Microsoft Business Solutions

Navision Security Hardening Guide

Vydáno: říjen 2004

Microsoft

Obsah

Úvod

Systém Microsoft® Windows® poskytuje propracované síťové zabezpečení založené na standardech. V nejširším smyslu se zabezpečení podobá plánování a vyhodnocování výměny ústupků a zisků. Počítač může být například uzamčen ve sklepě a přístupný pouze jednomu správci systému. Takový počítač je možná zabezpečený, ale není příliš užitečný, protože není připojen k žádnému jinému počítači. Je potřeba zvážit, jak síť co možná nejlépe zabezpečit, aniž by byla omezena její použitelnost.

Většina organizací počítá s externími útoky a vytváří brány firewall, řada společností však neuvažuje o tom, jak omezit porušení zabezpečení, jestliže uživatel se zlými úmysly bránu firewall překoná. Bezpečnostní opatření v klientském prostředí budou účinná, pokud nejsou uživatelé při řízení obchodních záležitostí zabezpečeným způsobem nuceni provádět příliš mnoho procedur a kroků. Implementace zásad zabezpečení by měla být pro uživatele co nejjednodušší, protože v opačném případě budou mít snahu hledat méně zabezpečené způsoby práce.

Vzhledem ke skutečnosti, že se velikost instalací aplikace Navision může značně lišit, je důležité pečlivě zvážit potřeby jednotlivých klientů a porovnat účinnost zabezpečení s možnými náklady. Jako důvěryhodný poradce použijte svůj nejlepší úsudek a doporučte klientům zásady, které odpovídají jejich potřebám v oblasti zabezpečení, nepředstavují však zátěž, jež by v konečném důsledku vedla k tomu, že klient přestane tyto zásady uplatňovat.

Doporučené postupy zabezpečení aplikace Navision

Následující obecná pravidla mohou přispět ke zvýšení zabezpečení prostředí Navision:

- Jestliže chcete spustit databázový server Navision jako službu nebo použít při spuštění serveru parametr příkazového řádku *installasservice*, měli byste se ujistit, zda je služba spuštěna jako účet NT Authority\Network Service. Účet NT Authority\Network Service existuje pouze v systémech Windows™ XP a Windows Server™ 2003. Pokud používáte server Windows 2000 Server, měli byste vytvořit účet s nejmenšími oprávněními ke službě, jinak bude ke službě přiřazen místní systémový účet. Tento účet by měl mít nejvýše stejná oprávnění jako normální účet Users nebo by se mělo jednat o účet domény, který není účtem správce v doméně ani v místním počítači.

  Nesmíte zapomenout udělit účtu NT Authority\Network Service nebo uživatelskému účtu, pod kterým je server spuštěn, přístup pro čtení a zápis do databázových souborů. Tímto způsobem bude uživatelům umožněno připojit se k databázi.

  Přidělení přístupu účtu NT Authority\Network Service pro čtení a zápis do databázového souboru v systému Windows XP:

  1. V Průzkumníku Windows přejděte do složky, která obsahuje databázový soubor.
  2. Vyberte databázový soubor, klepněte na něj pravým tlačítkem myši a potom klepněte na příkaz Vlastnosti.
  3. V okně ***Vlastnosti*** klepněte na kartu ***Zabezpečení*** a ve skupinovém rámečku **Název skupiny nebo jméno uživatele** klepněte na tlačítko Přidat.
  4. V okně ***Vyberte uživatele***, ***Vyberte počítače*** nebo ***Vyberte skupiny*** zadejte text *Network Service* a klepněte na tlačítko OK.
  5. Do pole **Název skupiny nebo jméno uživatele** v okně ***Vlastnosti*** je přidán účet NETWORK SERVICE.
  6. Vyberte účet NETWORK SERVICE a v seznamu **Oprávnění** mu přidělte oprávnění *Číst* a *Zapisovat*.

- Služba aplikačního serveru Navision je ve výchozím nastavení spuštěna jako účet NT Authority\Network Service, který umožňuje získat místní přístup k databázovému serveru Navision. Pokud však chcete, aby měla služba aplikačního serveru Navision přístup k databázovému serveru v síti, je nutné zajistit, aby byla spuštěna jako účet domény Windows, který je rozpoznán databázovým serverem Navision. Tento účet by neměl být účtem správce v doméně ani v žádném místním počítači.
- Pokud pro aplikaci Navision používáte možnost serveru SQL, je server Microsoft SQL Server™ spuštěn jako služba. Možnost serveru SQL pro aplikaci Navision vyžaduje, aby server SQL vyhledával v adresáři Active Directory seznamy skupin uživatelů systému Windows pro účely ověřování. Je proto nutné zajistit spuštění služby serveru SQL jako účtu NT Authority\Network Service.

  Zajištění spuštění služby jako účtu NT Authority\Network Service:

  1. V počítači se serverem SQL vyhledejte službu MSSQLSERVER, klepněte na ni pravým tlačítkem myši a klepněte na příkaz Properties (Vlastnosti).
  2. V okně ***Properties*** (Vlastnosti) klepněte na kartu ***Log On*** (Přihlášení).
  3. Na kartě ***Log On*** klepněte u možnosti Log on as (Účet pro přihlášení) na položku This Account (Tento účet), zadejte text *NT Authority\NetworkService* a klepněte na tlačítko OK.

  Další informace o zabezpečení serveru SQL získáte na následujících webech:

  http://www.microsoft.com/security/guidance/prodtech/SQLServer.mspx

  a

  http://www.microsoft.com/technet/security/prodtech/dbsql/default.mspx

- Jestliže používáte některý produkt Navision pro elektronické obchodování, například Commerce Gateway, ujistěte se, zda je správně nainstalován server požadavků Commerce Gateway včetně výchozího nastavení účtu pro požadované služby. Výchozí nastavení účtu je označeno jako *CGRSUser* a uděluje serveru Commerce Gateway přístup k minimální sadě dalších požadovaných služeb, včetně služby *MSSQLSERVER* a *BizTalk Service BizTalk Group: BizTalkServerApplication* a na rozdíl od účtu *Local System* nezahrnuje žádné globální nastavení účtu.
- Používejte vždy silná hesla. Další informace týkající se silných hesel získáte v části Silná hesla. Věnujte pozornost tomu, kde jsou hesla v počítačích uložena.
- Používejte přihlášení systému Windows. Aplikace Navision umožňuje vytvořit dva druhy přihlášení – přihlášení databáze a přihlášení systému Windows. Doporučujeme používat přihlášení systému Windows, protože je u něj použito ověřování systému Windows a umožňuje uplatňovat správné zásady pro tvorbu hesel.
- Hesla by neměla být používána opakovaně. Opakované použití hesel v systémech a doménách je často běžnou praxí. Správce zodpovědný za dvě domény například v každé z nich vytvoří účty správců domény, u kterých jsou použita stejná hesla, a dokonce nastaví stejná hesla místních správců v počítačích domény v rámci celé domény. Pokud je v tomto případě ohrožen jediný účet nebo počítač, může to vést k ohrožení celé domény.
- Po instalaci aplikace Navision a vytvoření nebo aktualizaci databází byste měli v aplikaci Navision vytvořit přihlášení systému Windows a přiřadit je k roli superuživatele. Tento superuživatel bude řídit správu databáze, zabezpečení a podobně. K tomuto přihlášení je třeba vytvořit silné heslo. Heslo by mělo být uchováno v tajnosti. Mělo by zaručit stejnou ochranu, jakou poskytuje heslo správce systému na serveru SQL. Role superuživatele spravuje veškerý přístup k databázi a vyžaduje nejvyšší úroveň ochrany. Heslo superuživatele by měl znát pouze správce systému.
- Všichni ostatní uživatelé, kteří mají přístup k databázi Navision, by měli pracovat s nejmenším oprávněním. To znamená, že je třeba přiřadit jim v aplikaci Navision role, které jim umožní pouze přístup k vlastnostem a funkcím potřebným k plnění jejich úkolů ve společnosti.
- Ujistěte se, zda importovat soubory FOB, měnit návrhy objektů a vytvářet a obnovovat zálohy databáze mohou pouze uživatelé, jejichž role v rámci společnosti to vyžaduje.
- Vytvářejte pravidelně zálohy databáze Navision a nezapomínejte na jejich testování, abyste se ujistili, že je lze úspěšně obnovit.
- Ukládejte zálohy na bezpečné místo. Omezíte tím například nebezpečí poškození ohněm, kouřem, prachem, vysokou teplotou, bleskem a živelnými pohromami (například zemětřesením).
- Přestože může být aplikace Navision spuštěna v několika verzích systému Windows, doporučujeme použít nejnovější operační systémy s nejaktuálnějšími funkcemi zabezpečení. Jedná se aktuálně o systémy Windows XP s aktualizací Service Pack 2 a Windows Server 2003.
- Používejte službu Windows Update, která je dodávána se systémem Windows 2000, Windows XP a Windows Server 2003, a instalujte nejnovější aktualizace zabezpečení. Všechny klientské počítače udržujte v aktualizovaném stavu pomocí funkce automatické aktualizace systému Windows a instalujte nejnovější opravy zabezpečení, aktualizace Service Pack a aktualizace.
- Doporučujeme, abyste ke komunikaci mezi klienty Navision a databázovým serverem Navision používali zabezpečený protokol TCPS. Protokol TCPS je zabezpečená verze protokolu TCP/IP, která používá rozhraní SSPI (Security Support Provider Interface) se zapnutým šifrováním a ověřováním pomocí protokolu Kerberos. Protokol TCPS je výchozí protokol databázového serveru Navision.

- Zákazník by měl mít plán zotavení pro případ havárie, který zajistí rychlé obnovení služeb po havárii. Plán zotavení by měl zahrnovat například následující položky:
  - získání nového/dočasného vybavení,
  - obnovení záloh v nových systémech,
  - testování skutečného fungování plánu zotavení.

Fyzické zabezpečení

Fyzické zabezpečení je naprostou nutností, protože neexistuje žádný způsob jeho doplnění softwarovým zabezpečením. Pokud je například pevný disk ukraden, budou ukradena také data na daném disku. Při vypracování zásad projednejte s klientem následující záležitosti týkající se fyzického zabezpečení:

- U rozsáhlých instalací s vyhrazenými odděleními IT je třeba zajistit, aby byly uzamčeny místnosti se servery a místa, kde je uložen software.
- Počítače v této kategorii zahrnují:
  - server Microsoft SQL Server 2000,
  - souborový server, na kterém jsou umístěny spustitelné programy Navision.
- Neoprávněným uživatelům je třeba zabránit v přístupu k počítačům.
- Je nutné zajistit instalaci poplašných zařízení, bez ohledu na citlivost dat.
- Zálohy důležitých dat je třeba uložit mimo pracoviště a zálohy musí být skladovány v ohnivzdorných kontejnerech.

Zaměstnanci

Je vhodné omezit oprávnění ke správě u všech produktů a funkcí. Ve výchozím nastavení by klienti měli svým zaměstnancům umožnit přístup k systémovým funkcím pouze pro čtení, pokud k vykonávání práce nepožadují větší rozsah přístupu. Společnost Microsoft navrhuje postupovat podle principu nejmenšího oprávnění: dát uživatelům pouze minimální oprávnění nutná k přístupu k datům a funkcím.
Nespokojení a bývalí zaměstnanci představují hrozbu zabezpečení sítě. Při projednávání zabezpečení s klienty navrhněte následující zásady týkající se zaměstnanců:

- Prověřujte předchozí činnost zaměstnanců před jejich přijetím do zaměstnání.
- Očekávejte „odvetu“ od nespokojených zaměstnanců a bývalých zaměstnanců.
- Ujistěte se, zda jsou při odchodu zaměstnance zakázány všechny příslušné účty a hesla systému Windows. Pro účely vykazování neodstraňujte uživatele. Nepoužívejte účty opakovaně.
- Veďte uživatele k ostražitosti a vyzvěte je, aby informovali o podezřelé činnosti.
- Neudělujte oprávnění automaticky. Pokud uživatelé nepotřebují přístup k určitým počítačům, místnostem s počítači nebo sadám souborů, zajistěte, aby k nim neměli přístup.
- Naučte vedoucí, aby identifikovali možné potíže zaměstnanců a reagovali na ně.
- Ujistěte se, zda zaměstnanci rozumějí svým rolím v udržování zabezpečení sítě.
- Poskytněte kopii zásad společnosti každému zaměstnanci.
- Nepovolujte zaměstnancům instalaci softwaru, který není schválen zaměstnavatelem.

Správce

Doporučujeme, aby správci systému klientů neustále sledovali nejnovější opravy zabezpečení, které jsou k dispozici od společnosti Microsoft. Útočníci dokáží velmi účinně kombinovat malé chyby tak, aby jim umožnily rozsáhlé útoky na síť. Správci by měli nejprve zajistit, aby byl každý jednotlivý počítač co nejlépe zabezpečen, a potom přidat aktualizace zabezpečení a použít antivirový software. Celá tato příručka obsahuje řadu odkazů a zdrojů, které vám pomohou najít cenné informace a doporučené postupy.

Další položkou, která ovlivňuje možnosti zabezpečení sítě, je složitost. Se složitostí sítě stoupá obtížnost jejího zabezpečení nebo odstranění potíží, jestliže útočník úspěšně získá přístup k síti. Správce by měl pečlivě dokumentovat topografii sítě a jeho cílem by mělo být udržení její největší možné jednoduchosti.

Zabezpečení primárně zasahuje do řízení rizika. Technologie není všelék, proto zabezpečení vyžaduje spojení technologie a zásad. Jinými slovy, nikdy nebude existovat produkt, který můžete jednoduše vybalit a nainstalovat do sítě a který okamžitě dosáhne dokonalého zabezpečení. Zabezpečení je výsledkem technologie a zásad – to znamená, že úroveň zabezpečení sítě je v podstatě určena způsobem použití technologie. Společnost Microsoft dodává technologii a funkce obsahující možnosti zabezpečení, pouze správce (s vaší pomocí) však může určit správné zásady v jednotlivých organizacích. Zabezpečení je třeba zahrnout do plánování v časné fázi procesu implementace a nasazení aplikací. Je nutné porozumět tomu, co chtějí klienti chránit a co jsou pro ochranu ochotni udělat.

Nakonec je třeba vyvinout plány pro mimořádné situace, a to dříve, než k nim dojde. Kombinujte důkladné plánování se spolehlivou technologií. Zajistíte tak klientům vysoké zabezpečení.

Další informace o zabezpečení obecně získáte v článku The Ten Immutable Laws of Security Administration (Deset neměnných zákonů správy zabezpečení) na webu:
http://www.microsoft.com/technet/archive/community/columns/security/essays/10salaws.mspx

a v článcích týkajících se správy zabezpečení na webu:
http://www.microsoft.com/technet/community/columns/secmgmt/smarch.mspx

Zabezpečení serverového operačního systému

I když řada menších zákazníků nepoužívá serverový operační systém, je důležité, abyste ovládali doporučené postupy zabezpečení a uměli je sdělit větším zákazníkům se složitějšími síťovými prostředími. Měli byste také vědět, že řadu zásad a postupů popsaných v tomto dokumentu lze snadno použít u zákazníků, kteří mají pouze klientské operační systémy.

Koncepce v této části se týkají produktů Microsoft Windows 2000 Server a Microsoft Windows Server 2003, přestože informace byly převzaty zejména z nápovědy online k serveru Windows Server 2003. Systém Windows Server 2003 poskytuje robustní sadu funkcí zabezpečení. Úplné informace o všech funkcích a procedurách zabezpečení obsahuje nápověda online k serveru Windows Server 2003.

Chcete-li získat další informace o serveru Windows 2000 Server, navštivte centrum zabezpečení Windows 2000 Server Security Center na webové adrese: http://www.microsoft.com/technet/security/prodtech/win2000/default.mspx

a přečtěte si příručku Windows 2000 Security Hardening Guide (Průvodce zesílením zabezpečení systému Windows 2000) na webu: http://www.microsoft.com/technet/security/prodtech/win2000/win2khg/default.mspx

Další informace o serveru Windows Server 2003 získáte v příručce *Windows Server 2003 Security Guide* (Příručka zabezpečení serveru Windows Server 2003) na webu: http://www.microsoft.com/technet/security/prodtech/win2000/default.mspx

Základními funkcemi modelu zabezpečení serveru Windows jsou ověřování, řízení přístupu a jednotné přihlášení:

- Ověřování je proces, kterým systém ověřuje platnost identity uživatelů pomocí jejich přihlašovacích pověření. Jméno a heslo uživatele je porovnáno s autorizovaným seznamem. Pokud systém rozpozná shodu, je uživateli pomocí autorizace udělen přístup v rozsahu zadaném v seznamu oprávnění pro daného uživatele.
- Řízení přístupu omezuje přístup uživatele k informacím nebo výpočetním prostředkům na základě identity uživatelů a jejich členství v různých předdefinovaných skupinách. Řízení přístupu používají obvykle správci systému k řízení přístupu uživatelů k síťovým prostředkům, například serverům, adresářům nebo souborům. Tato funkce je obvykle implementována udělením oprávnění uživatelům a skupinám, která jim umožní přístup k určitým objektům.
- Jednotné přihlášení umožňuje, aby se uživatel přihlásil k doméně Windows jednou, pomocí jediného hesla, a byl ověřen v libovolném počítači v doméně Windows. Jednotné přihlášení umožňuje správcům implementovat ověření hesla v celé síti Windows a současně poskytuje uživatelům snadný přístup.

Následující části obsahují podrobnější popis těchto tří klíčových funkcí.

Ověřování

Ověřování je základním aspektem zabezpečení systému a slouží k potvrzení identity libovolného uživatele, který se pokouší přihlásit k doméně nebo získat přístup k síťovým prostředkům. Slabým článkem ve většině systémů ověřování je heslo uživatele.

Heslo představuje první obrannou linii proti neoprávněnému přístupu k doméně a místním počítačům. Doporučte klientům následující nejvhodnější postupy týkající se hesel:

- Používejte vždy silná hesla.
- Pokud je nutné zapsat hesla na papír, uložte papír na bezpečné místo a jakmile jej nebudete potřebovat, zničte jej.
- Nikdy hesla nikomu nesdělujte.
- Použijte u každého uživatelského účtu jiné heslo.
- Měňte hesla v pravidelných intervalech.
- Věnujte pozornost tomu, kde jsou hesla v počítačích uložena.

Silná hesla

Role hesel v zabezpečení sítě organizace je často podceňována a přehlížena. Jak již bylo uvedeno, hesla představují první obrannou linii proti neoprávněnému přístupu k síti. Měli byste proto zajistit, aby klienti od svých zaměstnanců požadovali používání silných hesel.

Nástroje pro zjišťování hesel jsou však neustále zlepšovány a počítače používané ke zjištění hesel jsou výkonnější než kdykoli dříve. Při dostatečném množství času může automatický nástroj pro zjišťování hesel zjistit libovolné heslo. Silná hesla lze však zjistit mnohem obtížněji než slabá hesla.

Pokyny týkající se vytváření silných hesel, která si uživatelé mohou zapamatovat, naleznete na webu:

http://www.microsoft.com/athome/security/privacy/password.mspx

a

http://www.microsoft.com/ntworkstation/technicalresources/PWDguidelines.asp

Definování zásad hesel

Při přípravě definování zásad pro používání hesel ve spolupráci s klientem vytvořte zásadu, která bude u všech uživatelských účtů požadovat silná hesla. U většiny systémů je dostatečné, budete-li postupovat podle doporučení uvedených v příručce Windows Server 2003 Security Guide:

- Definujte nastavení zásady **Vynutit použití historie hesel**, která umožní zapamatování několika předchozích hesel. Po nastavení této zásady nemohou uživatelé po vypršení platnosti hesla použít stejné heslo.

  Doporučené nastavení: 24.

- Definujte nastavení zásady **Maximální stáří hesla**, která zajistí potřebnou četnost vypršení platnosti hesel pro prostředí klienta.

  Doporučené nastavení: v rozsahu 42 (výchozí) až 90.

- Definujte nastavení zásady **Minimální stáří hesla**, která zajistí, že nebude možné hesla měnit, dokud jejich stáří nepřekročí určitý počet dnů. Nastavení této zásady funguje ve spojení s nastavením zásady **Vynutit použití historie hesel**. Pokud je zadáno nejnižší stáří hesla, nemohou uživatelé obejít nastavení zásady **Vynutit použití historie hesel** tím, že budou opakovaně měnit hesla a potom použijí svá původní hesla. Před změnou hesel musí uživatelé zadaný počet dnů čekat.

  Doporučené nastavení: 2.

- U nastavení zásady **Minimální délka hesla** definujte, že hesla musí obsahovat alespoň zadaný počet znaků. Dlouhá hesla (sedm či více znaků) jsou obvykle silnější než krátká. Pokud je nastavena tato zásada, nemohou uživatelé používat prázdná hesla a musí vytvářet hesla obsahující nejméně určitý počet znaků.

  Doporučené nastavení: 8.

- Povolte zásadu **Heslo musí splňovat požadavky na složitost**. Po nastavení této zásady bude u všech hesel kontrolováno, zda splňují základní požadavky na silná hesla. Tímto nastavením lze zajistit, aby hesla obsahovala nejméně tři symboly ze čtyř kategorií (velká písmena, malá písmena, číslice, jiné než alfanumerické symboly) a neobsahovala žádnou část uživatelského jména ani jméno či příjmení uživatele.

  Poznámka
  Hesla, která splňují tyto požadavky, nemusí být velmi silná. Tyto požadavky splňuje například heslo „Heslo1“.

  Doporučené nastavení: Ano.

- Úplný seznam těchto požadavků naleznete v nápovědě online k serveru Windows Server v tématu Password Must Meet Complexity Requirements (Heslo musí splňovat požadavky na složitost).

- Ukládat hesla pomocí reverzibilního šifrování: Reverzibilní šifrování je používáno v systémech, u nichž je nutné získat přístup z aplikace k textovým heslům. U většiny instalací není nutné.

  Doporučené nastavení: Ne.

Další informace naleznete v příručce Windows Server 2003 Security Guide:

http://www.microsoft.com/technet/security/prodtech/Win2003/W2003HG/SGCH00.mspx

Definování zásad uzamčení účtů

Při definování zásad uzamčení účtů postupujte opatrně. V malém podniku by zásady uzamčení účtů neměly být nikdy nastaveny, protože je velmi pravděpodobné, že budou blokováni také ověření uživatelé, což může být pro klienta velmi nákladné.

Jestliže se klient rozhodne použít zásady uzamčení účtů, nastavte zásadu **Prahová hodnota pro uzamčení účtu** na dostatečně vysokou hodnotu, aby nedošlo k zablokování přístupu ověřených uživatelů k jejich uživatelským účtům z důvodu pouhého několikanásobného chybného zadání hesla.

Další informace o zásadách uzamčení účtů naleznete v nápovědě online k serveru Windows Server v tématu Account Lockout Policy Overview (Přehled zásad uzamčení účtů).

Informace o způsobu použití nebo změnách zásad uzamčení účtů naleznete v nápovědě online k serveru Windows Server v tématu To Apply or Modify Account Lockout Policy (Použití nebo změny zásad uzamčení účtů).

Řízení přístupu

Síť Windows a její prostředky (včetně aplikace Navision) je možné zabezpečit na základě vyhodnocení práv uživatelů, skupin uživatelů a jiných počítačů v síti. Počítač nebo několik počítačů můžete zabezpečit udělením určitých uživatelských práv uživatelům nebo skupinám. Objekt, například soubor nebo složku, je možné zabezpečit přiřazením oprávnění, která uživatelům nebo skupinám umožňují provádět určité akce s daným objektem. K důležitým koncepcím, které tvoří součást řízení přístupu, patří:

- oprávnění,
- vlastnictví objektů,
- dědičnost oprávnění,
- uživatelská práva,
- auditování objektů.

Oprávnění

Oprávnění definují typ přístupu udělený uživateli nebo skupině pro objekt nebo vlastnost objektu, například soubory, složky nebo objekty registru. Oprávnění jsou použita u všech zabezpečených objektů, jako jsou soubory nebo objekty registru. Oprávnění lze udělit libovolnému uživateli, skupině nebo počítači. Je vhodné přiřadit oprávnění skupinám.

Vlastnictví objektů

Při vytváření objektu je k objektu přiřazen vlastník. U systému Windows 2000 Server je ve výchozím nastavení vlastníkem objektu jeho autor. U systému Windows Server 2003 došlo ke změně, která se týká objektů vytvořených členy skupiny Administrators.

Jestliže člen skupiny Administrators vytvoří objekt na serveru Windows Server 2003, stane se vlastníkem skupina Administrators, nikoli jednotlivý účet, který daný objekt vytvořil. Toto chování je možné změnit v modulu snap-in Místní nastavení zabezpečení konzoly MMC (Microsoft Management Console) pomocí nastavení **Systémové objekty: Výchozí vlastník objektů vytvořených členy skupiny Administrators**. Bez ohledu na oprávnění nastavená u objektu může vlastník objektu vždy změnit oprávnění týkající se objektu.

Další informace získáte v nápovědě online k serveru Windows Server v tématu Ownership (Vlastnictví).

Dědičnost oprávnění

Dědičnost umožňuje správcům snadné přiřazení a správu oprávnění. Tato funkce automaticky způsobí, že objekty v rámci kontejneru zdědí všechna dědičná oprávnění daného kontejneru. Pokud například ve složce vytvoříte soubory, zdědí tyto soubory oprávnění dané složky. Děděna mohou být pouze oprávnění označená jako dědičná.

Uživatelská práva

Uživatelská práva slouží k udělení určitých oprávnění a přihlašovacích práv uživatelům a skupinám ve výpočetním prostředí.

Informace o uživatelských právech naleznete v nápovědě online k serveru Windows Server v tématu User Rights (Uživatelská práva).

Auditování objektů

Přístup uživatelů k objektům může být auditován. V takovém případě můžete tyto události související se zabezpečením zobrazit pomocí Prohlížeče událostí v protokolu zabezpečení.

Další informace získáte v nápovědě online k serveru Windows Server v tématu Auditing (Auditování).

Doporučené postupy pro řízení přístupu

- Vhodnější je přiřadit oprávnění skupinám, nikoli uživatelům. Vzhledem ke skutečnosti, že přímá údržba uživatelských účtů není účinná, měla by být oprávnění založená na uživatelích přidělována jen výjimečně.
- V určitých zvláštních případech použijte oprávnění Odepřít. Oprávnění Odepřít můžete například použít k vyloučení podmnožiny ze skupiny, která má oprávnění Povolit.
- Nikdy nenastavujte odepření přístupu k objektu skupině Everyone. Pokud odepřete přístup skupině Everyone, budou zahrnuti také správci. Lepším řešením je odebrání skupiny Everyone, pokud udělíte oprávnění pro daný objekt jiným uživatelům, skupinám nebo počítačům. Pamatujte, že nejsou-li definována žádná oprávnění, není povolen žádný přístup.
- Přiřaďte oprávnění k objektu na nejvyšší možné úrovni stromu a potom pomocí dědičnosti rozšiřte nastavení zabezpečení v celém stromu. Nastavení řízení přístupu můžete rychle a účinně použít u všech podřízených položek nebo podstromu nadřazeného objektu. Tímto způsobem získáte nejširší účinnost s vynaložením nejmenšího úsilí. Vytvořené nastavení oprávnění by mělo vyhovovat většině uživatelů, skupin a počítačů.
- Explicitní oprávnění mohou v některých případech přepsat zděděná oprávnění. Zděděná oprávnění Odepřít nezabrání přístupu k objektu, pokud je u objektu výslovně zadáno oprávnění Povolit. Explicitní oprávnění mají přednost před zděděnými oprávněními, a to i zděděnými oprávněními Odepřít.
- U oprávnění pro objekty služby Active Directory® se ujistěte, zda ovládáte doporučené postupy specifické pro objekty služby Active Directory.

Další informace naleznete v nápovědě online k serveru Windows Server 2003 v tématu Best Practices for Assigning Permissions on Active Directory Objects (Doporučené postupy přidělování oprávnění u objektů služby Active Directory).

Brána firewall pro externí zabezpečení

Brána firewall je hardware nebo software, který brání vstupu datových paketů do určené sítě nebo výstupu paketů ze sítě. Přenosy informačních paketů jsou řízeny otevřením nebo zavřením portů brány firewall. Pomocí brány firewall jsou v jednotlivých datových paketech sledovány některé informace: protokol, pomocí kterého je paket doručen, cíl nebo odesílatel paketu, typ obsahu paketu a číslo portu, do kterého je paket odeslán. Pokud je u brány firewall konfigurováno přijímání zadaného protokolu přes cílový port, je přenos paketu povolen. Se serverem Microsoft Windows Small Business Server 2003 Premium Edition je dodáván Microsoft Internet Security and Acceleration (ISA) Server 2000 představující řešení brány firewall. Small Business Server Standard Edition zahrnuje také bránu firewall.

ISA Server 2004

Internet Security and Acceleration (ISA) Server 2000 bezpečně směruje požadavky a odpovědi mezi Internetem a klientskými počítači v interní síti.

Server ISA funguje jako zabezpečená brána do Internetu pro klienty v místní síti. Počítač se serverem ISA je transparentní pro ostatní strany na komunikační cestě. Uživatel Internetu by neměl poznat, že je v činnosti server firewall, pokud se nepokusí získat přístup ke službě nebo přejít na web, ke kterému počítač se serverem ISA odepře přístup. Internetový server, na který uživatel přistupuje, interpretuje požadavky z počítače se serverem ISA, jako by pocházely z klientské aplikace.

Jestliže zvolíte filtrování fragmentů pomocí protokolu IP (Internet Protocol), povolíte filtrování fragmentů paketu službě Webový server proxy a Brána firewall. Při filtrování fragmentů paketů jsou všechny fragmentované pakety IP zamítnuty. Jeden ze známých způsobů útoku je prováděn tak, že jsou odesílány fragmentované pakety, které jsou potom znovu sestaveny způsobem umožňujícím poškození systému.

Server ISA obsahuje mechanismus zjišťování neoprávněných vniknutí, který označí čas pokusu o útok na síť a v případě útoku provede sadu konfigurovaných akcí (nebo výstrah).

Jestliže je v počítači se serverem ISA nainstalována Internetová informační služba (IIS), je nutné ji konfigurovat tak, aby nepoužívala porty používané serverem ISA pro odchozí webové požadavky (ve výchozím nastavení 8080) a příchozí webové požadavky (ve výchozím nastavení 80). Ve službě IIS je například možné změnit konfiguraci na monitorování portu 81 a potom konfigurovat počítač se serverem ISA tak, aby směroval příchozí webové požadavky na port 81 v místním počítači se službou IIS.

Pokud dojde ke konfliktu mezi porty používanými serverem ISA a Internetovou informační službou, zastaví instalační program službu pro publikování IIS. Potom můžete v Internetové informační službě nastavit sledování jiného portu a restartovat službu pro publikování IIS.

Zásady serveru ISA

Je možné definovat zásady serveru ISA určující příchozí a odchozí přístup. Pravidla pro weby a obsah určují weby a obsah, ke kterému lze získat přístup. Pravidla pro protokoly označují, zda je určitý protokol přístupný pro příchozí a odchozí komunikaci.

Můžete vytvořit pravidla pro weby a obsah, pravidla pro protokoly, pravidla pro publikování na webu a filtry paketů IP. Tyto zásady určují způsob komunikace klientů serveru ISA s Internetem a druh povolené komunikace.

Ochrana proti virům

Počítačový virus je spustitelný soubor, který je navržen tak, aby replikoval sám sebe, vymazal nebo poškodil datové soubory a programy a neumožnil rozpoznání. Viry jsou často přepisovány a upravovány, aby je nebylo možné rozpoznat. Viry jsou často odesílány jako e-mailové přílohy. Antivirové programy je nutné průběžně aktualizovat, aby dokázaly vyhledat nové a upravené viry. Viry představují nejpoužívanější metodu počítačového vandalství.

Antivirový software je speciálně navržen k rozpoznání virových programů a ochraně před nimi. Vzhledem ke skutečnosti, že jsou neustále vytvářeny nové viry, nabízí řada výrobců antivirových produktů zákazníkům periodické aktualizace svého softwaru. Společnost Microsoft důrazně doporučuje, abyste do klientského prostředí implementovali antivirový software.

Antivirový software je třeba obvykle instalovat na každé z těchto tří míst: pracovní stanice uživatelů, servery a síť, ve které do organizace přicházejí (a v některých případech z ní odcházejí) e-maily.

Typy virů

Existují tři hlavní typy virů, které infikují počítačové systémy: viry ve spouštěcím sektoru, viry napadající soubory a trojské koně.

Viry ve spouštěcím sektoru

Po spuštění počítače je před zavedením operačního systému nebo jiných spouštěcích souborů prohledán spouštěcí sektor pevného disku. Virus napadající spouštěcí soubor je navržen tak, aby nahradil informace ve spouštěcích sektorech pevného disku vlastním kódem. Pokud je počítač infikován virem ve spouštěcím sektoru, je kód viru přednostně načten do paměti. Jakmile je virus v paměti, může sám sebe replikovat na jiné disky, které jsou v infikovaném počítači používány.

Viry napadající soubory

Nejběžnější typ viru, virus napadající soubory, se připojí k souboru spustitelného programu, a to tak, že ke spustitelnému souboru přidá vlastní kód. Virový kód je obvykle přidán způsobem, který zabrání jeho rozpoznání. Po spuštění infikovaného souboru se virus může připojit k jiným spustitelným souborům. Soubory infikované tímto typem viru mají obvykle příponu názvu souboru COM, EXE a SYS.

Některé viry napadající soubory jsou navrženy pro určité programy. Typy programů, které představují cíl, jsou často soubory s příponou OVL (Overlay) a DLL (Dynamic Link Library). I když nejsou tyto soubory spouštěny, jsou volány spustitelnými soubory. Virus je přenesen během volání.

Spuštění viru způsobí poškození dat. Virus může být spuštěn spuštěním infikovaného souboru nebo splněním podmínky konkrétního nastavení prostředí (například určitého systémového data).

Trojské koně

Trojský kůň není ve skutečnosti virus. Nejdůležitější rozdíl mezi virem a trojským koněm spočívá v tom, že trojský kůň nereplikuje sám sebe, pouze ničí informace na pevném disku. Trojský kůň je maskován jako legitimní program, například hra nebo nástroj. Pokud je však spuštěn, může zničit nebo poškodit data.

Doporučené postupy pro ochranu proti virům

Rozšíření virů v makrech je možné zabránit. Následující část obsahuje několik tipů týkajících se ochrany proti infekci, které byste měli sdělit svým klientům.

- Nainstalujte řešení ochrany proti virům, které před předáním zpráv přes směrovač hledá viry v příchozích zprávách z Internetu. Tímto způsobem bude zajištěno hledání známých virů v e-mailech.
- Je třeba znát zdroj dokumentů, které jsou přijímány. Dokumenty by neměly být otevírány, pokud nepocházejí od uživatele, kterého klient považuje za důvěryhodného.
- Promluvte s osobou, která dokument vytvořila. Pokud si uživatelé nejsou jisti, zda je dokument bezpečný, měli by kontaktovat osobu, která dokument vytvořila.
- Používejte antivirovou ochranu maker sady Microsoft Office. Aplikace sady Office upozorní uživatele v případě, že dokument obsahuje makra. Tato funkce umožňuje uživateli povolit nebo zakázat makra při otevření dokumentu.
- Používejte software pro hledání virů k rozpoznání a odebrání virů v makrech. Pomocí softwaru pro hledání virů lze rozpoznat viry v makrech a často je odebrat z dokumentů. Společnost Microsoft doporučuje používání antivirového softwaru, který je certifikován organizací ICSA (International Computer Security Association).

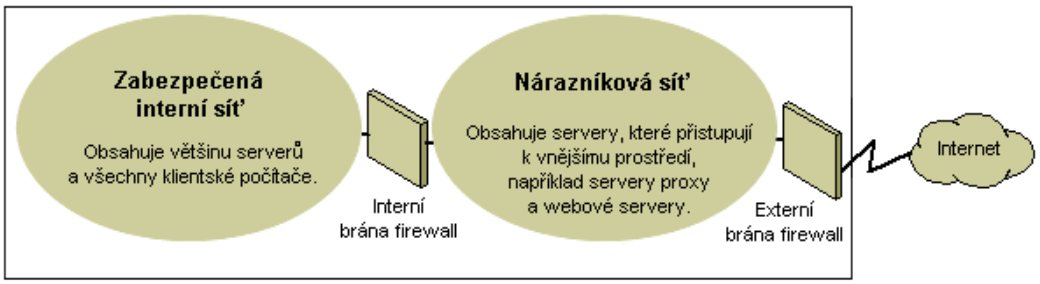
Další informace o virech a zabezpečení počítačů obecně naleznete na následujících webech společnosti Microsoft:

- Microsoft Security (Zabezpečení společnosti Microsoft) na webu http://www.microsoft.com/security/default.asp,
- dokumentace týkající se zabezpečení na webu Microsoft TechNet http://www.microsoft.com/technet/security/Default.mspx.

Strategie zabezpečení sítě

Návrh a nasazení prostředí IP pro práci v Internetu vyžaduje vyvážení zájmů privátní a veřejné sítě, a proto se brána firewall stala rozhodujícím prvkem zabezpečení integrity sítě. Brána firewall není tvořena jedinou součástí. Organizace NCSA (National Computer Security Association) definuje bránu firewall jako systém nebo kombinaci systémů vytvářejících hranici mezi nejméně dvěma sítěmi. I když jsou používány různé názvy, je tato hranice často označována jako nárazníková podsíť. Nárazníková podsíť řídí přístup z Internetu nebo jiných rozsáhlých sítí a chrání tak síť intranet nebo podnikovou místní síť (LAN) proti vniknutí.

Následující diagram zobrazuje nárazníkovou podsíť ohraničenou bránami firewall, která je umístěna mezi privátní sítí a Internetem a zabezpečuje privátní síť.



Základní nárazníková podsíť

Metody použití bran firewall k zajištění zabezpečení se v organizacích liší. Filtrování paketů IP poskytuje slabé zabezpečení, lze je snadno překonat a jeho správa je těžkopádná. Aplikační brány jsou lépe zabezpečeny než filtry paketů a jejich správa je snadnější, protože se vztahují pouze na několik určitých aplikací, například na konkrétní e-mailový systém. Brány na úrovni okruhu jsou nejúčinnější, jestliže je uživatel síťové aplikace důležitější než data předávaná příslušnou aplikací. Server proxy je komplexní nástroj zabezpečení, který zahrnuje aplikační bránu, bezpečný přístup pro anonymní uživatele a další služby. Následující část obsahuje informace o těchto různých možnostech:

- **Filtrování paketů IP**
  Filtrování paketů IP představovalo nejstarší implementovanou technologii brány firewall. V hlavičkách paketů jsou zjišťovány zdrojové a cílové adresy, čísla portů TCP (Transmission Control Protocol) a UDP (User Datagram Protocol) a další informace. Filtrování paketů je omezená technologie, která nejlépe funguje v prostředích s prostým zabezpečením, kde je například vše mimo nárazníkovou podsíť považováno za nedůvěryhodné, zatímco vše uvnitř této podsítě je důvěryhodné. V posledních letech byla metoda filtrování paketů různými dodavateli zlepšena přidáním funkcí inteligentního rozhodování k jádru pro filtrování paketů. Tím byla vytvořena nová forma filtrování paketů označovaná jako *stavové ověřování protokolu*. U filtrování paketů může být konfigurováno přijímání určitých typů paketů a zamítnutí všech ostatních, nebo zamítnutí určitých typů paketů a přijímání všech ostatních.
- **Aplikační brány**
  Aplikační brány jsou používány v případech, kdy je za nejdůležitější záležitost považován skutečný obsah aplikace. Skutečnost, že jsou specifické pro aplikace,

představuje jejich silnou stránku i jejich omezení, protože je není snadné přizpůsobit změnám technologie.

- **Brány na úrovni okruhu**
  Brány na úrovni okruhu jsou tunelová propojení vytvořená přes bránu firewall, která spojují určité procesy nebo systémy na jedné straně a určité procesy nebo systémy na straně druhé. Brány na úrovni okruhu je nejvhodnější použít v situacích, kde osoba používající aplikaci představuje možné větší riziko než informace obsažené v aplikaci. Brána na úrovni okruhu se od filtru paketů liší možností připojení ke schématu aplikací mimo pásmo, z něhož mohou být přidány další informace.
- **Servery proxy**
  Servery proxy jsou komplexní nástroje zabezpečení zahrnující funkci brány firewall a aplikační brány, která slouží ke správě internetových přenosů do místní sítě a z místní sítě. Servery proxy zajišťují také ukládání dokumentů do mezipaměti a řízení přístupu. Server proxy může přispět ke zvýšení výkonnosti tím, že ukládá často požadovaná data (například oblíbenou webovou stránku) do mezipaměti a dodává je přímo. Server proxy může také filtrovat a zahodit požadavky, které vlastník nepovažuje za vhodné, například požadavky na neoprávněný přístup ke speciálním souborům.

Ujistěte se, zda klienti využívají výhod funkcí zabezpečení brány firewall, které jim mohou pomoci. Umístěte nárazníkovou podsíť v topologii sítě do bodu, ve kterém musí všechna přenášená data z prostředí mimo podnikovou síť procházet nárazníkovou oblastí udržovanou externí bránou firewall. Funkci řízení přístupu, která je součástí brány firewall, je možné upravit pro potřeby klienta. U bran firewall můžete také nastavit hlášení všech pokusů o neoprávněný přístup.

Chcete-li minimalizovat počet portů, které je třeba otevřít u vnitřní brány firewall, můžete použít bránu firewall aplikační vrstvy, například ISA Server 2000.

Další informace týkající se protokolu TCP/IP získáte v tématu Designing a TCP/IP Network (Navrhování sítě TCP/IP) na webu http://www.microsoft.com/resources/documentation/WindowsServ/2003/all/deployguide/en-us/dnsbb_tcp_overview.asp.

Bezdrátové sítě

Ve výchozím nastavení jsou bezdrátové sítě obvykle konfigurovány způsobem, který umožňuje odposlouchávání bezdrátových signálů. Mohou být ohroženy uživatelem se zlými úmysly, který k nim může získat přístup v důsledku výchozího nastavení některého bezdrátového hardwaru, snadné přístupnosti, kterou bezdrátové sítě umožňují, nebo současných šifrovacích metod. Existují možnosti a nástroje konfigurace, které mohou chránit proti odposlouchávání, pamatujte však, že nechrání počítače proti počítačovým podvodníkům ani virům přicházejícím pomocí připojení k Internetu. Je proto mimořádně důležité chránit počítače před nežádoucími útočníky v Internetu pomocí brány firewall.

Další informace týkající se ochrany bezdrátové sítě získáte v dokumentu How to Make Your 802.11b Wireless Home Network More Secure (Jak lépe zabezpečit domácí bezdrátovou síť 802.11b) na webu http://support.microsoft.com/default.aspx?scid=kb;en-us;309369.

Scénáře zabezpečení sítě

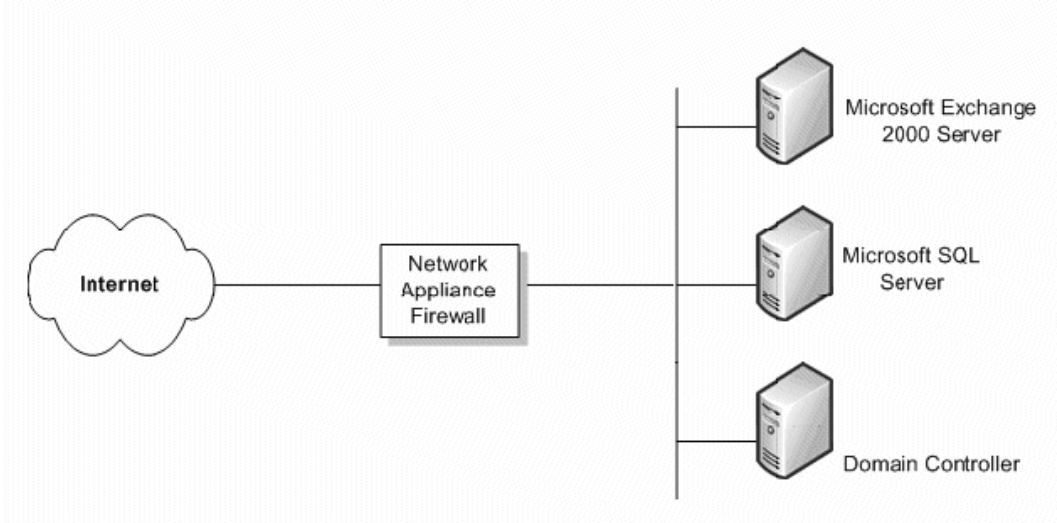
Úroveň zabezpečení sítě, kterou požaduje organizace klienta, závisí na několika faktorech. Dochází obvykle ke kompromisu mezi rozpočtem a potřebou zachování bezpečnosti podnikových dat. Je možné, aby malý podnik měl velmi složitou strukturu zabezpečení, která bude zajišťovat nejvyšší možnou úroveň zabezpečení, malý podnik si však pravděpodobně nebude moci takovou úroveň zabezpečení dovolit. V této části jsou popsány čtyři scénáře a u každého z nich jsou uvedena doporučení poskytující různou úroveň zabezpečení.

Bez brány firewall

Pokud má klient připojení k Internetu, nemá však žádnou bránu firewall, je nutné implementovat některá opatření týkající se zabezpečení sítě. Existují jednoduchá síťová zařízení brány firewall, která poskytují dostatečné zabezpečení proti přístupu potenciálních počítačových podvodníků.

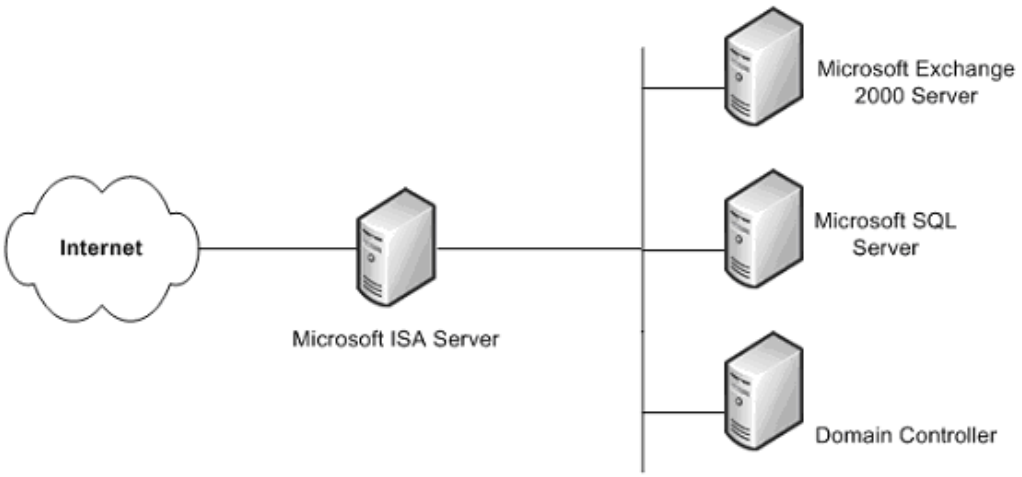
Jedna jednoduchá brána firewall

Minimální doporučenou úroveň zabezpečení představuje jedna brána firewall mezi Internetem a daty klienta. Tato brána firewall nebude pravděpodobně poskytovat žádnou úroveň rozšířeného zabezpečení a neměla by být považována za příliš bezpečnou. Je to však lepší než nic.



Jednoduchá brána firewall

Je možné, že rozpočet klienta umožní použít řešení s vyšším zabezpečením, které bude chránit podniková data. Jedním z takových řešení je server ISA. Zvýšené náklady na tento další server znamenají také výrazně vyšší zabezpečení, než je poskytováno průměrnou spotřebitelskou bránou firewall, protože ta obvykle zajišťuje pouze překládání adres (NAT) a filtrování paketů.



Server ISA jako brána firewall

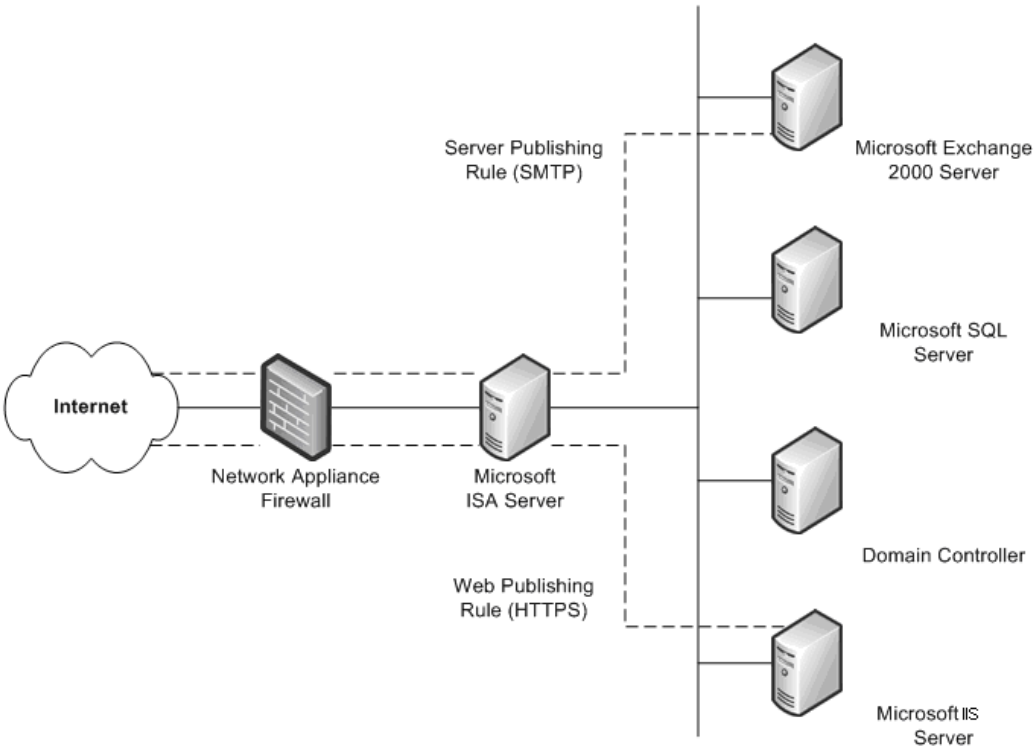
Toto řešení s jednou bránu firewall je bezpečnější než základní zařízení brány firewall a poskytuje služby zabezpečení specifické pro systém Windows.

Jedna existující brána firewall

Pokud má klient existující bránu firewall, která odděluje síť intranet od Internetu, bude vhodné posoudit možnost další brány firewall, která nabízí více způsobů konfigurace interních prostředků pro připojení k Internetu.

Jednou z metod je publikování na webu. Jedná se o případ, kdy je server ISA nasazen před webový server organizace, který poskytuje přístup k uživatelům Internetu. U příchozích webových požadavků může server ISA vzhledem k vnějšímu prostředí zastupovat webový server a plnit klientské požadavky na webový obsah ze své mezipaměti. Server ISA předá požadavky webovému serveru pouze v případě, že je nelze splnit pomocí mezipaměti serveru ISA.

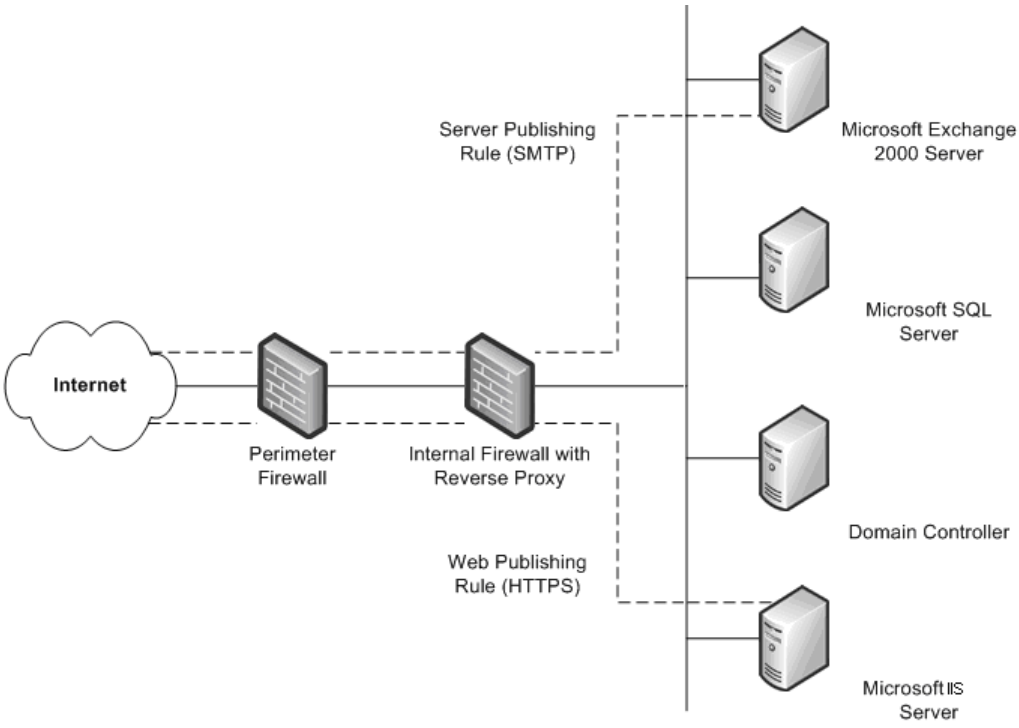
Jinou metodou je publikování serverů. Server ISA umožňuje publikovat interní servery na Internetu, aniž by bylo ohroženo zabezpečení interní sítě. Můžete konfigurovat pravidla publikování na webu a pravidla publikování serverů, která určí, jaké požadavky mají být odeslány na server v místní síti, a zajistí zvýšenou úroveň zabezpečení interních serverů.



Existující brána firewall s přidaným serverem ISA

Dvě existující brány firewall

Čtvrtý scénář představuje organizace se dvěma existujícími bránami firewall a vytvořenou nárazníkovou podsítí (DMZ). Nejméně jeden z těchto serverů zajišťuje služby obráceného serveru proxy, takže klienti v Internetu nezískávají přímý přístup na servery v síti intranet. Jedna z těchto bran firewall, ideálně interní brána firewall, zachytává síťové požadavky místo interních serverů, ověřuje pakety a předává je v zastoupení hostitelského počítače v Internetu.



Dvě existující brány firewall

Tento scénář se podobá předchozímu scénáři po přidání druhé brány firewall. Jediný rozdíl spočívá v tom, že interní bránu firewall fungující jako obrácený server proxy nepředstavuje server ISA. V tomto scénáři byste měli úzce spolupracovat se správci jednotlivých bran firewall na definování pravidel publikování serverů, která budou vyhovovat zásadám zabezpečení.

Správa oprav zabezpečení

Operační systémy a aplikace jsou často nesmírně složité. Mohou obsahovat miliony řádků kódu vytvořené řadou různých programátorů. Je velmi důležité, aby software pracoval spolehlivě a neohrozil zabezpečení nebo stabilitu prostředí IT. Z důvodu minimalizace potíží jsou programy před vydáním důkladně testovány. Předvídání všech možných budoucích útoků však není možné, protože se útočníci se neustále snaží najít slabá místa softwaru.

U řady organizací tvoří správa oprav součást jejich celkové strategie řízení změn a konfigurací. Bez ohledu na charakter a velikost organizace je však nezbytné používat dobrou strategii správy oprav, a to i v případě, že organizace dosud nemá účinnou strategii řízení změn a konfigurací. K velké většině úspěšných útoků proti počítačovým systémům dochází u systémů, ve kterých nebyly nainstalovány opravy zabezpečení.

Opravy zabezpečení jsou u většiny organizací spojeny se specifickými nároky. Po zjištění slabého místa v softwaru útočníci rychle rozšíří informace o něm v celé komunitě počítačových podvodníků. Pokud vznikne slabé místo v softwaru společnosti Microsoft, usiluje společnost Microsoft o nejdřívější možné vydání opravy zabezpečení. Do doby instalace opravy může být zabezpečení, na kterém je klient závislý a na které spoléhá, závažným způsobem oslabeno.

V prostředí Navision je nutné zajistit, aby měli klienti v celém systému nainstalovány nejnovější opravy zabezpečení. Ujistěte se, zda klient používá některou z technologií, které poskytuje společnost Microsoft. Patří k nim:

- **Služba Microsoft Security Notification**
  Služba Security Notification je e-mailový seznam určený k distribuci oznámení, která jsou odeslána, je-li k dispozici aktualizace. Tato oznámení slouží jako cenná součást proaktivní strategie zabezpečení. Jsou k dispozici také na webovém serveru TechNet Product Security Notification zaměřeném na oznámení týkající se zabezpečení produktů: http://www.microsoft.com/technet/security/bulletin/notify.mspx.
- **Automatické aktualizace společnosti Microsoft**
  Systém Windows může ve vašich počítačích automaticky použít aktualizace zabezpečení.
- **Nástroj Microsoft Security Bulletin Search**
  Nástroj pro vyhledávání bulletinů zabezpečení je k dispozici na webovém serveru služby bulletinů zabezpečení: http://www.microsoft.com/technet/security/current.aspx. Na základě aktuálně spuštěného operačního systému, aplikací a aktualizací Service Pack mohou klienti určit, které aktualizace potřebují.
- **Microsoft Baseline Security Analyzer (MBSA)**
  Tento grafický nástroj je k dispozici na webovém serveru Microsoft Baseline Security Analyzer: http://www.microsoft.com/technet/security/tools/mbsahome.mspx. Tento nástroj porovnává aktuální stav počítače se seznamem aktualizací udržovaným společností Microsoft. Nástroj MBSA provádí také některé základní kontroly zabezpečení, při nichž zjišťuje bezpečnost hesla a nastavení jeho vypršení a kontroluje zásady účtu hosta a řadu dalších oblastí. Nástroj MBSA hledá také chyby zabezpečení v Internetové informační službě společnosti Microsoft (IIS) a na serverech SQL Server™ 2000, Exchange 5.5, Exchange 2000 a Exchange Server 2003.
- **Microsoft Software Update Services (SUS)**
  Tento nástroj (dříve označován jako Windows Update Corporate Edition) umožňuje podnikům umístit na hostitelský počítač všechny důležité aktualizace a aktualizace Security Rollup Package, které jsou k dispozici na veřejném webu Windows Update. Tento nástroj společně s novým vydáním klientů automatické aktualizace tvoří základ výkonné strategie automatického stahování a instalace. Nová klientská sada automatické aktualizace zahrnuje klienta pro operační systémy Windows 2000 a Windows Server 2003 a obsahuje funkci automatické instalace stažených aktualizací. Další informace o službě Microsoft SUS najdete na webu http://www.microsoft.com/windows2000/windowsupdate/sus/default.asp.

  - **Sada funkcí služby Software Update Services pro server Microsoft Systems Management Server (SMS)**
    Sada funkcí služby Software Update Services pro server SMS obsahuje řadu nástrojů zaměřených na usnadnění procesu vydávání aktualizací softwaru v rámci podniku. K těmto nástrojům patří Security Update Inventory Tool, Microsoft Office Inventory Tool for Updates, Distribute Software Updates Wizard a nástroj SMS Web Reporting Tool s doplňkem Web Reports Add-in for Software Updates. Další informace o jednotlivých nástrojích najdete na webu http://www.microsoft.com/smserver/downloads/20/featurepacks/suspack/.

Informujte klienty o každém z těchto nástrojů a doporučte jim, aby je používali. Je velmi důležité, aby byly záležitosti spojené se zabezpečením vyřešeny co nejrychleji a současně byla zachována stabilita prostředí.

Nastavení zabezpečení serveru SQL Server 2000

Aplikaci Navision lze spustit také na serveru SQL Server 2000, a proto je důležité přijmout opatření ke zvýšení zabezpečení instalace serveru SQL Server 2000 u klienta. Ke zvýšení zabezpečení serveru SQL mohou přispět následující kroky:

- Ujistěte se, zda jsou nainstalovány nejnovější aktualizace Service Pack a aktualizace operačního systému a serveru SQL Server 2000. Nejnovější podrobnosti naleznete na webovém serveru Microsoft Security http://www.microsoft.com/security/default.asp.
- U zabezpečení na úrovni systému souborů se ujistěte, zda jsou všechny datové a systémové soubory serveru SQL Server 2000 nainstalovány v oddílech NTFS. Přístup k souborům by měl být umožněn pouze uživatelům na úrovni správce nebo systémové úrovni pomocí oprávnění NTFS. Tímto způsobem zabráníte přístupu uživatelů k těmto souborům v době, kdy není služba MSSQLSERVER spuštěna.
- U služby serveru SQL Server 2000 (MSSQLSERVER) použijte účet domény s nízkou úrovní oprávnění, například účet NT Authority\Network Service nebo LocalSystem (doporučeno). Tento účet by měl mít minimální práva v doméně a v případě ohrožení by měl přispět k zadržení (nikoli však k zastavení) útoku na server. Znamená to, že tento účet by měl v doméně mít pouze oprávnění na úrovni místního uživatele. Pokud je ke spuštění služeb na serveru SQL Server 2000 používán účet správce domény, způsobí ohrožení serveru také ohrožení celé domény. Chcete-li nastavení změnit, proveďte změnu pomocí programu SQL Server Enterprise Manager. Seznamy řízení přístupu k souborům, registr a uživatelská práva budou změněny automaticky.
- Ve většině vydání serveru SQL Server 2000 jsou nainstalovány dvě výchozí databáze, **Northwind** a **pubs**. Obě databáze jsou ukázkové a jsou používány k testování, školení a jako zdroj obecných příkladů. Neměly by být nasazeny v rámci výrobního systému. Útočník, který ví o existenci těchto databází, se může pokusit o využití chyb pomocí výchozího nastavení a výchozí konfigurace. Pokud databáze **Northwind** a **pubs** existují na výrobním počítači se serverem SQL Server 2000, měly by být odebrány.
- Auditování serveru SQL Server 2000 je ve výchozím nastavení vypnuto, nejsou proto auditovány žádné podmínky. Rozpoznání vniknutí je z toho důvodu obtížné a útočníci mohou snadno zakrýt stopy. Měli byste minimálně povolit auditování neúspěšných přihlášení.

Nejaktuálnější informace o zabezpečení serveru SQL Server 2000 naleznete na webu http://www.microsoft.com/sql/techinfo/administration/2000/security/default.asp.

Microsoft Business Solutions

Microsoft Business Solutions, divize společnosti Microsoft, nabízí široký výběr integrovaných koncových obchodních aplikací a služeb navržených tak, aby usnadnily a rozšířily spojení malých a středních podniků i velkých společností se zákazníky, zaměstnanci, partnery a dodavateli. Aplikace Microsoft Business Solutions umožňují optimalizaci strategických obchodních procesů v oblasti správy financí, analytiky, řízení lidských zdrojů, řízení projektů, řízení vztahů se zákazníky, řízení údržby, správy dodavatelského řetězce, elektronického obchodování, výroby a řízení obchodu. Aplikace jsou navrženy tak, aby podávaly zasvěcené informace a usnadnily zákazníkům dosažení obchodního úspěchu. Další informace o aplikacích Microsoft Business Solutions naleznete na webu http://www.microsoft.com/BusinessSolutions/.