databázi operačního systému i5/OS. K tomu můžete použít programy rozhraní CGI (Common Gateway Interface).

Další zabezpečovací funkcí, kterou můžete použít, je server proxy. Ten přijímá požadavky určené pro jiné servery, a poté tyto požadavky splní, přepošle, přesměruje nebo zamítne.

Server HTTP poskytuje protokol přístupů, který můžete využít k monitorování jak přístupů, tak pokusů o přístup prostřednictvím serveru.

Kromě programů CGI můžete na svých webových stránkách používat také programovací jazyk Java. S problematikou zabezpečení dat v jazyku Java byste měli být obeznámeni dříve, než přidáte jazyk Java do svých webových stránek.

Související pojmy

"Java a zabezpečení Internetu"
Programování v Javě je v současném světě počítačového zpracování stále rozšířenější. Měli byste být připraveni zabývat se bezpečnostními faktory, které s Javou souvisí.

Související informace

Typy serverů proxy a použití pro HTTP servery (provozovaných serverem Apache)

Rady pro zabezpečení serverů HTTP

Rozhraní obecné brány

Java a zabezpečení Internetu

Programování v Javě je v současném světě počítačového zpracování stále rozšířenější. Měli byste být připraveni zabývat se bezpečnostními faktory, které s Javou souvisí.

Ačkoliv ochranná bariéra představuje dobrou ochranu před nejběžnějšími bezpečnostními riziky Internetu, nezajišťuje ochranu proti řadě rizik, které s sebou používání jazyka Java přináší. Vaše strategie zabezpečení ochrany dat by měla zahrnovat podrobné zpracování ochrany systému ve třech oblastech Javy: aplikace, applety a servlety. Také byste si měli ujasnit, jakým způsobem probíhá interakce mezi Javou a zabezpečením ochrany dat na úrovni objektů ve smyslu autentizace a autorizace u programů v Javě.

Aplikace v Javě

Jako programovací jazyk má Java některé charakteristiky, které zabraňují programátorům jazyka Java dělat neúmyslné chyby, jež by mohly vést k problémům s integritou. (Ostatní jazyky běžně používané pro PC aplikace, jako jsou C nebo C++, nechrání programátory před neúmyslnými chybami tak silně jako Java.) Java například používá ″strong typing″, přísné vymáhání pravidel zadávání, čímž je programátorovi znemožněno používat objekty nezamýšleným způsobem. Java nedovoluje práci s ukazateli, v důsledku čehož programátor nemůže nechtěně přesáhnout hranice paměti daného programu. Z hlediska vývoje aplikací lze na Javu pohlížet jako na jakýkoliv vyšší programovací jazyk. Pro navrhování

aplikací byste měli používat stejná pravidla zabezpečení, která používáte u ostatních programovacích jazyků ve Vašem systému.

Java applety

Java applety jasou malé programy v Javě, které můžete zahrnout do HTML stránek provozovaných na klientovi, které mají potenciální přístup do Vašeho operačního systému i5/OS. Rovněž program ODBC (Open Database Connectivity) nebo komunikace APPC (advanced program-to-program communications) spouštěné na určitém PC ve Vaší síti m ůže potenciálně mít přístup do Vašeho operačního systému, pokud je například Váš systém používán tak, aby sloužil aplikacím, nebo je používán jako webov ý server. Obecně mohou Java applety vytvořit relaci pouze s tím operačním systémem i5/OS, z něhož daný applet pochází. Java applet tudíž může mít přístup k Vašemu operačnímu systému i5/OS z připojeného PC pouze v případě, že příslušný applet pochází z dotyčného operačního systému i5/OS.

Applet se může pokusit připojit k libovolnému portu TCP/IP v systému. Nemusí nutně komunikovat se softwarovým serverem, který je napsán v jazyce Java. Avšak v systémech napsaných pomocí aplikace IBM Toolbox pro jazyk Java musí applet uvést uživatelské ID a heslo, když vytváří připojení zpět do systému. Všechny systémy popsané v tomto materiálu jsou operační systémy i5/OS. (Aplikační server napsaný v jazyce Java nemusí používat aplikaci IBM Toolbox for Java.) Třída IBM Toolbox for Java obyčejně vyzývá uživatele k zadání ID a hesla uživatele při prvním připojení.

Applet může plnit funkce v operačním systému i5/OS pouze pokud je uživatelský profil pro tyto funkce autorizován. Proto se dobré schéma zabezpečení dat na úrovni prostředků stává nezbytností, pokud k zajištění nových funkcí aplikace začínáte používat Java applety. Když systém zpracovává požadavky pro applety, nepoužívá hodnotu omezených schopností specifikovanou v profilu daného uživatele.

Prohlížeč appletů vám umožní testovat applet v operačním systému i5/OS. Applet však není předmětem bezpečnostních omezení prohlížeče. Proto byste měli používat prohlížeč appletů pouze k testování svých vlastních appletů a nikdy ke spouštění appletů z vnějších zdrojů. Java applety často zapisují na pevný disk PC uživatele, což jim poskytuje příležitost provádět destruktivní činnost. Vy však můžete použít digitální certifikát a s jeho pomocí Java applet podepsat, což mu vytvoří autenticitu. Podepsaný applet může zapisovat na lokální jednotky PC, třebaže to předvolené nastavení prohlížeče nedovoluje. Podepsaný applet může rovněž zapisovat na mapované jednotky na vašem systému, protože se vůči PC jeví jako lokální jednotky.

V případě Java appletů pocházejících z Vašeho systému budete možná muset používat podepsané applety. Přesto byste měli instruovat své uživatele, aby běžně nepřijímali podepsané applety z neznámých zdrojů.

Počínaje verzí V4R4 můžete používat aplikaci IBM Toolbox for Java k nastavení prostředí SSL (Secure Sockets Layer). Můžete také použít aplikaci IBM Developer Toolkit for Java a zabezpečit aplikaci napsanou v jazyce Java pomocí SSL. Použití SSL s vašimi aplikacemi v Javě zajišťuje kódování dat včetně ID a hesel uživatelů, která se předávají mezi klientem a serverem. Pomocí produktu Digital Certificate Manager můžete nakonfigurovat registrované programy v jazyce Java tak, aby používaly protokol SSL.

Java servlety

Servlety jsou komponenty na straně serveru napsané v jazyce Java, které dynamicky rozšiřují funkčnost webového serveru beze změny kódu webového serveru. Server IBM WebSphere Application Server, jenž je součástí serveru IBM Web Enablement for i5/OS, poskytuje podporu pro používání servletů v operačních systémech i5/OS.

U servletů, s nimiž systém pracuje, musíte použít zabezpečení ochrany dat na úrovni prostředků. I když však na servlet aplikujete zabezpečení dat na úrovni prostředků, není jeho ochrana dostačující. Když webový server stáhne servlet, nezabrání zabezpečení dat na úrovni prostředků tomu, aby tento servlet spouštěli i ostatní. Z toho vyplývá, že byste měli zabezpečení dat na úrovni prostředků používat ve spojení s ovládacími prvky a směrnicemi pro zabezpečení HTTP serveru. Například nedovolte, aby byly servlety spouštěny pouze pod profilem webového serveru. Také byste měli využívat funkcí zabezpečení ochrany dat poskytovaných vašimi nástroji pro vývoj servletů, jako jsou např. funkce v aplikac WebSphere Application Server for i5/OS.

V následujících zdrojích najdete podrobnější informace o obecných bezpečnostních opatřeních pro jazyk Java:

- IBM Developer Kit for Java: zabezpečení dat pro jazyk Java.
- IBM Toolbox for Java: Třídy zabezpečení.
- Úvahy o zabezpečení pro prohlížeče Internetu.

Autentizace a autorizace jazyka Java vůči prostředkům

Aplikace IBM Toolbox for Java obsahuje třídy zabezpečení sloužící k ověření identity uživatele a volitelně též k přiřazení této identity k vláknu operačního systému pro aplikaci nebo servlet spouštěný v operačním systému i5/OS. Následné kontroly zabezpečení dat na úrovni prostředků pak probíhají pod touto přiřazenou identitou.

Aplikace IBM Developer Kit for Java poskytuje podporu pro službu Java Authentication and Authorization Service (JAAS), která je standardním rozšířením produktu Java 2 Software Development Kit (J2SDK), Standard Edition. V současné době produkt J2SDK zajišťuje řízení přístupu založené na tom, odkud kód pochází a kdo kód podepsal (řízení přístupu na bázi zdroje kódu).

Zabezpečení Vašich aplikací v jazyce Java pomocí SSL

Můžete použít Secure Sockets Layer (SSL) k zabezpečení komunikace pro aplikace operačního systému i5/OS, které jste vyvinuli pomocí nástrojů IBM Developer Kit for Java. Výhod protokolu SSL mohou také využívat klientské aplikace, které používají nástroje IBM Toolbox for Java. Proces aktivace SSL pro vaše vlastní aplikace v jazyku Java se liší od procesu aktivace SSL pro jiné aplikace.

Související pojmy

"Zabezpečení webových služeb" na stránce 16
Když poskytujete návštěvníkům přístup ke svým webovým stránkám, neodhalujte jim informace o tom, jak jsou vaše stránky nastaveny a jaké kódování je použito k jejich vygenerování. Návštěva Vašich stránek pro ně musí být snadná, rychlá a bezproblémová, přičemž veškerá práce musí být vykonána skrytě.

Konfigurace DCM

Služby ověření

Související informace

Java Authentication and Authorization Service

SSL (Secure Sockets Layer)

Zabezpečení elektronické pošty

Použití elektronické pošty v síti Internet nebo v jiné nedůvěryhodné síti představuje bezpečnostní riziko pro Váš systém, a to i pokud je chráněn ochrannou bariérou.

Těmto rizikům musíte porozumět, abyste si byli jisti, že je vaše strategie zabezpečení ochrany dat bude minimalizovat.

Elektronická pošta se podobá jiným formám komunikace. Je velmi důležité, abyste při zasílání důvěrných informací elektronickou poštou byli uvážliví. Protože vaše elektronická pošta prochází mnoha servery, než se k vám dostane, je možné, aby ji někdo zachytil a přečetl. V důsledku toho budete asi chtít použít bezpečnostní opatření na ochranu důvěrnosti vaší elektronické pošty.

Běžná rizika zabezpečení elektronické pošty

Některá rizika spojená s použitím elektronické pošty:

- **Záplava** (typ útoku s následkem přerušení síťových služeb) nastává, když je systém přetížen mnoha zprávami elektronické pošty. Pro vetřelce je poměrně snadné vytvořit jednoduchý program, který posílá miliony zpráv elektronické pošty (včetně prázdných zpráv) na jediný poštovní server a pokouší se jej zaplavit. Bez řádného zabezpečení může na cílovém serveru nastat přerušení síťových služeb, protože se disk serveru zaplní zbytečnými zprávami. Anebo může server přestat odpovídat, protože se všechny jeho prostředky zabývají zpracováním pošty v důsledku tohoto napadení.

- **Zasílání nevyžádaných e-mailů (spamming)** je další typ napadení běžný u elektronické pošty. S rostoucím počtem podniků nabízejících elektronický obchod přes Internet jsme byli svědky exploze nežádoucí nebo nevyžádané obchodní elektronické pošty. To je zanášení zásilkami, které se posílají podle rozsáhlého distribučního seznamu uživatelů elektronické pošty a přeplňují jejich schránky.
- **Ochrana důvěrných informací** je vystavena riziku, je-li elektronická pošta zasílána jiné osobě v síti Internet. Taková pošta prochází mnoha servery, než dosáhne zamýšleného příjemce. Pokud jste zprávu nezašifrovali, může ji hacker zachytit a přečíst v kterémkoliv bodu přenosové cesty.

Volby zabezpečení elektronické pošty

Chcete-li se chránit před rizikem zaplavování a zasílání nevyžádaných e-mailů, musíte patřičně konfigurovat svůj poštovní server. Většina aplikací serveru nabízí metody, jak se s takovým napadením vypořádat. Můžete také spolupracovat se svým poskytovatelem služeb sítě Internet (ISP) a zajistit, aby i on poskytl nějakou další ochranu před těmito útoky.

To, jaká další bezpečnostní opatření potřebujete, závisí na požadované úrovni důvěrnosti a také na tom, jaké zabezpečení poskytují aplikace elektronické pošty. Je například dostačující ponechat obsah zprávy elektronické pošty jako důvěrný? Nebo chcete, aby byly důvěrné všechny informace týkající se elektronické pošty, jako například počáteční a cílové IP adresy?

V některých aplikacích jsou integrovány funkce zabezpečení dat, které mohou poskytnout potřebnou ochranu. Například produkt Lotus Notes Domino nabízí několik integrovaných funkcí zabezpečení dat včetně schopnosti šifrování celého dokumentu nebo jednotlivých polí v dokumentu.

Při šifrování pošty vytvoří produkt Lotus Notes Domino jedinečný veřejný a soukromý klíč pro každého uživatele. Pomocí soukromého klíče zprávu zašifrujete tak, aby byla čitelná jen pro ty uživatele, kteří mají váš veřejný klíč. Veřejný klíč musíte poslat zamýšleným adresátům vaší zprávy, aby jej mohli použít při jejím dešifrování. Jestliže vám někdo pošle zašifrovanou zprávu, použije produkt Lotus Notes Domino veřejný klíč odesílatele k jejímu dešifrování.

Informace o používání těchto šifrovacích funkcí produktu Notes najdete v online nápovědě k tomuto programu.

Chcete-li pro elektronickou poštu a jiné informace, které kolují mezi pobočkami, vzdálenými klienty nebo obchodními partnery, zajistit vyšší stupeň důvěrnosti, máte několik možností.

Jestliže to aplikace poštovního serveru podporuje, můžete pomocí SSL (Secure Sockets Layer) vytvořit mezi serverem a klienty elektronické pošty zabezpečenou relaci. SSL také poskytuje podporu volitelné autentizace na straně klienta, pokud je aplikace typu klient napsána tak, aby SSL používala. Vzhledem k tomu, že je celá relace zašifrovaná, zajistí SSL integritu i při přenosu dat.

Další možností je nakonfigurovat spojení VPN (virtual Private Network). Můžete použít svůj systém ke konfiguraci připojení VPN, včetně připojení mezi vzdálenými klienty a Vaším systémem. Když používáte VPN, je veškerý provoz plynoucí mezi komunikujícími koncovými body zašifrovaný, což zaručuje důvěrnost a integritu dat.

Související pojmy

“Zabezpečení protokolu FTP” na stránce 20
Protokol FTP (File Transfer Protocol) poskytuje schopnost přenosu souborů mezi klientem (uživatelem v jiném systému) a vaším serverem. Měli byste porozumět bezpečnostním rizikům, s nimiž se můžete setkat při používání protokolu FTP, abyste zajistili, že Vaše strategie zabezpečení popisuje, jak tato rizika minimalizovat.

“Metoda zabezpečení ochrany dat pomocí vrstvené obrany” na stránce 4
Vaše strategie zabezpečení definuje, co chcete chránit a co očekáváte od uživatelů Vašeho systému.

Virtual private network (VPN)

Související odkazy

Terminologie zabezpečení

Související informace

Knihovna referencí pro Lotus Domino

Dokumentace pro Lotus

Odhalená červená kniha infrastruktury zabezpečení Lotus Notes a Domino R5.0

Červená kniha o internetové poště a dalších tématech pro Lotus Domino pro operační systém AS/400

Zabezpečení protokolu FTP

Protokol FTP (File Transfer Protocol) poskytuje schopnost přenosu souborů mezi klientem (uživatelem v jiném systému) a vaším serverem. Měli byste porozumět bezpečnostním rizikům, s nimiž se můžete setkat při používání protokolu FTP, abyste zajistili, že Vaše strategie zabezpečení popisuje, jak tato rizika minimalizovat.

K předání příkazů serveru můžete použít také schopnost předávat vzdálené příkazy. Díky tomu je FTP velmi užitečný při práci se vzdálenými systémy nebo k přesunu souborů mezi systémy. Avšak používání FTP v síti Internet nebo jiných nedůvěryhodných sítích vás vystavuje jistým bezpečnostním rizikům. Porozumění těmto rizikům Vám pomůže při zabezpečení Vašeho systému.

- Když povolíte protokol FTP v systému, může se stát, že vaše schéma oprávnění k objektům nebude poskytovat dostatečnou ochranu.

  Například můžete mít u objektů veřejné oprávnění *USE, ale dnes chcete zabránit většině uživatelů v přístupu k nim pomocí funkce ″zabezpečení menu″. (Funkce zabezpečení menu zabraňuje uživatelům dělat něco, co není jednou z voleb jejich menu.) Jelikož uživatelé FTP nejsou odkázáni jen na menu, mohou číst všechny objekty ve vašem systému.

  Níže je uvedeno několik voleb pro řízení tohoto bezpečnostního rizika:

  – Uplatněte úplné zabezpečení objektů v systému i5/OS (jinými slovy, změňte model zabezpečení systému ze ″zabezpečení menu″ na ″zabezpečení objektu″). Je to nejlepší a nejjistější volba.

  – Napište programy výstupního bodu pro FTP, kterými omezíte přístup k souborům přenášeným pomocí FTP. Programy výstupních bodů by měly poskytnout aspoň takové zabezpečení, které odpovídá minimálně zabezpečení poskytovanému programem menu. Možná byste chtěli, aby řízení přístupu FTP bylo ještě restriktivnější. Tato volba se týká pouze FTP a nikoli též jiných rozhraní, jako jsou ODBC (open database connectivity), DDM (distributed data management) či DRDA (Distributed Relational Database Architecture).

    Poznámka: Oprávnění k souboru *USE umožňuje, aby si uživatel soubor mohl stáhnout. Oprávnění k souboru *CHANGE umožňuje, aby uživatel mohl soubor odeslat.

- Vetřelec může provést na Vašem serveru FTP útok s následkem ″přerušení síťových služeb″, aby zablokoval uživatelské profily v systému. Provádí to tak, že se opakovaně pokouší přihlásit s nesprávným heslem uživatelského profilu, dokud není profil zablokován. Tento typ útoku zablokuje profil, jestliže dosáhne maximálního počtu přihlášení - tří.

  Tohoto rizika se můžete vyvarovat analýzou zvýhodněného zvýšení zabezpečení dat a minimalizace napadení na úkor poskytnutí snadného přístupu uživatelům. Server FTP normálně prosazuje systémovou hodnotu QMAXSIGN, aby vetřelcům neposkytl neomezený počet pokusů, při nichž by mohli uhodnout heslo a provést pak útok. Níže je uvedeno několik voleb, o jejichž použití byste měli uvažovat:

  – Použijte program výstupního bodu přihlášení k FTP, abyste zamítli požadavky na přihlášení všem uživatelským profilům systému a těm uživatelským profilům, u kterých určíte, že nebudou mít k FTP přístup. (Při použití takového programu výstupního bodu se pokusy o přihlášení zamítnuté výstupním bodem přihlášení k serveru u zablokovaných uživatelských profilů nepočítají v čítači profilu QMAXSIGN.)

  – Použijte program výstupního bodu přihlášení k FTP, abyste omezili počet počítačů klienta, ze kterých má daný uživatelský profil přístup k serveru FTP. Má-li například někdo z účtárny (profil Accounting) přístup k serveru FTP, povolte tomuto uživatelskému profilu přístup k serveru FTP pouze z počítačů, které mají IP adresy v oddělení účtárny.

– Použijte program výstupního bodu přihlášení k FTP, abyste zapsali do protokolu jméno uživatele a IP adresu u všech pokusů o přihlášení k serveru FTP. Pravidelně tyto protokoly prohlížejte a kdykoliv dojde k zablokování profilu kvůli maximálnímu počtu pokusů s heslem, identifikujte vetřelce na základě informací z IP adresy a učiňte příslušná opatření.
– Pomocí systému detekujícího vniknutí zjišťujte útoky s následkem přerušení síťových služeb.

Kromě toho můžete výstupní body serveru FTP využít k anonymní funkci FTP pro hostující uživatele. Nastavení zabezpečeného anonymního serveru FTP vyžaduje programy výstupních bodů jak pro přihlášení k serveru FTP, tak pro ověření platnosti požadavků na server FTP.

Chcete-li zabezpečit komunikační relace serveru FTP, můžete používat protokol SSL (Secure Sockets Layer). Použití SSL zajistí zašifrování všech přenosů FTP, aby byla zachována důvěrnost všech dat, která procházejí mezi serverem FTP a klientem, včetně jména uživatele a hesla. Server FTP také podporuje použití digitálních certifikátů včetně autentizace klienta.

Kromě těchto voleb FTP můžete zvážit použití anonymního FTP, které uživatelům jednoduše zajistí pohodlný způsob přístupu k materiálům, které nejsou důvěrné. Anonymní FTP povolí nechráněný přístup (není vyžadováno heslo) k vybraným informacím ve vzdáleném systému. Vzdálený server určí, jaké informace budou všeobecně dostupné. Tyto informace jsou považovány za veřejně přístupné a mohou být čteny kýmkoliv. Předtím, než budete konfigurovat anonymní server FTP, posuďte bezpečnostní rizika a zvažte možnost zabezpečení serveru FTP pomocí programů výstupního bodu.

Související pojmy

“Zabezpečení elektronické pošty” na stránce 18
Použití elektronické pošty v síti Internet nebo v jiné nedůvěryhodné síti představuje bezpečnostní riziko pro Váš systém, a to i pokud je chráněn ochrannou bariérou.

Související úlohy

Konfigurace anonymního protokolu FTP

Správa přístupu pomocí programů pro ukončení protokolu FTP

Související informace

Zabezpečení protokolu FTP

Použití SSL k zabezpečení serveru FTP

Volby zabezpečení přenosu dat

Chcete-li chránit svá data při jejich přenosu přes nedůvěryhodnou síť, měli byste přijmout náležitá bezpečnostní opatření. Tato opatření zahrnují připojení pomocí SSL, produkt System i Access for Windows a připojení VPN.

Vzpomeňte si, že společnost JKL Toy má ve scénáři dva primární systémy. Jeden používá pro vývoj a druhý pro výrobní aplikace. Oba systémy pracují s životně důležitými daty a aplikacemi. Proto společnost přijala rozhodnutí přidat do okrajové sítě nový systém obsluhující intranetové a internetové aplikace.

Vytvoření okrajové sítě zajistí určité fyzické oddělení interní sítě společnosti od sítě Internet. Takové oddělení snižuje riziko plynoucí z používání Internetu, vůči kterému jsou interní systémy zranitelné. Vymezením nového systému jako výlučně internetového serveru společnost rovněž zjednodušila správu svého zabezpečení sítě.

Vzhledem k naléhavé potřebě ochrany dat v prostředí sítě Internet pracuje společnost IBM průběžně na vývoji nabídky produktů, které by zajistily zabezpečení prostředí v sítích provozujících elektronické podnikání v síti Internet. V prostředí sítě Internet musíte zabezpečit ochranu jak systému, tak aplikací. Pohyb důvěrných informací ve vnitropodnikové síti nebo přes internetové spojení však dále zvyšuje potřebu implementace účinnějších bezpečnostních řešení. Chcete-li tato rizika potlačit, měli byste implementovat bezpečnostní opatření na ochranu přenosu dat, která procházejí sítí Internet.

Rizika spojená s pohybem informací po nedůvěryhodných systémech můžete minimalizovat pomocí dvou specifických položek nabídky zabezpečení operačního systému i5/OS na úrovni přenosu: zabezpečené komunikace SSL a připojení VPN.

Protokol SSL je průmyslovým standardem pro zabezpečení komunikace mezi klienty a servery. Protokol SSL byl původně vyvinut pro aplikace webového prohlížeče, ale v současnosti jej může využívat stále větší počet jiných aplikací. V operačním systému i5/OS mezi ně patří:

- HTTP server IBM pro operační systém i5/OS (původní a provozovaný na bázi Apache)
- Server FTP.
- Server Telnet.
- Server DRDA (Distributed Relational Database Architecture) a server DDM (distributed data management)
- Centrální správa v prostředí System i Navigator
- LDAP (Directory Services Server).
- System i Access for Windows aplikace, včetně System i Navigator a aplikace napsané do sady programovacích rozhaní aplikací (API) System i Access for Windows.
- Programy vyvinuté pomocí nástroje Developer Kit for Java a klientské aplikace, které používají IBM Toolkit for Java.
- Programy vyvinuté pomocí rozhraní API SSL (Secure Sockets Layer), které je možné použít k aktivaci SSL u aplikací. Další informace o tom, jak psát programy používající protokol SSL, najdete v tématu Rozhraní API protokolu SSL (Secure Sockets Layer).

Několik těchto aplikací také podporuje používání digitálních certifikátů pro autentizaci klienta. Protokol SSL spoléhá při autentizaci účastníků komunikace a při vytváření zabezpečeného spojení na digitální certifikáty.

VPN (Virtual Private Network)

Můžete použít připojení VPN k vytvoření zabezpečeného komunikačního kanálu mezi dvěma koncovými body. Podobně jako u spojení SSL mohou být data, která putují mezi dvěma koncovými body, zašifrovaná, což zaručuje jejich důvěrnost a integritu. Spojení VPN vám však umožňují omezit postup provozu ke koncovým bodům, které specifikujete, a omezit typ provozu, který může spojení použít. Proto poskytuje spojení VPN jisté zabezpečení na úrovni sítě tím, že vám pomáhá chránit síťové prostředky před neoprávněným přístupem.

Jakou metodu použít?

Obě metody, SSL i VPN, se zabývají potřebou bezpečné autentizace, důvěrností a integritou dat. To, kterou z těchto metod byste měli použít, závisí na několika faktorech. Měli byste vzít v úvahu, s kým chcete komunikovat, jak zabezpečenou komunikaci potřebujete a nakolik jste ochotni slevit ze svých nároků na náklady a výkon ve prospěch zabezpečení komunikace.

Rovněž, chcete-li použít specifickou aplikaci se SSL, musí být tato aplikace na použití SSL nastavena. Ačkoli mnoho aplikací nemůže využívat výhod SSL, mnoho jiných jako je Telnet System i Access for Windows schopnost využívání protokolu SSL má. Na druhé straně vám VPN umožňuje chránit veškerý provoz IP, který postupuje mezi koncovými body specifického spojení.

Můžete například použít běžně HTTP přes SSL a umožnit tak obchodnímu partnerovi komunikovat s webovým serverem ve vaší interní síti. Jestliže je webový server jedinou zabezpečenou aplikací, kterou potřebujete pro komunikaci se svým obchodním partnerem, pak asi nebudete potřebovat přejít na spojení VPN. Pokud byste však chtěli své komunikace rozšířit, možná se rozhodnete spojení VPN přece jen použít. Můžete se také ocitnout v situaci, kdy budete potřebovat ochránit provoz v části své sítě, ale nebudete chtít konfigurovat individuálně každého klienta a každý server, aby používaly SSL. Pro tuto část sítě byste také mohli vytvořit VPN spojení od jedné přenosové brány k druhé. To by zabezpečilo provoz, ale spojení zůstává transparentní pro individuální servery a klienty na obou stranách připojení.

Související pojmy

“Metoda zabezpečení ochrany dat pomocí vrstvené obrany” na stránce 4
Vaše strategie zabezpečení definuje, co chcete chránit a co očekáváte od uživatelů Vašeho systému.

“Scénář: Plán elektronického podnikání společnosti JKL Toy Company” na stránce 7
Typický scénář pro společnost JKL Toy, která se rozhodla rozšířit cíle svého podnikání pomocí využívání Internetu, Vám může pomoci při nastavení Vašeho vlastního plánu na elektronické obchodování.

Související odkazy

Rozhraní API protokolu SSL (Secure sockets Layer)

Související informace

SSL (Secure Sockets Layer)

Virtual Private Network (VPN)

Použití digitálních certifikátů pro SSL

Digitální certifikáty jsou základem pro používání vrstvy SSL (Secure Sockets Layer) pro bezpečnou komunikaci a jsou také silným nástrojem autentizace.

Operační systém i5/OS umožňuje jednoduše vytvářet a spravovat digitální certifikáty pro Vaše systémy a uživatele pomocí aplikace DCM (Digital Certificate Manager), integrované funkce operačního systému i5/OS.

Kromě toho můžete nakonfigurovat některé aplikace, například IBM HTTP Server for i5/OS, aby používaly digitální certifikáty jako účinnější metodu autentizace klienta místo používání uživatelského jména a hesla.

Co je to digitální certifikát?

Digitální certifikát je digitální ověření, které potvrzuje identitu vlastníka certifikátu, podobně jako cestovní pas. Důvěryhodný třetí účastník, nazývaný vydavatel certifikátů (CA), vydává digitální certifikáty uživatelům a serverům. Důvěra ve vydavatele (CA) je základem důvěry v certifikát jako platné pověření.

Každý CA má svou strategii, jak určit, jaké identifikační informace bude požadovat, aby certifikát vydal. Někteří CA v síti Internet mohou požadovat velmi málo informací, např. požadují jen rozlišovací jméno. Je to jméno osoby nebo systému, kterému vydavatel certifikátu vydá adresu digitálního certifikátu a digitální adresu elektronické pošty. Pro každý certifikát se generuje soukromý a veřejný klíč. Certifikát obsahuje veřejný klíč, zatímco prohlížeč nebo zabezpečený soubor ukládá soukromý klíč. Tyto páry klíčů, které jsou přidruženy k příslušnému certifikátu, lze používat k podpisu a zašifrování dat, jako jsou například zprávy a dokumenty, posílané mezi uživateli a servery. Digitální podpisy zajišťují spolehlivost původu položky a chrání její integritu.

Ačkoli mnoho aplikací nemůže využívat výhod SSL, mnoho jiných jako je Telnet System i Access for Windows schopnost využívání protokolu SSL má.

Související pojmy

Konfigurace DCM

SSL (Secure Sockets Layer)

Související odkazy

Terminologie zabezpečení

Zabezpečený přístup k Telnetu pomocí SSL (Secure Socket Layer)

Chcete-li zabezpečit komunikační relace Telnet, můžete nakonfigurovat server Telnet tak, aby používal protokol SSL (Secure Sockets Layer).

Chcete-li nakonfigurovat server Telnet, aby používal SSL, musíte použít produkt DCM (Digital Certificate Manager) a nakonfigurovat certifikát, který bude server Telnet používat. Server Telnet obsluhuje standardně jak zabezpečená, tak nezabezpečená připojení. Server Telnet však můžete konfigurovat tak, aby povoloval jen zabezpečené relace Telnet. Kromě toho můžete server konfigurovat tak, aby kvůli lepší autentizaci klientů používal digitální certifikáty.

Když zvolíte použití SSL u serveru Telnet, dosáhnete výrazného přínosu pro zabezpečení ochrany dat. U serveru Telnet se navíc k autentizaci serveru šifrují data předtím, než dojde k řízení toku dat protokolem Telnet. Jakmile se relace SSL zavede, zašifrují se všechny protokoly Telnet, včetně výměny ID uživatele a hesla.

Nejdůležitějším faktorem k uvážení při použití serveru Telnet je citlivost informací, které budete používat během relace klienta. Jde-li o citlivé nebo soukromé informace, může být pro vás výhodné nastavit server Telnet tak, aby používal SSL. Když pro aplikaci Telnet nakonfigurujete digitální certifikát, je server Telnet schopen obsluhovat jak klienty, kteří mají protokol SSL, tak i klienty, kteří protokol SSL nemají. Jestliže vaše strategie zabezpečení ochrany dat vyžaduje, abyste relace Telnet vždy šifrovali, můžete všechny relace Telnet bez SSL zašifrovat. Když nebude potřeba, abyste server SSL Telnet používali, můžete port SSL vypnout. Použití SSL pro relace Telnet můžete řídit pomocí příkazu (CHGTELNA (Change Telnet Attributes) a parametru ALWSSL (Allow Secure Socket Layer). Chcete-li zajistit, aby žádné aplikace nemohly používat porty SSL, případně Non-SSL, můžete k takovému omezení také použít příkaz ADDTCPPORT (Add TCP/IP Port Restriction).

Chcete-li zjistit více o serveru Telnet a radách týkajících se zabezpečení pro Telnet, téma IBM poskytuje informace, které potřebujete k používání produktu Telnet v operačním systému i5/OS.

Související pojmy

Scénář Telnet: Zabezpečení Telnetu pomocí SSL

Plánování pro DCM

Související informace

Telnet

SSL (Secure Sockets Layer) pro zabezpečení produktu System i Access for Windows

Abyste zabezpečili komunikační relace System i Access for Windows, můžete nakonfigurovat produkt System i Access for Windows tak, aby používal SSL (Secure Sockets Layer).

Použití SSL zajistí, že veškerý provoz pro relace System i Access for Windows je šifrován. To znemožňuje přečíst data procházející mezi lokálními a vzdálenými uzly.

Související informace

Správa SSL

Zabezpečení pro jazyk Java

Třídy zabezpečení

VPN pro zabezpečení soukromých komunikací

VPN (Virtual private network), rozšíření intranetu společnosti přes existující rámec buď veřejné nebo soukromé sítě, Vám může pomoci bezpečně a soukromě komunikovat uvnitř Vaší organizace.

Se vzestupem používání VPN a zabezpečení, které poskytuje, hledá společnost JKL Toy možnosti přenosu dat přes internet. Nedávno koupila další malou společnost na výrobu hraček a chce ji provozovat jako svou pobočku. Společnost JKL Toy bude potřebovat předávat si s pobočkou informace. Obě společnosti používají operační systém i5/OS a připojení VPN, které může poskytovat potřebné zabezpečení komunikace mezi dvěma sítěmi. Vytvoření VPN je z hlediska nákladů výhodnější než tradiční pevné linky.

Jmenujme některé uživatele, kteří by měli prospěch z použití VPN pro připojitelnost:

- Vzdálení a mobilní uživatelé.
- Domácí kancelář komunikující s kancelářemi pobočky nebo jinými externími pracovišti.
- Komunikace mezi podniky.

Jestliže neomezíte přístup uživatelů k citlivým systémům, vyskytnou se bezpečnostní rizika. Jestliže nevymezíte, kdo může mít k systému přístup, zvyšujete pravděpodobnost toho, že důvěrnost vašich informací nebude zachována. Potřebujete plán, který povolí přístup k systému pouze těm, kdo informace v tomto systému sdílejí. VPN vám umožňuje řídit síťový provoz a přitom nabízí důležité funkce zabezpečení dat, jako například autentizaci a soukromí

dat. Vytvoření několika spojení VPN vám umožňuje řídit, kdo v nich bude mít přístup k jednotlivým systémům. Například účtárna a osobní oddělení mohou být spojeny vlastní sítí VPN.

Když uživatelům povolíte, aby se k systému připojili přes Internet, může dojít k tomu, že budete veřejnými sítěmi posílat citlivá data společnosti, která tak mohou být napadena. Jednou z voleb, jak ochránit přenášená data, je použít metody šifrování a autentizace k zajištění soukromí a zabezpečení před vnějšími zásahy. Spojení VPN nabízí řešení specifické potřeby ochrany dat - zabezpečení komunikace mezi systémy. Spojení VPN poskytuje ochranu pro data, která postupují mezi dvěma koncovými body spojení. Mimoto můžete použít zabezpečení pomocí pravidel paketů a definovat, které IP pakety smějí sítí VPN procházet.

VPN můžete použít, chcete-li vytvořit zabezpečené spojení mezi řízenými a důvěryhodnými koncovými body. Přesto musíte neustále zvažovat, kolik možností přístupu svým partnerům ve VPN poskytnete. spojení VPN může zakódovat data, která procházejí veřejnými sítěmi. Ale podle toho, jak je nakonfigurujete, nemusí být data přicházející z Internetu, přenášena přes připojení VPN. V takovém případě by tato data neměla být šifrována, protože prochází přes interní sítě, jež komunikují prostřednictvím těchto připojení. V důsledku toho byste měli pečlivě naplánovat, jak jednotlivá spojení VPN nastavit. Dbejte na to, abyste svému partnerovi ve VPN poskytli přístup jenom k těm hostitelům nebo prostředkům vaší interní sítě, u kterých si to přejete.

Můžete mít například prodejce, který potřebuje získat informace o tom, jaké díly máte na skladě. Tyto informace máte v databázi, kterou používáte k aktualizaci webových stránek ve vaší vnitropodnikové síti. Chtěli byste prodejci povolit přístup k těmto stránkám přímo přes spojení VPN. Nechcete však, aby měl přístup k jiným systémovým prostředkům, jako například k samotné databázi. Naštěstí můžete spojení VPN konfigurovat tak, že provoz mezi oběma koncovými body je omezen na port 80. Port 80 je standardní port, který používá provoz HTTP. V důsledku toho může váš prodejce odesílat a přijímat požadavky HTTP pouze přes toto spojení.

Díky tomu, že můžete omezit typ provozu, který prochází spojením VPN, zabezpečuje toto spojení ochranu na úrovni sítě. VPN však nepracuje stejným způsobem jako ochranná bariéra při regulaci provozu do systému a ze systému. Připojení VPN rovněž není jediným dostupným prostředkem k zabezpečení komunikace mezi Vaším operačním systémem i5/OS a ostatními systémy. V závislosti na Vašich potřebách zabezpečení můžete zjistit, že Vám lépe vyhovuje použití SSL.

To, zda spojení VPN poskytuje zabezpečení, které potřebujete, záleží na tom, co chcete ochránit. Závisí to také na změnách, které jste ochotni udělat, abyste požadovaného zabezpečení dosáhli. Tak, jako u všech rozhodnutí, která se týkají zabezpečení ochrany dat, byste měli zvážit, jak spojení VPN podporuje strategii zabezpečení ochrany vašich dat.

Související pojmy

"Produkt System i a otázky zabezpečení Internetu" na stránce 2
Bezpečnostní otázky spojené s Internetem jsou významné. Toto téma nabízí přehled silných stránek zabezpečení a možností zabezpečení operačního systému i5/OS.

Virtual private networks (VPN)

Dodatek. Upozornění

Tyto informace platí pro produkty a služby nabízené v USA.

IBM nemusí v ostatních zemích nabídnout produkty, služby a funkce popsané v tomto dokumentu. Informace o produktech a službách, které jsou momentálně dostupné ve vašem regionu, můžete získat od místního zástupce IBM. Žádný odkaz na produkt, program nebo službu IBM neznamená a ani z něj nelze vyvozovat, že smí být použit pouze uvedený produkt, program či služba společnosti IBM. Použít lze jakýkoli funkčně ekvivalentní produkt, program či službu neporušující práva IBM k duševnímu vlastnictví. Za vyhodnocení a ověření činnosti libovolného produktu, programu či služby jiného výrobce než IBM však odpovídá uživatel.

IBM může mít patenty nebo podané žádosti o patent, které zahrnují předmět tohoto dokumentu. Získání tohoto dokumentu uživateli neposkytuje licenci na tyto patenty. Písemné dotazy ohledně licencí můžete zaslat na adresu:

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

Pokud máte zájem o licenci v zemi s dvoubajtovou znakovou sadou (DBCS), kontaktujte zastoupení společnosti IBM ve vaší zemi, nebo písemně zastoupení společnosti IBM na adrese:

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

Následující odstavec neplatí pro Velkou Británii a další země, ve kterých tato opatření nejsou v souladu s místními právními předpisy: IBM POSKYTUJE TUTO PUBLIKACI " JAK JE" (AS-IS), BEZ JAKÝCHKOLI ZÁRUK, VYJÁDŘENÝCH VÝSLOVNĚ NEBO VYPLÝVAJÍCÍCH Z OKOLNOSTÍ VČETNĚ, A TO ZEJMÉNA ZÁRUK NEPORUŠOVÁNÍ PRÁV TŘETÍCH STRAN, PRODEJNOSTI NEBO VHODNOSTI PRO URČITÝ ÚČEL VYPLÝVAJÍCÍCH Z OKOLNOSTÍ. Právní řády některých zemí nepřipouštějí vyloučení záruk vyjádřených výslovně nebo vyplývajících z okolností v určitých transakcích a proto se na Vás výše uvedené omezení nemusí vztahovat.

Tato publikace může obsahovat technické nepřesnosti nebo typografické chyby. Informace zde uvedené jsou pravidelně aktualizovány a v nových vydáních této publikace již budou tyto změny zahrnuty. IBM má právo kdykoliv bez upozornění zdokonalovat nebo měnit produkty a programy popsané v této publikaci.

Jakékoli odkazy v této publikaci na webové stránky jiných společností než IBM jsou poskytovány pouze pro pohodlí uživatele a nemohou být žádným způsobem vykládány jako doporučení těchto webových stránek ze strany IBM. Materiály obsažené na takovýchto webových stránkách nejsou součástí materiálů k tomuto produktu IBM a tyto webové stránky mohou být používány pouze na vlastní nebezpečí.

IBM může použít nebo distribuovat jakékoliv informace, které jí sdělíte, libovolným způsobem, který společnost považuje za odpovídající, bez vzniku jakýchkoliv závazků vůči vám.

Držitelé licence na tento program, kteří si přejí mít přístup i k informacím o programu za účelem (i) výměny informací mezi nezávisle vytvořenými programy a jinými programy (včetně tohoto) a (ii) vzájemného použití sdílených informací, mohou kontaktovat:

IBM Corporation
Software Interoperability Coordinator, Department YBWA
3605 Highway 52 N

Rochester, MN 55901
U.S.A.

Informace tohoto typu mohou být dostupné za určitých podmínek. V některých případech připadá v úvahu zaplacení poplatku.

IBM poskytuje licencovaný program popsaný v těchto informacích a veškeré dostupné licencované materiály na základě podmínek uvedených ve smlouvě IBM Customer Agreement, v Mezinárodní licenční smlouvě IBM na programy nebo v jiné ekvivalentní smlouvě mezi námi.

Všechna zde obsažená data týkající se výkonu byla zjištěna v řízeném prostředí. Výsledky získané v jiných provozních prostředích se proto mohou významně lišit. Některá měření mohla být prováděna v systémech na úrovni vývoje a nelze tedy zaručit, že tato měření budou ve všeobecně dostupných systémech stejná. Některá měření mohla být navíc odhadnuta pomocí extrapolace. Skutečné výsledky se mohou lišit. Uživatelé tohoto dokumentu by měli ověřit příslušná data pro své specifické prostředí.

Informace týkající se produktů jiných společností byly získány od dodavatelů těchto produktů, z jejich tištěných materiálů nebo z jiných veřejně dostupných zdrojů. IBM nezkoumala tyto produkty a nemůže tudíž potvrdit spolehlivost, kompatibilitu a další konstatování, vztahující se k těmto produktům. Dotazy na možnosti produktů pocházejících z jiného zdroje než od IBM adresujte dodavatelům těchto produktů.

Tyto informace jsou poskytovány pouze za účelem plánování. Informace zde poskytované se mohou změnit dříve, než budou popisované produkty k dispozici.

Informace obsahují příklady dat a zpráv, které jsou běžně používány v denních obchodních činnostech. Příklady obsahují jména a názvy osob, společností, značek a produktů, aby bylo možno je vysvětlit v plném rozsahu. Všechna tato jména a názvy jsou zcela fiktivní a jakákoliv podobnost se jmény či adresami existujících společností je zcela náhodná.

LICENČNÍ INFORMACE:

Tyto informace obsahují vzorové aplikační programy ve zdrojovém jazyce, které ilustrují programovací techniky na různých provozních platformách. Jste oprávněni bezplatně kopírovat, modifikovat a distribuovat tyto vzorové programy v jakékoliv formě, a to pro účely vývoje, užívání, marketingu nebo distribuce aplikačních programů vhodných pro rozhraní API pro operační platformu, pro kterou byly vzorové programy napsány. Uvedené příklady nebyly důkladně testovány za všech podmínek. IBM proto nemůže zaručit nebo potvrdit spolehlivost, obsluhovatelnost nebo funkčnost těchto produktů.

Každá kopie nebo část těchto vzorových programů nebo práce z nich odvozené musí zahrnovat následující copyrightovou výhradu:

© (jméno Vaší společnosti) (rok). Části tohoto kódu jsou odvozeny od vzorových programů IBM © Copyright IBM Corp. _zadejte rok nebo roky_. Všechna práva vyhrazena.

Pokud si tyto informace prohlížíte ve formě softcopy, nemusí se zobrazit fotografie a barevné ilustrace.

Programování informací o rozhraní

Tato publikace o System i a zabezpečení Internetu dokumentují zamýšlená Programovací rozhraní, která umožňují zákazníkovi psát programy k získání služeb operačního systému IBM i5/OS.

Ochranné známky

Následující výrazy jsou ochrannými známkami IBM v USA a případně v dalších jiných zemích:

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

Adobe, logo Adobe, PostScript a logo PostScript jsou buď registrované ochranné známky nebo ochranné známky of Adobe Systems Incorporated ve SPojených státech amerických a/nebo dalších zemích.

Microsoft, Windows, Windows NT a logo Windows jsou ochranné známky společnosti Microsoft Corporation ve Spojených státech a případně v dalších jiných zemích.

Java a všechny ochranné známky obsahující slovo Java jsou ochrannými známkami společnosti Sun Microsystems, Inc. ve Spojených státech a případně v dalších jiných zemích.

Další jména společností, produktů nebo služeb mohou být ochrannými známkami jiných společností.

Ustanovení a podmínky

Oprávnění k užívání těchto publikací je uděleno na základě následujících ustanovení a podmínek.

Osobní použití: Pokud zachováte všechny výhrady týkající se vlastnických práv, můžete tyto publikace kopírovat pro své osobní nekomerční použití. Tyto publikace ani jakékoliv jejich části nesmíte bez výslovného souhlasu IBM distribuovat, prezentovat ani z nich vytvářet odvozená díla.

Komerční použití: Pokud zachováte všechny výhrady týkající se vlastnických práv, můžete tyto publikace kopírovat, distribuovat a prezentovat výhradně uvnitř svého podniku. Bez výslovného souhlasu IBM nesmíte z těchto publikací vytvářet odvozená díla ani je (nebo jejich části) nesmíte kopírovat, distribuovat či prezentovat mimo rámec svého podniku.

Kromě oprávnění, která jsou zde výslovně udělena, se na publikace nebo jakékoliv informace, data, software a další duševní vlastnictví obsažené v těchto publikacích nevztahují žádná další vyjádřená ani odvozená oprávnění, povolení či práva.

IBM si vyhrazuje právo odvolat oprávnění zde udělená, kdykoli usoudí, že používání publikací poškozuje jeho zájmy nebo že výše uvedené pokyny nejsou řádně dodržovány.

Tyto informace můžete stahovat, exportovat či reexportovat pouze při dodržení všech příslušných zákonů a nařízení včetně veškerých vývozních zákonů a nařízení USA.

IBM NEPOSKYTUJE ŽÁDNOU ZÁRUKU, POKUD JDE O OBSAH TĚCHTO PUBLIKACÍ. TYTO PUBLIKACE JSOU POSKYTOVÁNY NA BÁZI ″JAK JSOU″ (AS-IS), BEZ JAKÝCHKOLIV ZÁRUK, VYJÁDŘENÝCH VÝSLOVNĚ NEBO VYPLÝVAJÍCÍCH Z OKOLNOSTÍ VČETNĚ, A TO ZEJMÉNA, ZÁRUK PRODEJNOSTI, NEPORUŠENÍ PRÁV TŘETÍCH STRAN NEBO VHODNOSTI PRO URČITÝ ÚČEL VYPLÝVAJÍCÍCH Z OKOLNOSTÍ.

Vytištěno v Dánsku společností IBM Danmark A/S.