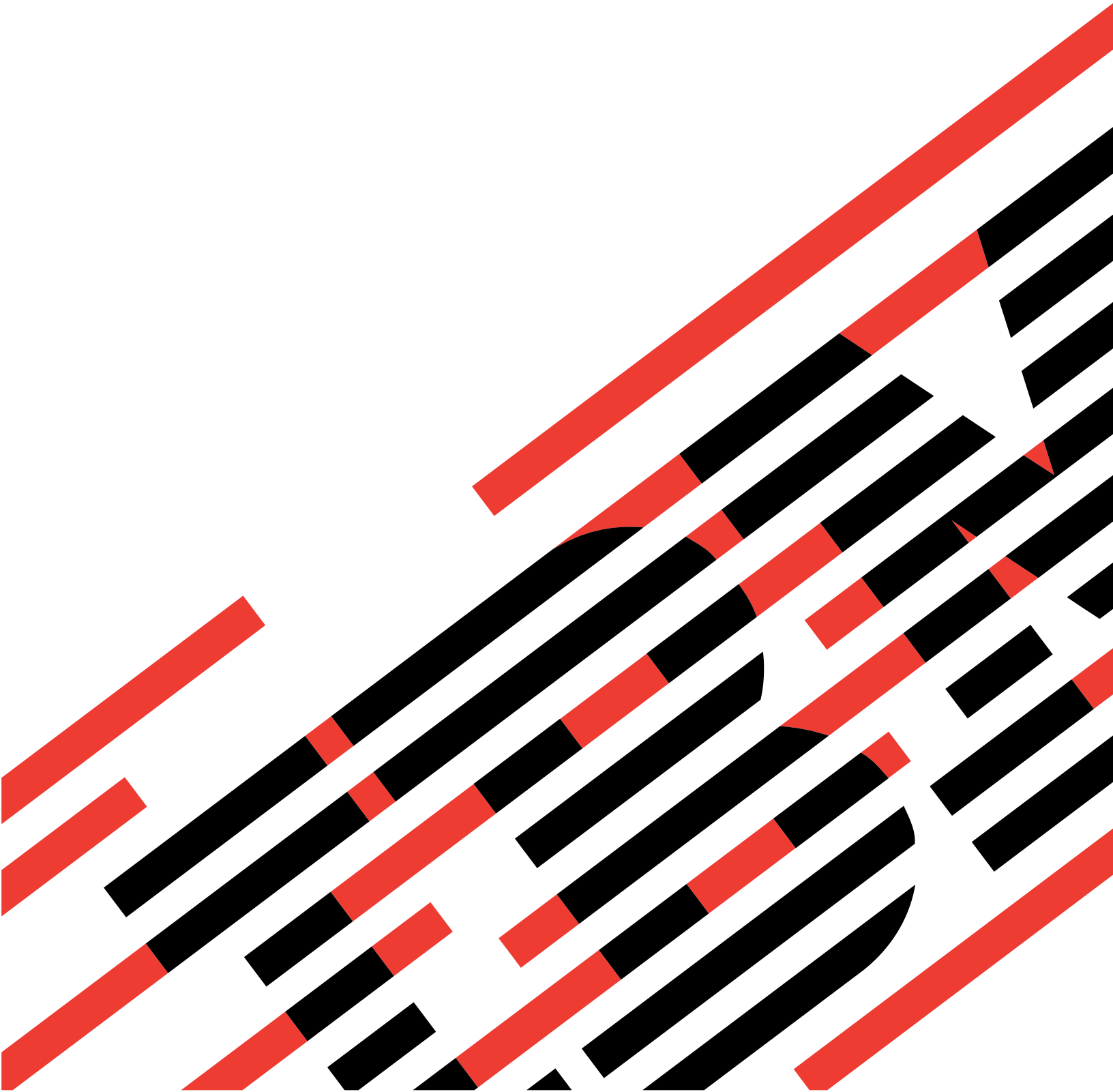
IBM

eserver

iSeries

IBM SecureWay: iSeries 400 a Internet



IBM

@server

iSeries

IBM SecureWay: iSeries 400 a Internet

Obsah

Část 1. IBM SecureWay: iSeries a Internet 1

Kapitola 1. Co je nového ve verzi V5R1 . 3

Kapitola 2. Tisk tohoto tématu 5

Kapitola 3. Server iSeries 400 a zabezpečení Internetu 7

Kapitola 4. Plánování zabezpečení Internetu 9
Metoda zabezpečení dat pomocí vrstvené obrany. 10
Strategie a cíle zabezpečení ochrany dat 11
Scénář: Plán elektronického podnikání firmy JKL Toy . . 14

Kapitola 5. Úrovně zabezpečení pro základní přípravu na Internet 17

Kapitola 6. Možnosti zabezpečení sítě 19
Bezpečnostní bariéra 20
Pravidla paketu systému iSeries 22
Výběr voleb zabezpečení sítě iSeries 23

Kapitola 7. Volby zabezpečení aplikací 25
Zabezpečení webových služeb 25
Zabezpečení Internetu a Java 26
Zabezpečení elektronické pošty 29
Zabezpečení protokolu FTP 30

Kapitola 8. Volby zabezpečení přenosu dat 33
Použití digitálních certifikátů pro SSL 34
Zabezpečený přístup k Telnet pomocí SSL 35
Zabezpečení produktu Client Access Express pomocí SSL 35
Zabezpečení soukromých komunikací pomocí VPN . . . 36

Kapitola 9. Terminologie zabezpečení Internetu 39

Část 1. IBM SecureWay: iSeries a Internet

Přístup k Internetu ze sítě LAN je významným krokem v rozvoji vaší sítě, který bude vyžadovat, abyste přehodnotili své požadavky na zabezpečení ochrany dat. Váš server iSeries 400 má naštěstí integrovaná softwarová řešení a architekturu zabezpečení dat, pomocí nichž si můžete vybudovat silnou ochranu proti možným nástrahám a vetřelcům, ohrožujícím bezpečnost dat v síti Internet. Správné použití nabídky serveru iSeries zajistí, aby vaši zákazníci, zaměstnanci a obchodní partneři získali potřebné informace a mohli s vámi spolupracovat v zabezpečeném prostředí.

Informace, které zde najdete, vás poučí o známých okolnostech představujících ohrožení zabezpečení dat a o tom, jaký mají tato rizika vztah k vašim cílům v internetovém a elektronickém podnikání. Dozvíte se také, jak odhadnout riziko ve srovnání s přínosem použití různých voleb zabezpečení dat, které pro odstranění rizika nabízí server iSeries. A konečně můžete určit, jak tyto informace využít při vývoji plánu pro zabezpečení ochrany dat, který by odpovídal potřebám vašeho podnikání a vytvořit tak vlastní strategii zabezpečení ochrany dat.

Chcete-li se dovědět víc o riziku pro zabezpečení ochrany dat v síti Internet a o zabezpečovacích řešeních serveru iSeries, která můžete použít k nastavení ochrany systémů a zdrojů, prostudujte si tyto informace:

- **Co je nového ve verzi V5R1**
  Informuje o změnách a dodatcích k nabídce produktů serveru iSeries pro zabezpečení dat v síti Internet ve verzi V5R1.
- **Tisk tohoto tématu**
  Informuje o tom, jak získat přístup k tomuto tématu ve verzi Adobe Acrobat a jak je vytisknout.
- **Server iSeries a zabezpečení Internetu**
  Na základě těchto informací získáte všeobecný přehled o výhodách zabezpečení ochrany dat serveru iSeries pro elektronické podnikání a o nabídce dostupných produktů.
- **Plánování zabezpečení Internetu**
  Z těchto informací se dozvíte, jak vytvořit strategii zabezpečení ochrany dat, která splní vaše požadavky na zabezpečení Internetu a elektronického podnikání.
- **Úrovně zabezpečení systému serveru iSeries základní příprava na Internet**
  Z těchto informací se dozvíte, jaké systémové zabezpečení dat byste měli mít předtím, než se připojíte k Internetu.
- **Volby zabezpečení sítě**
  Z těchto informací se dozvíte o opatřeních pro zabezpečení dat na úrovni sítě, o jejichž použití byste měli při nastavení ochrany vašich interních prostředků uvažovat.
- **Volby zabezpečení aplikací**
  Z těchto informací se dozvíte o běžných rizicích zabezpečení dat v síti Internet u řady oblíbených internetových aplikací a služeb a o opatřeních pro zvládání takového rizika.
- **Volby zabezpečení přenosu dat**
  Z těchto informací se dozvíte o opatřeních pro zabezpečení dat, která můžete implementovat a ochránit tak data, když postupují přes nedůvěryhodné sítě, jako například Internet. Prostudujte si více o bezpečnostních opatřeních při používání připojení SSL (Secure Sockets Layer), Client Access Express a Virtuální privátní sítě (VPN).
- Volby zabezpečení Internetu na serveru **iSeries**
  Tato stručná diskuse o volbách zabezpečení dat na serveru iSeries vám pomůže vybrat nabídky a nastavit ochranu vašich systémů a prostředků podle vlastního plánu využívání Internetu a elektronického podnikání.

Poznámka: Jestliže nejste obeznámeni s terminologií týkající se ochrany dat a Internetu, můžete se podívat na běžnou terminologii zabezpečení dat dále v tomto materiálu.

Kapitola 1. Co je nového ve verzi V5R1

U verze V5R1 je řada zlepšení a dodatků k nabídce produktů zabezpečení ochrany dat pro systém iSeries 400. Následující seznam popisuje některá významnější vylepšení funkčního zabezpečení:

- **Vylepšení DCM (Digital Certificate Manager)**
  Nyní můžete používat DCM k vytváření a správě certifikátů, které lze použít k digitálnímu podpisu objektů a zajistit tak jejich integritu a dodat k objektům důkaz o původu. Je také možné vytvořit a spravovat odpovídající certifikáty pro ověření podpisu, které je možné použít k prokázání pravosti podpisu na podepsaném objektu a zajistit tak, že data v objektu jsou nezměněná a ověřit důkaz o původu objektu. DCM a odpovídající rozhraní API je také možné použít k podepsání objektu a ověření podpisu na objektu.
- **Digitálně podepsaný operační systém**
  Od verze V5R1 bude firma IBM digitálně podepisovat systém OS/400 a licencované programy IBM LPP. Uživatelé si mohou ověřit, že programy od IBM nebyly pozměněny od té doby, co je IBM podepsala. Ověření digitálního podpisu je možné provést v době obnovy nebo příkazem CHKOBJITG. K dispozici jsou také rozhraní API, která umožní zákazníkům a obchodním partnerům digitálně podepsat a ověřovat jejich aplikace.
- **Nová pravidla pro heslo uživatelského profilu (QPWDLVL 2 a 3)**
  Délka hesla uživatelského profilu byla zvýšena tak, že připouští 1 až 128 znaků. Hesla rozlišují velká a malá písmena a povolují vložené mezery, například ″To je moje nové heslo.″ Koncové mezery se odstraňují a heslo nemohou tvořit samé mezery.
- **Vylepšení hesla uživatelského profilu**
  Novou systémovou hodnotu QPWDLVL můžete použít k nastavení čtyř voleb pro kontrolu úrovně hesla systému:
  – PWDLVL 0 — Toto nastavení připouští heslo o délce 10 bajtů, a umožňuje, aby hesla serveru NetServer byla podržena. Toto je výchozí nastavení.
  – PWDLVL 1 — Toto nastavení připouští hesla 10 bajtů dlouhá a vylučuje hesla serveru NetServer.
  – PWDLVL 2 — Toto nastavení připouští hesla o délce 128 znaků a zadržuje hesla, která odpovídají jak starému, tak novému formátu hesla.
  – PWDLVL 3 — Toto nastavení připouští hesla o délce 128 znaků a odstraní staré formáty hesla.
- **IBM 4758 – 023 PCI Cryptographic Coprocessor pro zabezpečenější uložení klíče**
  Máte-li v systému nainstalován produktu IBM 4758–023 PCI Cryptographic Coprocessor, můžete jej použít k bezpečnějšímu uložení klíčů vašeho digitálního certifikátu. Při použití DCM k vytvoření nebo obnovení certifikátů můžete zvolit přímé uložení klíče v koprocesoru nebo použít hlavní klíč koprocesoru k zašifrování soukromého klíče a jeho uložení do zvláštního souboru pro uložení klíčů. Když používáte koprocesor pro uložení klíčů, můžete navíc zlepšit výkon vrstvy SSL u aplikací, které SSL podporují. Vzhledem k tomu, že koprocesor obsluhuje úlohu týkající se dešifrování soukromého klíče předkládaného při navazování komunikace SSL, je také možné vyvážit zatížení při zpracování navázání komunikace SSL přes několik karet 4758.
- **Podpora certifikátu VPN**
  Před verzí V5R1 se mohly servery VPN Internet Key Exchange (IKE) vzájemně autentizovat pouze použitím předem sdíleného klíče. Použití předem sdíleného klíče je méně bezpečné, protože musíte předat tento klíč ručně administrátorovi druhého koncového bodu vaší VPN. V důsledku toho je zde možnost, že by klíč mohl být v procesu předávání objeven někým jiným. Ve verzi V5R1 se tomuto riziku můžete vyhnout použitím digitálních certifikátů k autentizaci koncových bodů namísto použití předem sdíleného

klíče. Pomocí produktu DCM (Digital Certificate Manager) můžete spravovat certifikáty, které používá váš server IKE k vytvoření dynamického připojení VPN.

- **Zlepšení aplikací aktivovaných pomocí SSL (Secure Sockets Layer)**
  Ve verzi V5R1 je řada vylepšení SSL. Nyní můžete nakonfigurovat server FTP iSeries tak, aby používal SSL k zabezpečení komunikačních relací. Server FTP také můžete nakonfigurovat tak, aby k autentizaci klienta používal digitální certifikáty. A kromě toho poskytuje systém OS/400 ve verzi V5R1 podporu 128bitové šifry AES. AES je nový a rychlejší šifrovací algoritmus, který nahrazuje algoritmus DES.
- **Vylepšení SMTP (Simple Mail Transfer Protocol)**
  SMTP nyní poskytuje podporu ″černé listiny″ (blacklist), která se vytváří z položek Předmět, Odesílatel a IP adresa.
- **Průvodce nastavením sítě Internet**
  Oblíbený průvodce nastavením Internetu, který byl v posledním vydání dostupný jako soubor ke stažení, je nyní přímo v produktu Operations Navigator. Pomocí průvodce můžete v systému iSeries konfigurovat internetové spojení a zabezpečit je automaticky generovanými filtrovací pravidly.
- **Vylepšení doby uchování dat pro vytvoření programu**
  Programy vytvořené pro verzi V5R1 a novější verze systémů iSeries obsahují informace, které umožňují program znovu vytvořit v čase obnovy, je-li to zapotřebí. Informace potřebné pro znovuvytvoření programu zůstávají u programu i tehdy, když je pozorovatelnost programu odstraněna. Jestliže se během obnovy zjistí, že došlo k chybě ověření platnosti, bude program znovu vytvořen, aby se chyba ověření platnosti opravila. Operace znovuvytvoření programu během obnovy není ve verzi V541 systému iSeries nová. V předchozích vydáních měla každá chyba ověření platnosti programu zjištěná během obnovy za následek to, že byl program podle možnosti znovu vytvořen (jestliže v obnovovaném programu existovala pozorovatelnost). Rozdíl je v tom, že u programů od verze V5R1 iSeries informace potřebné ke znovuvytvoření zůstávají, i když byla pozorovatelnost z programu odstraněna. Jakýkoliv program od verze V5R1 nebo novější, u kterého byla zjištěna chyba ověření platnosti, je tedy znovu vytvořen a změna, která chybu ověření platnosti způsobila, je odstraněna.

Kapitola 2. Tisk tohoto tématu

Máte možnost vytisknout nebo stáhnout PDF verzi tohoto dokumentu. Chcete-li si soubory ve formátu PDF prohlížet, musíte mít nainstalovaný produkt Adobe Acrobat Reader. Můžete si jej stáhnout z domovské stránky společnosti Adobe. 

Chcete-li zobrazit nebo stáhnout tento dokument ve formátu PDF, vyberte IBM SecureWay: iSeries and the Internet (416 KB nebo 60 stran).

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

1. Otevřete PDF ve svém prohlížeči (klepněte na výše uvedený odkaz).
2. V menu prohlížeče klepněte na **File** (Soubor).
3. Klepněte na **Save As...** (Uložit jako...).
4. Navigujte do adresáře, kam chcete PDF uložit.
5. Klepněte na **Save** (Uložit).

Kapitola 3. Server iSeries 400 a zabezpečení Internetu

Jako majitel serveru iSeries 400 zkoumající možnosti připojení svých systémů k Internetu se obvykle budete nejdříve ptát ″Jak mám začít používat Internet k podnikatelským účelům?″ Druhá otázka je ″Co bych měl vědět o zabezpečení ochrany dat a o Internetu?″ Záměrem tohoto materiálu je pomoci vám získat odpověď na druhou otázku.

Odpověď na otázku ″Co bych měl vědět o zabezpečení ochrany dat a o Internetu?″ je, že to záleží na tom, jak chcete Internet využívat. Problémy týkající se zabezpečení Internetu jsou významné. Problémy, kterými se budete zabývat, záleží na tom, jak hodláte Internet používat. Vaší první akcí v síti Internet by mohlo být umožnit uživatelům interní sítě přístup k WWW a k elektronické poště přes Internet. Možná budete potřebovat také schopnost přenášet citlivé informace z jednoho uzlu do druhého. A konečně můžete plánovat použití Internetu pro elektronický obchod nebo pro vytvoření sítě typu extranet mezi vaší firmou 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. Při vytváření plánu využití Internetu vám může pomoci část Scénář: Plán elektronického podnikání firmy JKL Toy. (Poznámka: Jestliže nejste obeznámeni s terminologií týkající se zabezpečení dat a Internetu, můžete se podívat na rejstřík terminologie v oblasti zabezpečení dat, který je uveden dále v tomto dokumentu).

Jakmile budete vědět, jak chcete Internet pro elektronické podnikání využít a také jaké jsou problémy zabezpečení ochrany dat a dostupné nástroje, funkce a nabídky produktů, můžete vyvinout strategii pro zabezpečení ochrany dat a její cíle. Vaše volby při vyvíjení strategie zabezpečení ochrany dat bude ovlivňovat řada faktorů. Když svou organizaci rozšiřujete na Internet, představuje strategie zabezpečení ochrany dat rozhodující faktor pro zajištění bezpečnosti vašich systémů a prostředků.

Charakteristika zabezpečení ochrany dat v systému iSeries 400

Kromě velké nabídky specifických produktů pro zabezpečení dat chránících vaše systémy v síti Internet má systém iSeries 400 velmi účinné charakteristiky zabezpečení systému, jako například:

- Integrované zabezpečení dat se nesmírně obtížně obchází, srovnáme-li je s nabídkami přídavných softwarových balíků v jiných systémech.
- Objektová architektura, která technicky ztěžuje vytvoření a rozšíření viru. V systému iSeries nemůže soubor předstírat, že je program, a program nemůže změnit jiný program. Vlastnosti integrity systému iSeries 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 hackerů v architektuře jiných systémů.
- Flexibilita, která vám umožňuje nastavit zabezpečení systému tak, aby vyhovovalo vašim specifickým požadavkům. Můžete využít aplikaci Technical Studio, téma Security Advisor,

která vám pomůže určit doporučení pro zabezpečení dat odpovídající potřebám vaší

Rozšířená nabídka produktů pro zabezpečení ochrany dat systému iSeries

Systém iSeries také nabízí několik specifických produktů pro zabezpečení ochrany dat, které můžete použít k rozšíření zabezpečení systému, když se připojujete k Internetu. Podle toho, jak Internet používáte, budete se rozhodovat pro využití některých z těchto nabízených produktů:

- Virtuální soukromé sítě (VPN) jsou rozšířením soukromé vnitropodnikové sítě do veřejné sítě, jakou je například Internet. Chcete-li vytvořit zabezpečené soukromé připojení, můžete k tomu použít VPN a v podstatě vytvořit soukromý ″tunel″ do veřejné sítě. Virtuální soukromá síť (VPN) je integrovaná funkce systému OS/400, dostupná z rozhraní Operations Navigator.
- Pravidla paketů jsou integrovanou funkcí systému OS/400, která je dostupná z rozhraní Operations Navigator. Tato funkce vám umožňuje konfigurovat pravidla pro filtr IP paketu a převod síťových adres (NAT) pro řízení postupu provozu TCP/IP do a ze systému iSeries.
- SSL (Secure Sockets Layer), komunikační zabezpečení aplikace, vám umožňuje konfigurovat aplikace tak, aby používaly SSL k vytvoření zabezpečeného spojení mezi aplikacemi serverů a jejich klienty. Funkce SSL byla původně vyvinuta pro zabezpečený prohlížeč WWW a aplikace serveru, je však možné povolit i jiným aplikacím, aby ji používaly. Mnoho aplikací serveru iSeries má nyní povoleno používat SSL; patří mezi ně server IBM HTTP Server for iSeries, Client Access Express, protokol FTP, Telnet a mnoho jiných.

Jakmile si ujasníte, jak chcete použít Internet a také jaké jsou problémy zabezpečení dat a jaké nástroje ochrany, funkce a nabídky produktů jsou dostupné, budete připraveni vyvinout strategii a cíle zabezpečení ochrany dat. Vaše volby při vyvíjení strategie zabezpečení ochrany dat bude ovlivňovat řada faktorů. Když svou organizaci rozšiřujete na Internet, představuje strategie zabezpečení ochrany dat rozhodující faktor pro zajištění bezpečnosti vašeho systému.

Poznámka: Chcete-li zjistit podrobnější informace o tom, jak začít používat Internet pro podnikatelské účely, podívejte se na online témata aplikace Information Center a červené knihy IBM (redbooks):

- *Connecting to the Internet*
- *AS/400 Internet Security: Protecting Your AS/400 from HARM on the Internet* (SG24-4929) .

Kapitola 4. Plánování zabezpečení Internetu

Při vývoji plánů na použití sítě Internet musíte pečlivě naplánovat i potřeby jeho zabezpečení. Musíte shromáždit podrobné informace o plánovaném využití Internetu a zdokumentovat konfiguraci vaší interní sítě. Na bázi výsledků těchto shromážděných informací můžete dospět k přesnému ohodnocení požadavků zabezpečení dat.

Měli byste například zdokumentovat a popsat následující skutečnosti:
- Aktuální konfiguraci vaší sítě.
- Informace o konfiguraci serveru DNS a serveru elektronické pošty.
- Vaše připojení k poskytovateli služeb sítě Internet (ISP).
- Jaké internetové služby chcete používat.
- Jaké služby chcete poskytovat uživatelům Internetu.

Zdokumentování takových 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 využila 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 rozhodnout, jaká další bezpečnostní opatření byste měli implementovat pro zajištění utajení dat při tomto využití (aktivace SSL (Secure Sockets Layer)).

Při práci na vývoji plánu využití sítě Internet a plánu pro zabezpečení ochrany dat vám mohou pomoci tyto části:
- Část **Metoda zabezpečení ochrany dat pomocí vrstvené obrany** podává informace o otázkách spojených s vytvořením vyčerpávajícího plánu pro zabezpečení ochrany dat.
- Část **Strategie a cíle zabezpečení ochrany dat** podává informace, které vám pomohou lépe pochopit otázky spojené s vytvořením vyčerpávajícího plánu pro zabezpečení ochrany dat.
- Část **Scénář: Plán elektronického podnikání firmy JKL Toy** poskytuje praktický model typického využití Internetu a plánu pro zabezpečení ochrany dat, který můžete využít při tvorbě vlastního plánu.

I když tento produkt již není podporován, možná bude přesto užitečné, když si pro zdokumentování svých plánů upravíte a použijete pracovní formuláře pro plánování z produktu IBM Firewall for AS/400. Tyto pracovní formuláře vám pomohou shromáždit důležité, podrobné informace o vašich plánech na využití Internetu a konfiguraci interní sítě a také provést hodnocení požadavků pro zabezpečení ochrany dat. Přístup k těmto pracovním formulářům získáte z tématu Firewall: Getting started  ve verzi V4R5 aplikace Information Center iSeries. Ať už se rozhodnete použít nějaký produkt bezpečnostní bariéry (firewall) nebo ne, musíte při plánování strategie zabezpečení ochrany dat shromáždit zhruba stejná data.

Metoda zabezpečení dat pomocí vrstvené obrany

Strategie zabezpečení ochrany dat definuje to, co chcete ochránit a to, 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 vytvoření složitých hesel.

Poznámka: Ve své organizaci musíte vytvořit a prosadit strategii zabezpečení ochrany dat, která minimalizuje riziko pro vaši interní síť. Inherentní funkce zabezpečení dat serveru iSeries 400, jsou-li správně konfigurovány, vám poskytnou možnost minimalizovat mnohá rizika. Když připojíte systém iSeries k Internetu, musíte ovšem učinit další bezpečnostní opatření, aby byla zajištěna bezpečnost vaší 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 typická bezpečnostní rizika, se kterými se můžete setkat:

- **Pasivní napadení**: Při pasivním napadení vetřelec prostě 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. Měli byste proto předpokládat, že někdo špehuje 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 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 vetřelec pokouší zasahovat do vašich operací nebo je ukončit tak, že přesměruje provoz nebo zavalí systém spoustou nevyžádaných dat.
  - Při **šifrovacích napadeních** se vetřelec pokusí uhodnout nebo ukrást vaše hesla nebo použije specializované nástroje, aby dešifroval zašifrovaná data.

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. Místo toho byste měli předpokládat, že **určitě** dojde k problému se zabezpečením dat. 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 tyto 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 iSeries základních nastavení zabezpečení systému.

Zabezpečení na úrovni sítě
Opatření pro zabezpečení sítě řídí přístup k vašemu systému iSeries a k jiným systémům v síti. Když připojíte síť k Internetu, měli byste učinit odpovídající opatření pro zabezpečení na úrovni sítě vhodná k ochraně vašich interních prostředků v síti před neoprávněným přístupem a vniknutím. Nejběžnějším prostředkem pro zajištění bezpečnosti sítě je bezpečnostní bariéra (firewall). Poskytovatel služeb sítě Internet (ISP) by měl 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). Část

Zabezpečení na úrovni aplikace
Opatření pro zabezpečení na úrovni aplikace řídí, jak mohou uživatelé zacházet se specifickými aplikacemi. 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 pro zabezpečení na úrovni přenosu chrání 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.

Strategie a cíle zabezpečení ochrany dat

Uživatelská strategie zabezpečení ochrany dat

Každá internetová služba, kterou používáte nebo poskytujete, představuje riziko pro váš systém iSeries a pro síť, ke které 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 například zabezpečení dat zaměstnanců, administrativy a sítě.

Strategie zabezpečení ochrany dat definuje to, co chcete ochránit a to, 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 se někdo pokouší vaše zabezpečení obejít.

Při vyvíjení strategie zabezpečení ochrany dat musíte jasně definovat její cíle. Jakmile ji vytvoříte, musíte podniknout kroky, kterými se v ní obsažená pravidla budou realizovat. Mezi ně patří školení zaměstnanců a 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. To má zajistit, že postihnete případná nová rizika, která ze změn vyplynou. Pod tématem ″Basic system security and planning″ v rámci aplikace iSeries Information Center najdete příklad strategie zabezpečení ochrany dat firmy JKL Toy.

Úkoly vašeho zabezpečení ochrany dat

Když vytváříte a realizujete strategii zabezpečení ochrany dat, musíte mít jasný cíl. Úkoly zabezpečení ochrany dat spadají do jedné nebo více z těchto kategorií:

Ochrana prostředků
Plán ochrany prostředků zajistí, aby přístup k objektům v systému měli pouze oprávnění uživatelé. Schopnost zabezpečit všechny typy systémových prostředků je silnou stránkou serveru iSeries. 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 poskytnout bezpečnější metodu autentizace a přitom nabízejí 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, která se zakládají 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 uložených ve vaší síti budete možná potřebovat další zabezpečení dat, abyste zajistili integritu dat vstupujících do vašeho systému z nedůvěryhodných zdrojů. Když do vašeho systému vstupují data z veřejné sítě, budete potřebovat metody zabezpečení dat, abyste mohli udělat dále uvedené akce:
  - Ochránit data před “čmucháním” a interpretací, obvykle jejich zašifrováním.
  - 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, očekávané výsledky při očekávaném výkonu. U serveru iSeries je integrita systému nejčastěji přehlíženou komponentou zabezpečení ochrany dat, protože je základní součástí jeho architektury. Architektura serveru iSeries například vetřelcům nesmírně ztěžuje, aby imitovali nebo změnili program operačního systému, pokud používáte úroveň zabezpečení 40 nebo 50.

Neodmítání

Neodmítání je důkazem toho, že transakce proběhla nebo že jste odeslali nebo přijali zprávu. Použití digitálních certifikátů a kryptografie s veřejným klíčem k ″podpisu″ transakcí, zpráv a dokumentů neodmítání podporuje. 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 zabezpečené vrstvy SSL pomůže zajistit důvěrnost při přenosu dat přes nedůvěryhodné sítě. Strategie zabezpečení ochrany dat by se měla zabývat tím, jak zajistit důvěrnost informací ve vaší síti a také tehdy, když informace síť opustí.

Prověřování zabezpečovacích činností

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.

Pochopení cílů zabezpečení ochrany dat vám pomůže vytvořit strategii, která pokryje všechny potřeby zabezpečení ochrany dat ve vaší síti i v síti Internet. Při definování vašich cílů a vytváření strategie zabezpečení ochrany dat vás může inspirovat scénář elektronického podnikání firmy JKL Toy. Využití Internetu a plán zabezpečení ochrany dat společnosti ve scénáři je reprezentativní pro mnoho implementací z reálného světa.

Scénář: Plán elektronického podnikání firmy JKL Toy

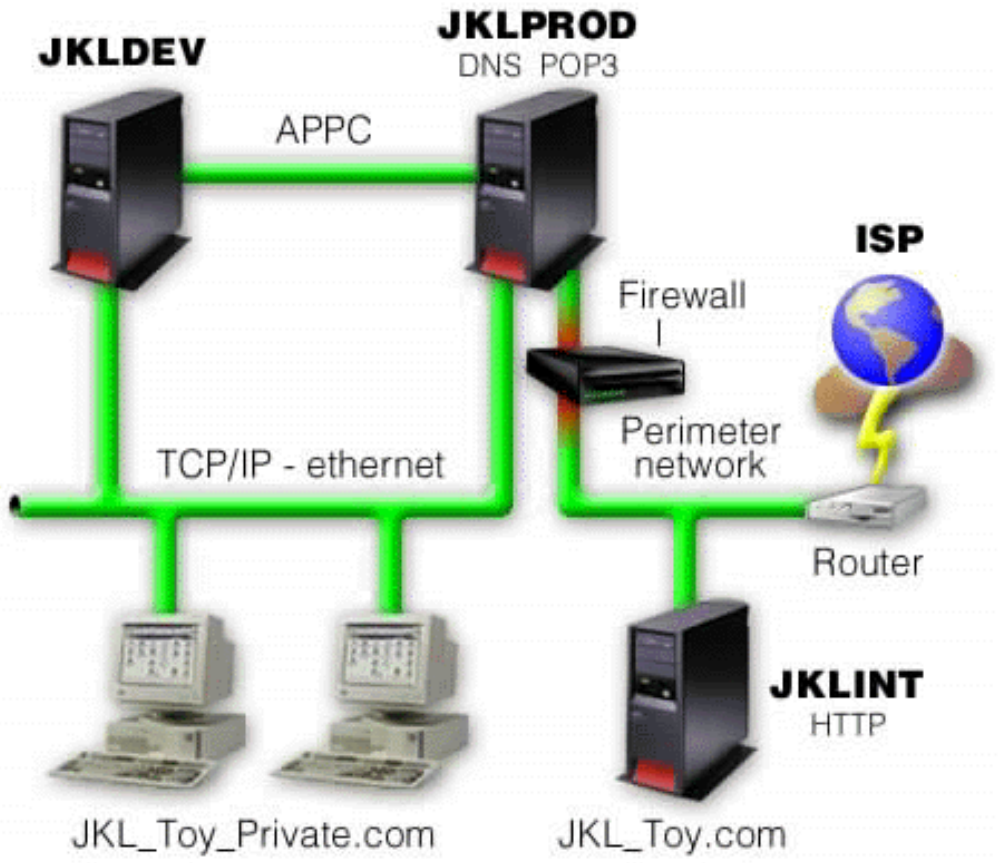
Tento scénář popisuje typickou firmu, JKL Toy, která se rozhodla rozšířit své obchodní záměry používáním sítě Internet. I když jde o fiktivní společnost, jsou její plány na využití sítě Internet pro elektronické podnikání a z toho vyplývající potřeby zabezpečení ochrany dat reprezentativní pro situaci mnoha firem v reálném světě.

Firma JKL Toy je malý, ale rychle rostoucí výrobce hraček od švihadel, přes draky až po vycpané leopardy na hraní. Prezident společnosti je nadšený růstem podniku a tím, jak jeho nový systém iSeries ulehčí zátěž, která s oním růstem souvisí. Sharon Jonesová, vedoucí účtárny, je zodpovědná za administraci systému iSeries a za jeho bezpečnost.

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 firma umožnit zaměstnancům ve vývojové laboratoři přístup k síti Internet za účely výzkumu a vývoje. A konečně chce firma umožnit, aby zákazníci používali její webovou stránku pro přímé online nákupy. Sharon pracuje na zprávě o specifických potenciálních rizicích těchto aktivit a o tom, jaká bezpečnostní opatření by měla firma podniknout, aby tato rizika minimalizovala. Sharon bude zodpovědná za aktualizaci strategie zabezpečení ochrany dat a za realizaci bezpečnostní opatření, která má firma v úmyslu použít.

Zvýšení přítomnosti 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.

Poté, co firma JKL Toy zajistila výrazné základní zabezpečení svých systémů iSeries, rozhodla se zakoupit a používat produkt bezpečnostní bariéry (firewall), která má zabezpečit ochranu na úrovni sítě. Bezpečnostní bariéra ochrání její interní síť před rizikem spojeným s používáním sítě Internet. Zde vidíte ilustraci konfigurace sítě Internet uvedené firmy.



Na diagramu vidíte, že firma JKL Toy má dva primární systémy iSeries. Jeden systém používá pro aplikace vývoje (JKLDEV) a druhý pro výrobní aplikace (JKLPROD). Oba systémy pracují se životně důležitými daty a aplikacemi. V důsledku toho firmě příliš nevyhovuje spouštět v těchto systémech internetové aplikace. Místo toho se rozhodla přidat nový systém iSeries (JKLINT), kde se takové aplikace budou spouštět.

Společnost umístila nový systém do hraniční sítě a používá bezpečnostní bariéru mezi ní a svou hlavní interní sítí, aby zajistila lepší oddělování mezi vlastní sítí a sítí Internet. Takové oddělování snižuje riziko plynoucí z použití Internetu, vůči kterému jsou její interní systémy zranitelné. Vymezením nového serveru iSeries jako výlučně internetového serveru snižuje firma také složitost správy zabezpečení své sítě.

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

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

Kapitola 5. Úrovně zabezpečení pro základní přípravu na Internet

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 OS/400. 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 máte systém vysoce orientovaný na transakce nebo aplikaci, která rozsáhle využívá integrovaný systém souborů, může provoz na úrovni zabezpečení 50 způsobit, že váš systém nebo aplikace zaznamenají snížení výkonu.

  Podrobnější informace o jednotlivých úrovních zabezpečení serveru iSeries najdete v publikaci Tips and Tools for Securing your iSeries.

  Poznámka: Jestliže v současné době pracujete na nižší úrovni zabezpečení než 50, budete muset aktualizovat buď obslužné procedury, nebo vlastní aplikace. Měli byste se podívat na informace v knize iSeries Security Reference ještě předtím, než přejdete na vyšší úroveň zabezpečení.
- Nastavte systémové hodnoty, které jsou důležité pro zabezpečení, aby vyjadřovaly alespoň taková omezení, jako doporučená nastavení. K porovnání vašich nastavení s doporučenými nastaveními můžete použít průvodce Operations Navigation Security Wizard nebo pomocný program Security Advisor z aplikace Technical Studio.
- 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 **musíte** nastavit oprávnění k objektu. Další informace o práci s oprávněním k objektu jsou v kapitole iSeries Navigator Tips and Tools for Securing your iSeries .

Při konfigurování těchto minimálních požadavků zabezpečení systému vám může pomoci buď pomocný program **Security Advisor** (dostupný z webové stránky aplikace Technical Studio), nebo průvodce **Security Wizard** (dostupný v prostředí produktu iSeries Navigator). Pomocný program Security Advisor v aplikaci Technical Studio 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. Průvodce Security Wizard také poskytuje doporučení na základě vašich odpovědí na řadu otázek. Na rozdíl od pomocného programu Security Advisor můžete průvodce použít k tomu, aby nastavení zabezpečení systému nakonfiguroval za vás.

Inherentní funkce zabezpečení dat severu iSeries, jsou-li správně konfigurovány a spravovány, vám poskytnou možnost minimalizovat mnohá rizika. Když však připojíte váš server iSeries k síti Internet, budete muset učinit další bezpečnostní opatření, aby byla zajištěna bezpečnost vaší interní sítě. Poté, co zajistíte, aby váš server iSeries měl dobré všeobecné zabezpečení systému, jste připraveni konfigurovat další bezpečnostní opatření jako součást vašeho celkového plánu zabezpečení využití Internetu.

Kapitola 6. Možnosti zabezpečení sítě

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

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

I když bezpečnostní 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 poskytnou více obranných vrstev proti takovým rizikům.

Bezpečnostní bariéra sice představuje obrovské zabezpečení proti určitým typům napadení, je však jen jednou součástí celkového řešení vaší bezpečnosti. Bezpečnostní 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 získat přístup, když putují Internetem na místo určení.

O použití nějakého produktu bezpečnostní bariéry (firewall) byste měli vážně uvažovat, kdykoli budete připojovat systém iSeries nebo svou interní síť k síti Internet. Ačkoli již není možné zakoupit produkt IBM Firewall for AS/400 a ani podpora produktu již není k dispozici, existuje mnoho jiných produktů, které můžete použít.

O přechodu ze stávajícího produktu IBM Firewall for AS/400 na jiné produkty nebo na funkce nativního zabezpečení sítě iSeries se dočtete v publikaci All You Need to Know When Migrating from IBM Firewall for AS/400  (SG24-6152).

Vzhledem k tomu, že komerční produkty bezpečnostních bariér poskytují celé spektrum technologií pro zabezpečení sítě, firma JKL Toy si vybrala jednu z nich pro svůj scénář zabezpečení elektronického podnikání, aby nastavila ochranu své sítě. Zvolená bezpečnostní bariéra však neposkytuje žádnou ochranu jejího nového internetového serveru iSeries. Proto se firma rozhodla implementovat funkci iSeries pravidla paketu za účelem vytvoření filtrů a pravidel NAT pro řízení provozu internetového serveru.

O pravidlech paketu systému iSeries

Pravidla pro filtrování paketu umožňují nastavit ochranu počítačových systémů 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 produkt firewall. Při rozhodování mezi kompletním produktem bezpečnostní bariéry (firewall) a funkcí pravidel paketu iSeries byste měli pečlivě analyzovat požadavky a cíle vašeho zabezpečení dat.

Část Výběr vhodných voleb pro zabezpečení sítě iSeries vám pomůže při rozhodování, který přístup odpovídá potřebám vašeho zabezpečení ochrany dat.

Bezpečnostní bariéra

Bezpečnostní bariéra (firewall) je blokáda mezi zabezpečenou sítí a nedůvěryhodnou sítí, jakou je například Internet. Většina společností používá bezpečnostní bariéru k bezpečnému připojení interní sítě k Internetu, i když ji lze použít také k zabezpečení jedné interní sítě před druhou.

Bezpečnostní bariéra poskytuje jediný řízený bod kontaktu mezi vaší zabezpečenou interní sítí a nedůvěryhodnou sítí, nazývaný jako ″chokepoint″. Bezpečnostní bariéra:
- 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 bezpečnostní bariéru jako bránu do sítě Internet (nebo do jiné sítě), podstatně snižujete riziko hrozící interní síti. Použití bezpečnostní bariéry usnadňuje i správu zabezpečení sítě, protože její funkce provádějí mnoho direktiv vaší strategie zabezpečení ochrany dat.

Jak pracuje bezpečnostní bariéra

Chcete-li pochopit, jak bezpečnostní 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 bezpečnostní bariéry

Bezpečnostní 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 bezpečnostní bariéry obvykle tvoří samostatný počítač nebo zařízení vyhrazené pro provádění softwarových funkcí bariéry.
- Software. Software bezpečnostní bariéry nabízí celou řadu aplikací. V kontextu zabezpečení sítě poskytuje bezpečnostní bariéra prostřednictvím různých technologií tyto bezpečnostní kontroly:
  - Filtrování IP paketů.
  - Služby NAT (převod síťových adres).
  - Server SOCKS.
  - Proxy servery pro nejrůznější služby, jako například HTTP, Telnet, FTP, atd.
  - Služby přenosu pošty.
  - Rozdělení - DNS.
  - Protokolování.
  - Monitorování v reálném čase.

Poznámka: Některé bezpečnostní bariéry poskytují služby VPN (virtuální soukromé sítě), takže můžete nastavit zašifrované relace mezi vaší bezpečnostní bariérou a jinými kompatibilními bariérami.

Použití technologií bezpečnostní bariéry

Pomocí proxy serverů, serveru SOCKS nebo pravidel NAT bezpečnostní bariéry můžete interním uživatelům poskytnout bezpečný přístup k službám sítě Internet. Proxy server a server SOCKS přeruší spojení TCP/IP u bezpečnostní 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 bezpečnostní bariérou. Bezpečnostní bariéra přesto vaši síť ochrání, protože NAT skryje interní IP adresy.

Bezpečnostní 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 bezpečnostní 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 bezpečnostní 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 bezpečnostní 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 bezpečnostní 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 bezpečnostní bariéra ochránit vaši síť

Bezpečnostní bariéru instalujete mezi vaši síť a bod připojení k Internetu (nebo jiné nedůvěryhodné síti). Bariéra pak umožňuje, abyste omezili vstupní body do vaší sítě. Bezpečnostní bariéra poskytuje jediný bod kontaktu 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.

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

Bezpečnostní 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 bezpečnostní bariéra pro ochranu vaší sítě nemůže udělat

Bezpečnostní bariéra sice představuje obrovské zabezpečení proti určitým typům napadení, je však jen jednou součástí celkového řešení vaší bezpečnosti. Bezpečnostní 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 získat přístup, když putují Internetem na místo určení.

Pravidla paketu systému iSeries

Pravidla paketů systému iSeries 400 je integrovaná funkce systému OS/400 dostupná z prostředí produktu Operations Navigator. Funkce pravidel paketu umožňuje konfigurovat na ochranu vašeho systému iSeries dvě základní technologie pro zabezpečení sítě, které řídí provoz TCP/IP:

- Převod síťových adres (NAT).
- Filtrování IP paketu.

Protože jsou NAT a filtrování IP paketu integrální součástí systému OS/400, nabízejí úsporný způsob, jak systém zabezpečit. V některých případech mohou tyto bezpečnostní technologie obstarat všechno, co potřebujete a nemusíte nic dalšího kupovat. Tyto technologie však nevytvářejí opravdovou funkční bezpečnostní bariéru (firewall). Zabezpečení IP paketů můžete použít samostatně nebo ve spojení s bezpečnostní bariérou podle požadavků a cílů vaší ochrany.

Poznámka: Jestliže plánujete zabezpečení provozního systému iSeries, neměli byste se pokoušet využívat výhody úspory nákladů. V podobných situacích by mělo mít zabezpečení vašeho systému přednost před náklady. Chcete-li pro váš provozní systém zajistit maximální možnou ochranu, měli byste uvažovat o použití bezpečnostní bariéry (firewall).

Co je to NAT a filtrování IP paketu a jakým způsobem tyto funkce spolupracují?

Převod síťových adres (NAT) změní zdrojové nebo cílové IP adresy paketů, které procházejí systémem. NAT nabízí transparentnější alternativu serverů proxy a serverů a SOCKS serverů bezpečnostní 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 systém iSeries fungoval jako brána mezi dvěma sítěmi, které mají konfliktní nebo nekompatibilní schéma 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 bezpečnostní bariérou. Veřejné IP adresy pro webový server se převádějí na soukromé 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 paketu nabízí schopnost selektivně zablokovat nebo ochránit provoz IP na základě informací v záhlaví paketů. K rychlému a snadnému nakonfigurování základních filtrovacích pravidel a zablokování nežádoucího provozu v síti můžete použít průvodce Internet Setup Wizard v prostředí produktu Operations 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.
- Specifikujte, zda filtrovací pravidlo vytvoří záznam v protokolu systémového deníku o paketech, které pravidlu odpovídají. Jakmile se informace zapíší do systémového deníku, nemůžete již záznam v protokolu změnit. Díky tomu je protokol ideálním nástrojem pro prověřování aktivity sítě.

Výběr voleb zabezpečení sítě iSeries

Řešení zabezpečení sítě, která chrání před neoprávněným přístupem, obvykle spoléhají na technologie bezpečnostní bariéry (firewall). Chcete-li nastavit ochranu systému iSeries 400, můžete se rozhodnout pro použití plně funkční bezpečnostní bariéry (firewall) nebo pro specifické technologie zabezpečení sítě, které jsou součástí implementace OS/400 TCP/IP. Tato implementace se skládá z funkce pravidel paketu (zahrnuje filtrování IP a NAT) a z funkce proxy serveru HTTP for iSeries.

Volba mezi použitím funkce pravidel paketů nebo bezpečnostní bariéry záleží na prostředí vaší sítě, přístupových požadavcích a potřebách zabezpečení. O použití nějakého produktu bezpečnostní bariéry byste měli **vážně** uvažovat, kdykoli budete připojovat systém iSeries nebo svou interní síť k Internetu nebo jiné nedůvěryhodné síti.

Bezpečnostní bariéra je v tomto případě vhodnější, protože je to typicky jednoúčelové hardwarové a softwarové zařízení s omezeným počtem rozhraní pro externí přístup. Když použijete technologie OS/400 TCP/IP pro ochranu přístupu k Internetu, používáte univerzální počítačovou platformu s nesčíslným počtem rozhraní a aplikací otevřených externímu přístupu.

Tento rozdíl je důležitý z mnoha důvodů. Produkt jednoúčelové bezpečnostní bariéry například neposkytuje žádné další funkce ani aplikace mimo ty, které patří k samotné bariéře. Proto, i kdyby vetřelec bezpečnostní bariéru úspěšně obešel a získal k ní přístup, nemohl by toho moc udělat. Naopak, kdyby obešel funkce zabezpečení TCP/IP na serveru iSeries, mohl by mít potenciálně přístup k různým užitečným aplikacím, službám a datům. Vetřelec je může použít a způsobit škody v samotném systému anebo získat přístup k dalším systémům ve vaší interní síti.

Je tedy vůbec někdy přijatelné použít funkce zabezpečení dat iSeries TCP/IP? Jako u každého rozhodování ve věcech ochrany, musíte svá rozhodnutí založit na poměru získaného prospěchu vůči nákladům, které jste ochotni vynaložit. Musíte analyzovat cíle svého podnikání a rozhodnout, jaké riziko jste ochotni přijmout v poměru k nákladům na to, jakým zabezpečením chcete riziko minimalizovat. Následující tabulka nabízí informace o tom, kdy je odpovídající použít funkce zabezpečení dat TCP/IP oproti plně funkčnímu zařízení firewall. Tabulku můžete použít k rozhodnutí, zda byste měli k zabezpečení sítě a ochraně systému použít firewall, funkce zabezpečení dat TCP/IP nebo kombinaci obou přístupů.

Technologie zabezpečení ochrany dat	Nejlepší použití technologie OS/400 TCP/IP	Nejlepší použití plně funkční bezpečnostní bariéry
Filtrování IP paketu	• Poskytnout **přídavnou** ochranu pro jediný systém iSeries, jako například veřejný webový server nebo systém intranet s citlivými daty. • Chránit dílčí síť společné sítě **intranet**, když systém iSeries působí jako brána (příležitostný směrovač) do zbývající části sítě. • Řídit komunikaci s poněkud důvěryhodným partnerem přes **soukromou síť** nebo extranet, kde systém iSeries působí jako brána.	• Chránit celou společnou síť proti síti **Internet** nebo jiné nedůvěryhodné síti, ke které je vaše síť připojena. • Chránit velkou dílčí síť před hustým provozem ze zbývající části společné sítě.
NAT (převod síťových adres)	• Umožnit spojení dvou **soukromých sítí** s nekompatibilní strukturou adresování. • Skrýt adresy dílčí sítě před méně důvěryhodnou sítí.	• Skrýt adresy klientů přistupujících k síti **Internet** nebo jiné nedůvěryhodné síti. Použít jako alternativu k serverům proxy a SOCKS. • Zpřístupnit služby nějakého systému v soukromé síti klientům v síti **Internet**.
Proxy server	• Fungovat jako proxy server ve **vzdálených systémech** ve společné síti, když centrální bezpečnostní bariéra poskytuje přístup k síti Internet.	• Fungovat jako proxy server pro celou společnou síť při přístupu k síti **Internet**.

Další informace o používání funkcí zabezpečení dat OS/400 TCP/IP najdete v těchto zdrojích:
- Packet rules (filtering and NAT).
- HTTP Server Documentation Center. .
- AS/400 Internet Security Scenarios: A Practical Approach (SG24-5954).

Kapitola 7. Volby zabezpečení aplikací

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 v síti Internet 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.

I když je důležité zabezpečit každou aplikaci, kterou používáte, hrají tato bezpečnostní opatření malou úlohu v implementaci celkové strategie zabezpečení ochrany dat.

Další informace o tom, co byste měli udělat pro zabezpečení některých běžných aplikací v síti Internet, najdete v níže uvedených částech:
- “Zabezpečení webových služeb”
- “Zabezpečení Internetu a Java” na stránce 26
- “Zabezpečení elektronické pošty” na stránce 29
- “Zabezpečení protokolu FTP” na stránce 30

Zabezpečení webových služeb

Když poskytujete návštěvníkům přístup ke svým webovým stránkám, nechcete jim samozřejmě odhalovat informace o tom, jak jsou vaše stránky nastaveny a jaké kódování je použito k jejich vygenerování. Chcete, aby pro ně byla návštěva vašich stránek snadná, rychlá a bezproblémová a aby veškerá práce byla prováděna skrytě. Jako administrátorovi vám jistě záleží na tom, aby zvolené metody zabezpečení negativně neovlivňovaly vaše webové stránky. Pokud jako webový server používáte iSeries 400, uvažte následující body:

- Než dojde k interakci mezi klientem a HTTP serverem, musí administrátor serveru definovat pro server určité směrnice. Existují dvě metody pro vytvoření bezpečnostních kontrol: všeobecné směrnice pro server a směrnice pro ochranu serveru. Každý požadavek vůči webovému serveru musí splňovat všechna omezení obsažená v těchto směrnicích. Teprve pak je serverem akceptován.
- Tyto směrnice můžete vytvářet a editovat pomocí administračních webových stránek určených pro konfigurování serveru. Směrnice pro server vám umožňují řídit veškeré chování webového serveru. Směrnice pro ochranu serveru dovolují specifikovat a řídit modely zabezpečení ochrany dat, které server používá pro specifické adresy URL, s nimiž webový server pracuje.
- Při konfiguraci serveru můžete použít směrnice typu ″map″ a směrnice typu ″pass″ a dále webové stránky pro administraci serveru.
  - Směrnice typu ″map″ a ″pass″ slouží k maskování jmen souborů na vašem webovém serveru iSeries. Konkrétně se jedná o směrnice serveru PASS a směrnice serveru MAP, které řídí adresáře, z nichž webový server obsluhuje URL. Můžete se setkat rovněž s se směrnicí serveru EXEC, která řídí knihovny, v nichž jsou uloženy programy CGI-BIN.

    Směrnice pro ochranu definujete pro každou adresu URL serveru. Ne všechny adresy URL vyžadují směrnici pro ochranu. Pokud však chcete řídit to, kdo a jak přistupuje ke zdroji adresy URL, je směrnice pro ochranu dané adresy URL nezbytná.
  - Namísto použití příkazu WRKHTTPCFG (Work with HTTP Configuration) a psaní směrnic máte také možnost použít ke konfigurování serveru webové stránky pro administraci serveru. Práce se směrnicemi pro ochranu prostřednictvím rozhraní příkazové řádky může být velmi složitá. Z toho důvodu doporučujeme, abyste raději použili administrační webové stránky a zajistili tak správné nastavení vašich směrnic.

Protokol HTTP vám poskytuje schopnost zobrazovat data, nikoliv však možnost upravovat data v databázových souborech. Nicméně některé aplikace, které napíšete, budou vyžadovat aktualizaci databázového souboru. V takových případech se využívají programy CGI-BIN. Například budete potřebovat vytvořit formuláře a poté, co je uživatelé vyplní, jimi aktualizovat databázi iSeries. Jako administrátor systému byste měli monitorovat autorizace tohoto uživatelského profilu a funkce, které programy CGI provádějí. Také byste měli zhodnotit, které citlivé objekty by mohly mít nepřiměřené veřejné oprávnění.

Poznámka: Rozhraní CGI (Common Gateway Interface) je průmyslovým standardem pro výměnu informací mezi webovým serverem a počítačovými programy, které jsou vůči němu externí. Programy mohou být napsány v libovolném programovacím jazyce, který je podporován operačním systémem, pod nímž se webový server spouští.

Kromě programů CGI můžete chtít na svých webových stránkách používat také programovací jazyk Java. Dříve, než přidáte Javu do svých webových stránek, byste měli chápat zabezpečení dat v Javě.

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

Proxy server přijímá požadavky HTTP z prohlížečů WWW a přeposílá je webovým serverům. Webové servery, které tyto požadavky přijímají, znají pouze IP adresu proxy serveru. Nemohou zjistit jména nebo adresy těch PC, od nichž požadavky vzešly. Proxy server může pracovat s požadavky URL pro HTTP, FTP (File Transfer Protocol), Gopher a WAIS.

Můžete rovněž použít podporu HTTP proxy, kterou poskytuje server IBM HTTP Server for iSeries  ke konsolidaci přístupu k WWW. Proxy server může také zaznamenávat všechny požadavky URL, které slouží pro účely sledování. Vzniklé protokoly vám pak pomohou monitorovat používání a nesprávné používání (zneužívání) síťových prostředků.

Podrobné informace k této problematice obsahuje kniha *Tips and Tools for Securing Your iSeries*. 

Zabezpečení Internetu a Java

Programování v Javě je v současném světě počítačového zpracování stále rozšířenější. K vývoji nových aplikací ve vašem systému můžete například používat aplikaci IBM Toolbox for Java či IBM Development Kit for Java. Proto musíte být připraveni zabývat se bezpečnostními otázkami, které s Javou souvisejí. Ačkoliv bezpečnostní bariéra (firewall) představuje dobrou ochranu před nejběžnějšími bezpečnostními riziky na Internetu, nezajišťuje ochranu proti řadě rizik, které s sebou použití Javy přináší. Vaše strategie zabezpečení ochrany dat by měla zahrnovat podrobné zpracování ochrany systému před třemi Javy: aplikacemi, applety a servlety. Také byste si měli ujasnit, jakým způsobem probíhá interakce mezi Javou a zabezpečením dat na úrovni prostředků ve smyslu autentizace a autorizací u programů v Javě.

Aplikace v Javě

Jako programovací jazyk má Java některé charakteristiky, které zabraňují javovským programátorům dělat neúmyslné chyby, jež by mohly vést k problémům s integritou. (Ostatní jazyky běžně používané pro PC aplikace, jako jsou např. C nebo C++, nechrání programátory před bezděčnými chybami v takové míře jako Java.) Java například ″strong typing″, díky němuž je programátorovi znemožněno používat objekty neočekávaným způsobem. Java

nedovoluje práci s ukazovátkem, v důsledku čehož programátor nemůže nechtěně přesáhnout hranice paměti daného programu. Z hlediska vývoje aplikací lze na Javu pohlížet jako na jakýkoliv jiný vyšší programovací jazyk. Při návrhu aplikací byste měli používat stejná pravidla pro zabezpečení ochrany dat, jaká používáte u ostatních programovacích jazyků v systému iSeries 400.

Java applety

Java applety jsou malé javovské programy, které můžete zahrnout do svých HTML stránek. Jelikož jsou applety prováděny na klientovi, jde to, co tyto applety učiní, na vrub klienta. Java applet však má jisté možnosti přístupu do vašeho systému iSeries 400. (Rovněž program ODBC nebo APPC (advanced program-to-program communications) spouštěný na nějakém PC ve vaší síti může mít přístup do vašeho systému iSeries.) Obecně řečeno mohou Java applety vytvořit relaci pouze se serverem, z něhož byly spuštěny. Z toho důvodu může mít Java applet přístup do vašeho systému iSeries z PC pouze tehdy, když pochází z vašeho systému iSeries (např. z webového serveru).

Applet se může pokusit připojit k libovolnému portu TCP/IP na serveru. Nemusí nutně komunikovat se softwarovým serverem, který je napsán v Javě. Avšak v případě serverů napsaných pomocí aplikace IBM Toolbox for Java musí applet poskytnout ID a heslo uživatele, chce-li vytvořit připojení zpět do serveru. Všechny servery popsané v tomto dokumentu jsou servery iSeries. (Server napsaný v Javě 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 provádět funkce v systému iSeries pouze za předpokladu, že má uživatelský profil k těmto funkcím autorizaci. 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 v profilu daného uživatele.

Prohlížeč appletů vám umožní testovat applet v systému serveru. Applet však není předmětem bezpečnostních omezení prohlížeče. Z toho důvodu byste měli prohlížeč appletů používat pouze k testování vašich vlastních appletů, v žádném případě ke spouštění appletů z cizích zdrojů. Java applety často zapisují na pevný disk PC uživatele a dostávají tak příležitost provádět destruktivní činnost. Vy však můžete použít digitální certifikát, který dá Java appletu pokyn, aby provedl autentizaci (prokázal svou pravost). Podepsaný applet může zapisovat na lokální jednotky PC, třebaže to předvolené nastavení prohlížeče nedovoluje. Podepsaný applet může rovněž zapisovat na mapované jednotky ve vašem systému iSeries, jelikož se vůči PC jeví jako lokální jednotky.

Poznámka: Výše popisované chování je obecně platné pro Netscape Navigator a MS Internet Explorer. To, co se děje ve skutečnosti, závisí na tom, jak máte nakonfigurovány a spravovány vámi používané prohlížeče.

U Java appletů, které pocházejí z vašeho systému iSeries, budete možná potřebovat používat podepsané applety. Přesto byste měli instruovat své uživatele, aby běžně nepřijímali podepsané applety z neznámých zdrojů.

Počínají verzí V4R4 můžete použít aplikaci IBM Toolbox for Java k nastavení prostředí SSL (Secure Sockets Layer). K zajištění ochrany aplikace v Javě prostřednictvím SSL lze také využít aplikaci IBM Developer Toolkit for Java. Použití SSL s vašimi aplikacemi v Javě zajišťuje kódování dat včetně ID a hesel uživatelů, která se předávají mezi klientem a serverem. Chcete-li nakonfigurovat registrované programy v Javě tak, aby používaly SSL, můžete k tomu použít produkt DCM (Digital Certificate Manager).

Java servlety

Servlety představují komponenty na straně serveru, které jsou napsány v Javě a které dynamicky rozšiřují funkčnost webového serveru, aniž by bylo nutné měnit kód webového serveru. Server IBM WebSphere Application Server dodávaný se serverem IBM HTTP Server for iSeries poskytuje podporu pro použití servletů v systémech iSeries.

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. Kromě toho byste měli řídit, kdo může spouštět servlet (maskovat klíčová slova ve směrnici pro ochranu), a to prostřednictvím skupin a přístupových seznamů (ACL) HTTP serveru. Také byste měli využívat funkcí zabezpečení dat poskytovaných vašimi nástroji pro vývoj servletů, jako jsou např. funkce v aplikaci WebSphere Application Server for iSeries.

V následujících zdrojích najdete podrobnější informace o obecných bezpečnostních opatřeních pro Javu:
- IBM Developer Kit for Java zabezpečení dat a Java.
- IBM Toolbox for Java třídy zabezpečení.
- Tips and Tools for Securing Your iSeries  .

Autentizace a autorizace Javy vůči prostředkům

Aplikace IBM Toolbox for Java obsahuje třídy zabezpečení sloužící k ověření identity uživatele a k volitelnému přiřazení této identity vláknu (thread) operačního systému pro aplikaci nebo servlet spuštěný v systému iSeries. Následné kontroly zabezpečení dat na úrovni prostředků pak probíhají pod touto přiřazenou identitou. Další informace o těchto třídách zabezpečení viz IBM Toolbox for Java Authentication Services.

Aplikace IBM Developer Kit for Java poskytuje podporu pro službu JAAS (Java Authentication and Authorization Service), která je standardním rozšířením k 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). Více informací o používání produktu J2SDK viz Java Authentication and Authorization Service.

Zabezpečení aplikací v Javě pomocí SSL

Komunikace pro aplikace iSeries, které byly vyvinuty pomocí aplikace IBM Developer Kit for Java, můžete zabezpečit prostřednictvím SSL (Secure Sockets Layer). Výhod SSL mohou využívat také klientské aplikace, které používají aplikaci IBM Toolbox for Java. Proces aktivace SSL u vašich vlastních aplikací v Javě se liší od aktivace u jiných aplikací.

Další informace o administraci SSL pro aplikace v Javě obsahují tato témata v rámci aplikace Information Center:
- IBM Toolbox for Java Secure Sockets Layer (SSL) environment .
- IBM Developer Toolkit for Java to make a Java application secure with SSL.

Zabezpečení elektronické pošty

Použití elektronické pošty v síti Internet nebo v jiné nedůvěryhodné síti představuje bezpečnostní riziko, před kterým vás bezpečnostní bariéra (firewall) nemusí ochránit. 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. Je tomu tak proto, že vaše elektronická pošta prochází mnoha servery, než se k vám dostane, a 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 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 vyhmátnout 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 zabezpečit potřebnou ochranu. Například aplikace Lotus Notes Domino nabízí několik integrovaných funkcí zabezpečení dat včetně schopnosti šifrování celého dokumentu nebo jeho jednotlivých polí.

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 poštu použije Lotus Notes Domino veřejný klíč odesilatele k jejímu dešifrování.

Informace o používání funkce Lotus Notes pro kódování dat najdete v online nápovědě k tomuto programu.

Podrobnější informace o zabezpečení u produktu Domino v systému iSeries najdete v těchto tématech:

- Lotus Domino reference library.
- Lotus Notes user assistance web site.
- Lotus Notes and Domino R5.0 Security Infrastructure Revealed (SG24-5341).
- Lotus Domino for AS/400 Internet Mail and More (SG24-5990).

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.

Jinou možností je nakonfigurovat připojení virtuální soukromé sítě (VPN). Od verze V4R4 můžete použít server iSeries a nakonfigurovat různá připojení VPN také mezi vzdálenými klienty a vaším systémem iSeries. Když používáte VPN, je veškerý provoz plynoucí mezi komunikujícími koncovými body zašifrovaný, což zaručuje důvěrnost a integritu dat.

Zabezpečení protokolu FTP

Protokol FTP (File Transfer Protocol) poskytuje schopnost přenosu souborů mezi klientem (uživatelem v jiném systému) a vaším serverem. 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. Těmto rizikům musíte porozumět, abyste zajistili, že vaše strategie zabezpečení ochrany dat zabezpečí minimalizaci rizika.

- 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 iSeries (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 zabezpečení poskytovanému programem menu. Mnoho zákazníků by asi chtělo, aby řízení přístupu FTP bylo ještě restriktivnější. Tato volba se týká pouze FTP, ne ostatních rozhraní, jako například ODBC, DDM nebo DRDA.

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

- Hacker může provést útok s následkem ″přerušení síťových služeb″ a přimět váš server FTP, 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 hackerům 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 programem 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.

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.

Od verze V5R1 můžete pro zabezpečení komunikačních relací vašeho serveru FTP používat 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.

Chcete-li se dovědět více o použití FTP, rizicích a dostupných bezpečnostních opatřeních, prostudujte si tyto zdroje:
- Implementing FTP security.
- Anonymous FTP.
- Securing FTP.
- Tips and Tools for Securing your iSeries  .

Kapitola 8. Volby zabezpečení přenosu dat

Připomeňte si, že ve scénáři má firma JKL Toy dva primární systémy iSeries 400. Jeden používá pro vývoj a druhý pro výrobní aplikace. Oba systémy pracují s životně důležitými daty a aplikacemi. Proto se rozhodla přidat do okrajové sítě nový systém iSeries, který by pracoval s jejich aplikacemi v síti intranet a Internet.

Vytvoření okrajové sítě zajistí určité fyzické oddělení interní sítě firmy od sítě Internet. Takovéto oddělení snižuje riziko plynoucí z použití Internetu, vůči kterému jsou interní systémy firmy zranitelné. Vymezením nového serveru iSeries 400 jako výlučně internetového serveru snižuje firma také složitost správy zabezpečení své sítě.

Vzhledem k naléhavé potřebě ochrany dat v prostředí sítě Internet pracuje 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 v nedůvěryhodných systémech můžete minimalizovat pomocí dvou produktů pro zabezpečení systému iSeries na úrovni přenosu: zabezpečení komunikací pomocí SSL (Secure Sockets Layer) a připojení VPN (virtuálních soukromých sítí).

Zabezpečení aplikací pomocí SSL

Protokol SSL (Secure Sockets Layer) je de facto odvětvová norma pro zabezpečení komunikace mezi klienty a servery. Protokol SSL byl původně vyvinut pro aplikace prohlížeče WWW, ale v současné době jej může používat stále rostoucí počet aplikací. V systému iSeries mezi ně patří:

- Server IBM HTTP Server for iSeries (původní a provozovaný na bázi Apache).
- Server FTP.
- Server Telnet.
- DRDA (Distributed relational database architecture) a DDM (distribuovaný systém řízení dat).
- Server (DDM).
- Centrální správa.
- Server LDAP (Directory Services Server).
- Aplikace Client Access Express, včetně produktu Operations Navigator, a aplikace, které jsou zapisovány do sady rozhraní API programu Client Access Express.
- 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, které používají SSL, viz téma Secure Sockets Layer APIs.

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

VPN iSeries

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

Jakou metodu byste měli použít?

Obě tyto metody zabezpečení se zabývají potřebami zajištění autentizace, důvěrnosti a integrity dat. To, kterou z těchto metod byste měli použít, závisí na několika faktorech. Mezi faktory, které je nutno vzít v úvahu, patří to, s kým komunikujete, jaké aplikace pro tuto komunikaci používáte, jak zabezpečené musí komunikace být a jaká zvýhodnění na úkor nákladů a výkonu jste ochotni udělat, aby tato komunikace byla zajištěna.

Rovněž, chcete-li použít specifickou aplikaci se SSL, musí být tato aplikace na použití SSL nastavena. Ačkoliv mnohé aplikace ještě nemohou využívat výhody SSL, mnoho jiných, jako je Telnet a Client Access Express, již tuto schopnost mají. Na druhé straně vám VPN umožňuje chránit veškerý provoz IP, který postupuje mezi koncovými body specifického spojení.

Můžete například použít HTTP přes SSL a umožnit tak běžně 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, budete muset spojení VPN přece jen použít. Může také nastat situace, 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.

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. Server iSeries 400 nabízí možnost snadno vytvářet a spravovat digitální certifikáty pro vaše systémy a uživatele pomocí DCM (Digital Certificate Manager), integrované funkce systému OS/400.

Dále můžete konfigurovat některé aplikace, jako například IBM HTTP Server for iSeries, aby používaly certifikáty jako účinnější metodu ověřování klienta místo jména uživatele 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 jako **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 serveru, 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. Vlastník certifikátu může tyto klíče použít k

″podpisu″ a zašifrování dat, jako jsou například zprávy a dokumenty odesílané mezi uživateli a servery. Digitální podpisy zajišťují spolehlivost původu položky a chrání její integritu.

Ačkoliv mnohé aplikace ještě nemohou využívat výhody SSL, mnoho jiných, jako je Telnet a Client Access Express, již tuto schopnost mají. Chcete-li se dovědět, jak použít SSL u aplikací iSeries, přečtěte si téma **Securing applications with SSL** v aplikaci iSeries Information Center.

Zabezpečený přístup k Telnet pomocí SSL

Od verze V4R4 můžete konfigurovat server Telnet, aby používal SSL (Secure Sockets Layer) pro komunikační relace se zabezpečeným serverem Telnet. 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 kromě autentizace serveru data zašifrují předtím, než dojde k řízení toku dat protokolem Telnet. Jakmile se relace SSL zavede, zašifrují se všechny protokoly Telnet, včetně uživatelského ID a výměny 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 iSeries Telnet tak, aby používal SSL. Když pro aplikaci serveru Telnet nakonfigurujete digitální certifikát, je Telnet schopen obsluhovat jak klienty, kteří mají SSL, tak klienty, kteří 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. Porty je možné uzavřít příkazem ADDTCPPORT. Jakmile port vypnete, poskytuje server klientům Telnet bez SSL a relace SSL Telnet jsou zablokované.

Další informace o serveru Telnet a rady k zabezpečení dat na serveru Telnet používajícím SSL i bez SSL uvádějí tyto zdroje:

- Téma Telnet v aplikaci Information Center poskytuje informace, které potřebujete při používání serveru Telnet v systému iSeries.
- Téma Securing Telnet podává informace použití SSL na serveru Telnet pro zabezpečení komunikačních relací Telnet.
- Publikace Tips and Tools for Securing Your iSeries  poskytuje podrobné informace zabezpečení dat na serveru Telnet v sekci TCP/IP.

Zabezpečení produktu Client Access Express pomocí SSL

Od verze V4R4 můžete konfigurovat server Client Access Express, aby používal SSL (Secure Sockets Layer) pro komunikační relace se zabezpečeným serverem Client Access Express. Například, jak se firma JKL Toy rozrůstala, přibylo k zaměstnancům hodně regionálních obchodních agentů. Tito prodejci potřebují přístup k informacím z provozního systému iSeries ve svých domovských kancelářích, aby věděli, které hračky jsou k dostání a znali data výroby. Protože jsou tyto údaje citlivé, rozhodla se firma JKL Toy povolit prodejcům přístup k informacím jedině prostřednictvím zabezpečeného produktu Client Access Express.

Použití SSL zajistí, aby byl veškerý provoz u relací Client Access Express zašifrovaný. To znemožňuje přečíst data procházející mezi lokálními a vzdálenými uzly.

Další informace o použití Client Access Express se SSL najdete v těchto zdrojích:

- Secure Sockets Layer Administration.
- Securing Client Access Express and Operations Navigator.
- IBM Developer Kit for Java SSL.
- IBM Java Toolbox SSL.

Zabezpečení soukromých komunikací pomocí VPN

Protože firma JKL Toy stále větší měrou používá virtuální soukromé sítě (VPN) a zabezpečení ochrany dat, které nabízejí, hledá nyní možnost přenosu dat prostřednictvím sítě Internet. Nedávno koupila další malou firmu na výrobu hraček a chce ji provozovat jako svou pobočku. Firma JKL Toy bude potřebovat předávat si s pobočkou informace. Obě firmy používají systém iSeries a použití připojení VPN může zajistit zabezpečení dat potřebné pro komunikaci mezi oběma sítěmi. Vytvoření VPN je z hlediska nákladů výhodnější než tradiční pronajaté linky.

Připojením VPN můžete řídit a zabezpečit spojení s kancelářemi pobočky, mobilními zaměstnanci, dodavateli, obchodními partnery a dalšími osobami.

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 připojení 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 společná data, 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. Připojení VPN nabízejí řešení specifické potřeby ochrany dat: zabezpečení komunikace mezi systémy. Připojení 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.

Virtuální soukromé sítě 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. Připojení VPN může zakódovat data, která procházejí veřejnými sítěmi. Ale podle toho, jak je nakonfigurujete, nemusí připojení VPN zašifrovat data procházející přes interní sítě, které s tímto připojením komunikují. V důsledku toho byste měli pečlivě naplánovat, jak jednotlivá připojení 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 připojení VPN. Nechcete však, aby měl přístup k jiným systémovým prostředkům, jako například k samotné databázi. Naštěstí můžete připojení 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 připojením VPN, zabezpečuje toto připojení ochranu na úrovni sítě. VPN však nepracuje stejným způsobem jako bezpečnostní bariéra při regulaci provozu do systému a ze systému. Připojení VPN není také jediným dostupným prostředkem pro zabezpečení komunikace mezi vaším serverem iSeries a jinými systémy. Podle potřeb vašeho zabezpečení ochrany dat můžete dojít k závěru, že vám lépe vyhovuje použití SSL.

To, zda připojení 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 připojení VPN podporuje strategii zabezpečení ochrany vašich dat.

Kapitola 9. Terminologie zabezpečení Internetu

Základem pro diskusi o zabezpečení Internetu je definovat některé termíny, které se Internetu týkají. Jestliže jste v této oblasti již poučeni, můžete tuto kapitolu přeskočit.

Authentication (autentizace)
Autentizace je ověření, vzdálený klient je skutečně tím, co tvrdí. Autentizace zajistí, že můžete důvěřovat vzdálenému serveru peer, ke kterému se připojujete.

Cracker
Počítačový fanda, který má špatné úmysly.

Cryptography (šifrování)
Schopnost zabezpečit data. Šifrování umožňuje ukládat informace nebo komunikovat s jinými účastníky a zajistit, aby účastníci, kterých se to netýká, uloženým informacím ani vaší komunikaci neporozuměli. Šifrování transformuje srozumitelný text do nesrozumitelných dat (zašifrovaný text). Dešifrování rekonstruuje z nesrozumitelných dat srozumitelný text. Oba procesy zahrnují matematický vzorec nebo algoritmus a tajnou posloupnost dat (klíč).

Existují dva typy šifrování:
- Ve sdíleném/tajném **(symetrickém)** šifrování je jeden klíč sdíleným tajemstvím mezi dvěma komunikujícími účastníky. Šifrování i dešifrování používá stejný klíč.
- U **asymetrického** šifrování s veřejným klíčem používá kódování a dekódování odlišné klíče. Účastník má dva klíče: veřejný a soukromý. Mezi oběma klíči je matematická souvislost, ale je prakticky nemožné soukromý klíč z veřejného klíče odvodit. Zprávu, která je zašifrovaná něčím veřejným klíčem, je možné dešifrovat pouze přidruženým soukromým klíčem. Alternativně může server nebo uživatel použít soukromý klíč k ″podpisu″ dokumentu a pomocí veřejného klíče digitální podpis dešifrovat. Tím se ověří zdroj dokumentu.

Digital certificate (digitální certifikát)
Digitální certifikát je digitální dokument, který ověřuje identitu vlastníka certifikátu, podobně jako cestovní pas. Důvěryhodný účastník zvaný vydavatel certifikátu (CA) vydává digitální certifikáty uživatelům a serverům. Důvěra ve vydavatele (CA) je základem důvěry v certifikát jako platné pověření. Můžete je použít k následujícím účelům:
- Identifikace - kdo je uživatel.
- Autentizace - zajištění, že uživatel je tím, za koho se prohlašuje.
- Integrita - určení, zda byl obsah dokumentu změněn ověřením digitálního ″podpisu″ odesílatele.
- Neodmítání - záruka, že uživatel nemůže tvrdit, že neprovedl nějakou akci. Uživatel nemůže například popřít, že poskytl oprávnění k elektronickému nákupu pomocí kreditní karty.

Digital signature (digitální podpis)
Digitální podpis na elektronickém dokumentu je rovnocenný s osobním podpisem na písemném dokumentu. Digitální podpis poskytuje důkaz o původu dokumentu. Vlastník certifikátu ″podepíše″ dokument tak, že použije soukromý klíč přidružený k certifikátu. Příjemce dokumentu použije odpovídající veřejný klíč, aby podpis dešifroval, čímž ověří odesilatele jakožto zdroj.

Digital Certificate Manager (DCM)
Produkt DCM (Digital Certificate Manager) umožňuje, aby se systém OS/400 stal lokálním vydavatelem certifikátu (CA).Pomocí DCM můžete vytvořit digitální

certifikáty pro servery nebo uživatele. Můžete importovat digitální certifikáty, které vydali jiní CA. Digitální certifikát můžete připojit také k profilu uživatele systému OS/400. Pomocí DCM můžete také konfigurovat aplikace tak, aby pro zabezpečení komunikace používaly SSL (Secure Sockets Layer).

Distinguished name (rozlišovací jméno)
Rozlišovací jméno je jméno osoby nebo serveru, kterým vydavatel certifikátu (CA) vydá digitální certifikát. Certifikát poskytuje toto jméno pro označení vlastnictví certifikátu. Podle strategie CA, který certifikát vydává, může rozlišovací jméno zahrnout i další informace o oprávnění.

Domain name server (server DNS)
Hostitelský systém Internetu, který převádí internetová jména na IP adresy, často v interakci s jinými servery DNS v síti Internet. Například, mnoho serverů DNS může rozpoznat stránku

```
vnet.ibm.com
```

Ale pravděpodobně jen málo z nich zná úplnou IP adresu:

```
system1.vnet.ibm.com
```

Když se připojíte k Internetu, použije váš internetový klient server DNS, aby určil IP adresu hostitelského systému, se kterým chcete komunikovat.

Encryption (šifrování)
Šifrování transformuje data do tvaru, který je nečitelný pro každého, kdo nevlastní správnou metodu dešifrování. Neoprávnění účastníci mohou přesto informace zachytit. Avšak bez správné metody dešifrování jsou informace nesrozumitelné.

Extranet (síť typu extranet)
Soukromá podniková síť několika spolupracujících organizací, umístěná mimo společnou bezpečnostní bariéru (firewall). Služba extranet používá stávající infrastrukturu Internetu, včetně standardních serverů, klientů elektronické pošty a prohlížečů WWW. Díky tomu je extranet úspornější než vytvoření a údržba soukromé sítě. Dovoluje obchodním partnerům, dodavatelům a zákazníkům se společným zájmem používat rozšířený Internet a vytvářet jednak těsné obchodní vztahy, jednak silný komunikační svazek.

Firewall (bezpečnostní bariéra)
Logická bariéra mezi vaší interní sítí a externí sítí, jako například Internetem. Bezpečnostní bariéru tvoří jeden nebo více hardwarových a softwarových systémů. Ovládá přístup a tok informací mezi zabezpečenými nebo důvěryhodnými systémy a nezabezpečenými a nedůvěryhodnými systémy.

Hacker (počítačový pirát)
Každá osoba, která se neoprávněně pokouší proniknout do vašeho systému.

Hypertext links (hypertextové odkazy)
Způsob nabídky informací online pomocí propojení (zvaných hypertextové odkazy) mezi jednou informací (zvanou hypertextový uzel) a jinou informací.

Hypertext Markup Language (jazyk HTML)
Jazyk, který se používá při definování hypertextových dokumentů. Pomocí jazyka HTML můžete označit, jak by váš dokument měl vypadat (například zvýraznění a druh písma) a jak by měl být spojen s jinými dokumenty nebo objekty.

Hypertext transport protocol (protokol HTTP)
Standardní metoda přístupu k hypertextovým dokumentům.

Internet
Celosvětová "síť sítí", které jsou navzájem spojeny. A rovněž sada spolupracujících aplikací, které počítačům připojeným k této ″síti sítí″ umožňují vzájemně

komunikovat. Internet nabízí informace k prohlížení, přenos souborů, vzdálené přihlášení, elektronickou poštu, zprávy a další služby. Internetu se často říká jen "Net".

Internet client (klient Internetu)
Program (nebo uživatel), který používá Internet, zadává požadavky programu na serveru Internetu a přijímá od něj výsledky. Jsou k dispozici různé programy klienta, od nichž je možné vyžadovat různé typy internetových služeb. Jedním typem klientského programu je prohlížeč WWW. Jiným je protokol pro přenos souborů (FTP).

Internet host (internetový hostitelský systém)
Počítač, který je připojen k síti Internet nebo intranet. Internetový hostitelský systém může provádět více než jeden program internetového serveru. Internetový hostitelský systém může například provozovat server FTP a odpovídat na požadavky aplikací typu klient FTP. Stejný hostitelský systém by mohl provozovat server HTTP a odpovídat na požadavky od klientů používajících prohlížeče WWW. Programy serverů se v hostitelském systému typicky spouštějí na pozadí (v dávkách).

Internet key exchange (IKE, výměna internetového klíče)
Protokol IKE, je-li použit s architekturou zabezpečení IP (IPSec), podporuje automatické vyjednávání zabezpečovacích asociací, stejně jako automatické generování a aktualizaci šifrovacích klíčů. Protokol IKE se obvykle používá jako součást vytváření virtuálních privátních sítí.

Internet name (internetové jméno)
Alias pro IP adresu. IP adresa je dlouhý numerický útvar a je obtížné si ji zapamatovat, jako například 10.5.100.75. Tuto IP adresu můžete přiřadit internetovému jménu, například

```
system1.vnet.ibm.com
```

Internetové jméno se také nazývá plně kvalifikované jméno domény. Když uvidíte reklamu, která říká, "Navštivte naši domovskou stránku", pak ″adresa domovské stránky″ obsahuje internetové jméno, nikoli IP adresu, protože internetové jméno se snáze zapamatuje.

Plně kvalifikované jméno domény má několik částí. Například,

```
system1.vnet.ibm.com
```

má následující části:

com: Všechny komerční sítě. Tuto část jména domény přiřazuje externí organizace, které se říká IA (*Internet authority*). Různým druhům sítí se přiřazují různé znaky (jako například com komerčním a edu vzdělávacím institucím).

ibm: Identifikátor organizace. Tuto část jména domény také přiřazuje IA (Internet authority) a je jedinečná. Jen jedna organizace na světě může mít identifikátor

```
ibm.com
```

vnet: Seskupení systémů uvnitř

```
ibm.com
```

Tento identifikátor se přiřadí interně. Správce ibm.com může vytvořit jedno nebo více seskupení.

system1:
Jméno internetového hostitelského systému uvnitř skupiny vnet.ibm.com.

Internet server (internetový server)
Program (nebo sada programů), který přijímá požadavky od odpovídajících klientských programů přes Internet a přes Internet těmto klientům odpovídá. Internetový server si můžete představit jako počítač, ke kterému může mít internetový klient přístup nebo jej může navštívit. Různé programy serveru podporují různé služby, jako například:

- Prohlížení ("domovské stránky" a odkazů na jiné dokumenty a objekty).
- Přenos souborů. Klient může například požadovat přenos souborů ze serveru na klienta. Soubory mohou být softwarové aktualizace, výpisy nebo dokumenty.
- Elektronický obchod, jako například možnost požádat o informace nebo objednat produkty.

Internet service provider (ISP, poskytovatel služeb sítě Internet)
Organizace, která poskytuje připojení k síti Internet podobně, jako vaše místní telefonní společnost poskytuje připojení k celosvětové telefonní síti.

Intranet (vnitropodniková síť)
Vnitropodniková interní síť, která používá internetové nástroje, jako například prohlížeč WWW nebo protokol FTP.

IP address (IP adresa)
Díky IP adrese jste známi v síti TCP/IP (síť Internet je obrovská síť TCP/IP). Internetový server má obvykle přiřazenu jedinečnou IP adresu. Internetový klient by mohl používat dočasnou, ale jedinečnou IP adresu, kterou přiděluje poskytovatel služeb sítě Internet (ISP).

IP datagram
Informační jednotka, která je odeslána po síti TCP/IP. IP datagram (také nazývaný paket) obsahuje jak data, tak informace záhlaví, jako například IP adresy původu a místa určení.

IP filters (filtry IP)
Filtrování IP poskytuje základní ochranný mechanizmus pro bezpečnostní bariéru. Umožňuje vám určit, jaký provoz přes ni prochází na základě podrobných údajů o relaci IP. Tím chrání zabezpečenou síť před cizími jedinci, kteří používají nekomplikované techniky (např. snímání zabezpečených serverů), nebo i nejsložitější techniky (jako například vylákání IP adresy). O funkci filtrování byste měli uvažovat jako o základu, na kterém se konstruují ostatní nástroje. Poskytuje infrastrukturu, ve které fungují, a odepře přístup všem, snad s výjimkou nejvíce cílevědomého hackera.

IPSec (protokol IPSec)
Sada protokolů na podporu zabezpečení výměny paketů ve vrstvě IP. IPSec je sada standardů, které používá iSeries a mnoho dalších systémů k provedení virtuálních soukromých sítí.

IP spoofing (vylákání IP)
Pokus o přístup do vašeho systému předstíráním, že jde o systém (IP adresu), které normálně důvěřujete. Potenciální vetřelec nastaví systém s IP adresou, které důvěřujete. Výrobci směrovačů vypracovali a vestavěli do svých systémů ochranu k detekování a odmítnutí pokusů o vylákání.

Network address translation (NAT) (převod síťových adres)
Poskytuje transparentnější alternativu k serverům proxy a SOCKS. Zjednodušuje také konfiguraci sítě tím, že povoluje připojení sítí s nekompatibilním členěním adresování. NAT nabízí dvě hlavní funkce. Může ochránit veřejný webový server, který chcete provozovat zevnitř vaší interní sítě. NAT vám tuto ochranu poskytne tím, že vám umožní skrýt ″pravou″ adresu vašeho serveru za adresu, kterou dáváte k dispozici veřejnosti. Poskytuje také mechanizmus, aby interní uživatelé měli přístup

k Internetu a přitom skryli vlastní interní IP adresy. NAT poskytuje ochranu, když povolíte interním uživatelům přístup k internetovým službám, protože můžete skrýt jejich soukromé adresy.

Non-repudiation (neodmítání)
Neodmítání je důkazem toho, že transakce proběhla nebo že jste odeslali nebo přijali zprávu. Použití digitálních certifikátů a kryptografie s veřejným klíčem k ″podpisu″ transakcí, zpráv a dokumentů neodmítání podporuje.

Packet (paket)
Datagram, který obsahuje informace o linkovém protokolu, jako je například Token-ring typu Ethernet nebo přenos rámce.

Proxy Proxy server je aplikace TCP/IP, která opakovaně posílá požadavky a odpovědi mezi klienty v zabezpečené interní síti a servery v nedůvěryhodné síti. Proxy server přeruší spojení TCP/IP, aby skryl informace o vaší interní síti (jako například interní IP adresy). Hostitelské systémy mimo vaši síť vnímají proxy server jako zdroj komunikace.

Public key infrastructure (PKI) (infrastruktura veřejného klíče)
Systém digitálních certifikátů, CA a dalších registračních institucí, které ověřují a prokazují pravost a platnost každého účastníka v internetové transakci.

Secure Sockets Layer (SSL)
Vrstva SSL (Secure Sockets Layer) je vytvořena pomocí Netscape a je de facto odvětvovou normou pro kódování relace mezi klienty a servery. SSL používá k zašifrování relace mezi serverem a klientem (uživatelem) kódování podle metrického klíče. Klient a server vyjednávají o tomto klíči během výměny digitálních certifikátů. Pro každou relaci SSL klienta a serveru se vytvoří odlišný klíč. V důsledku toho, i kdyby neoprávnění uživatelé klíč relace zachytili a dešifrovali (což není pravděpodobné), nemohou jej použít k odposlouchávání současných, budoucích, ani minulých relací SSL.

Sniffing
Praxe monitorování nebo odposlouchávání elektronických přenosů. Informace, které se posílají po Internetu, mohou někdy projít řadou směrovačů, než se dostanou na místo určení. Výrobci směrovačů, poskytovatelé služeb sítě Internet a vývojáři operačních systémů se velmi snažili zajistit, aby v páteřní síti Internetu nemohlo ke čmuchání dojít. Výskyt úspěšného čmuchání je stále vzácnější. Většinou se vyskytne spíše v soukromých sítích LAN, které jsou napojeny na Internet, než na samotné páteřní síti. Musíte si však být vědomi možnosti čmuchání proto, že většina přenosů TCP/IP zašifrována není.

SOCKS
SOCKS je architektura klient/server, která přenáší provoz TCP/IP zabezpečenou branou. Server SOCKS provádí mnoho stejných služeb jako proxy server.

Spoofing
Vetřelci se maskují jako důvěryhodný systém a snaží se vás přesvědčit, abyste jim zaslali utajované informace.

TCP/IP (protokol TCP/IP)
Primární komunikační protokol, který se používá v síti Internet. TCP/IP je zkratka vytvořená ze začátečních písmen Transmission Control Protocol/Internet Protocol. Protokol TCP/IP můžete použít také ve vaší interní síti.

Trojan horse (trojský kůň)
Trojský kůň je počítačový program (virus), který zdánlivě provádí užitečnou a nevinnou funkci. Obsahuje však skryté funkce, které používají schválená oprávnění přiřazená uživatelům, když program spustí. Například mohou zkopírovat interní informace o oprávnění z vašeho počítače a odeslat je zpět původci trojského koně.

Virtual private network (VPN)

Rozšíření soukromé vnitropodnikové sítě podniku. Můžete ji použít ve veřejné síti, jako například v síti Internet, a vytvořit zabezpečené vlastní připojení, v podstatě soukromý ″tunel″. VPN bezpečně předávají informace přes Internet a připojují další uživatele k vašemu systému. Patří mezi ně:

- Vzdálení uživatelé.
- Pobočky úřadů.
- Obchodní partneři a dodavatelé.

Web browser (prohlížeč WWW)

Aplikace protokolu HTTP typu klient. Prohlížeč WWW interpretuje HTML a zobrazuje uživateli hypertextové dokumenty. Uživatel má přístup k objektu připojenému prostřednictvím hypertextového odkazu tak, že klepne na oblast aktuálního dokumentu (provede výběr). Tato oblast se často nazývá **aktivní bod**. Příkladem prohlížeče WWW je Internet Connection Web Explorer a Netscape Navigator.

World Wide Web (WWW)

Síť vzájemně propojených serverů a klientů, které používají standardní formát při tvorbě dokumentů (HTML) a přístupu k nim (HTTP). Síti odkazů jak ze serveru na server, tak z dokumentu na dokument, se metaforicky říká **Web** (pavučina).

Vytištěno v Dánsku společností IBM Danmark A/S.