Microsoft Business Solutions

Navision Security Hardening Guide

Publicerad: oktober 2004

Microsoft

Innehåll

Inledning 1

Metodtips om Navision-säkerhet 2

Fysisk säkerhet 4

Anställda 4

Administratör 5

Säkra serveroperativsystem 5
- Autentisering 6
- Starka lösenord 7
- Åtkomstkontroll 9
- Extern säkerhetsbrandvägg 10

ISA Server 2004 11
- Principer för ISA Server 11

Virusskydd 12
- Typer av virus 12
- Metodtips om virus 13

Säkerhetsstrategier för nätverk 13
- Trådlösa nätverk 15
- Scenarier för nätverkssäkerhet 15

Hantering av säkerhetskorrigeringar 18

Säkerhetsinställningar för SQL Server 2000 20

Om Microsoft Business Solutions 21

Inledning

Med Microsoft® Windows® får du avancerad standardbaserad nätverkssäkerhet. Säkerhet innebär planering och kompromisser. En dator kan till exempel låsas in i ett kassavalv som endast systemadministratören kommer åt. Den här datorn är säkrad men inte särskilt användbar eftersom den inte är ansluten till någon annan dator. Du behöver tänka igenom hur nätverket kan göras så säkert som möjligt utan att användbarheten försämras.

De flesta företag förbereder sig för externa attacker och använder brandväggar, men många företag tänker inte på hur säkerhetsproblem ska lösas när till exempel en obehörig användare väl kommit innanför brandväggen. Säkerhetsåtgärderna i kundens miljö fungerar bra om användarna inte behöver utföra allt för många procedurer och steg för att driva affärsverksamheten på ett säkert sätt. Implementeringen av säkerhetsprinciper bör vara så enkel som möjlig för användarna, annars tenderar de att hitta egna, mindre säkra lösningar.

Eftersom storleken på Navision-installationer varierar mycket är det viktigt att tänka igenom varje kunds behov och väga verkan av säkerheten mot kostnader. Som din kunds rådgivare bör du rekommendera en princip som möter kundens säkerhetskrav utan att den blir en belastning, och till slut kanske tvingar kunden att avbryta användningen av principen.

Metodtips om Navision-säkerhet

Följande allmänna regler kan hjälpa till att öka säkerheten i Navision-miljön:

- Om du vill köra Navision-databasservern som en tjänst eller använda kommandoradsparametern *installasservice* när du startar servern, bör du se till att tjänsten körs som kontot NT INSTANS\Network Service. NT INSTANS\Network Service-kontot finns endast på Windows™ XP och Windows Server™ 2003. Om du kör Windows 2000 Server bör du skapa ett konto med så få privilegier som möjligt för tjänsten, annars blir tjänsten ett lokalt systemkonto. Det här kontot bör högst ha samma privilegier som ett normalt användarkonto eller domänkonto som inte är en administratör i domänen eller på någon lokal dator.

  Kom ihåg att ge NT INSTANS\Network Service-kontot, eller användarkontot som servern körs med, läs- och skrivbehörighet i databasfiler så att användarna kan ansluta till databasen.

  Så här delar du ut läs- och skrivbehörighet i databasfiler för NT INSTANS\Network Service-kontot på Windows XP:

  1. Gå till mappen som innehåller databasfilen i Utforskaren.
  2. Markera databasfilen, högerklicka och välj Egenskaper.
  3. Klicka på fliken ***Säkerhet*** i fönstret ***Egenskaper*** och klicka på Lägg till under fältet **Grupp- eller användarnamn**.
  4. Skriv *Network Service* i fönstret ***Välj Användare, Datorer eller Grupper*** och klicka på OK.
  5. NETWORK SERVICE har lagts till i fältet **Grupp- eller användarnamn** i fönstret ***Egenskaper***.
  6. Markera NETWORK SERVICE och välj behörigheterna *Läsa* och *Skriva* i fältet **Behörigheter**.
- Navision Application Server-tjänsten körs med NT INSTANS\Network Service-kontot som standard vilket gör att den kommer åt Navision-databasservern lokalt. I ett nätverk måste du emellertid se till att Navision Application Server-tjänsten körs med Windows-domänkontot som Navision-databasservern känner igen om du vill att den ska komma åt databasservern. Det här kontot ska inte vara en administratör i domänen eller på någon lokal dator.
- Om du kör SQL Server Option för Navision körs Microsoft SQL Server™ som en tjänst. SQL Server Option för Navision kräver att SQL Server kan söka i Active Directory och hämta listor över användargrupper i Windows av autentiseringsskäl. Du måste därför se till att SQL Server-tjänsten körs som NT INSTANS\Network Service-kontot.

  Så här kör du tjänsten som NT INSTANS\Network Service:

  1. Leta upp MSSQLSERVER-tjänsten på SQL-serverdatorn, högerklicka och välj Egenskaper.
  2. Klicka på fliken ***Inloggning*** i fönstret ***Egenskaper***.
  3. Markera Det här kontot under Logga in som på fliken ***Inloggning***, skriv *NT INSTANS\NetworkService* och klicka på OK.

  Mer information om SQL Server-säkerhet finns på:

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

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

- Om du kör en Navision e-handelsprodukt, till exempel Commerce Gateway, bör du se till att Commerce Gateway Request Server är korrekt installerad med standardkontoinställningen för tjänsterna. Standardkontoinställningen kallas *CGRSUser* och beviljar Commerce Gateway Server åtkomst endast till de tjänster den behöver, inklusive *MSSQLSERVER-tjänsten* och *BizTalk Service BizTalk Group : BizTalkServerApplication,* och inkluderar inte några globala kontoinställingar som kontot *Lokalt system* gör.
- Använd alltid starka lösenord. Mer information om starka lösenord finns i avsnittet Starka lösenord.
- Använd Windows-inloggning. Navision tillåter två typer av inloggning – databasinloggning och Windows-inloggning. Windows-inloggning rekommenderas eftersom den använder Windows-autentisering och tillåter att du använder en lämplig lösenordsprincip.
- Lösenord bör inte återanvändas. Det är vanligt att lösenord återanvänds över system och domäner. En administratör, som till exempel ansvarar för två domäner, skapar kanske domänadministratörskonton med samma lösenord för båda domänerna, och anger samma lokala administratörslösenord för alla datorer i domänen. Om ett lösenord för ett enskilt konto eller en enskild dator avslöjas innebär det en stor säkerhetsrisk för hela domänen i det här fallet.
- När Navision har installerats och databaser skapats eller uppdaterats bör du skapa en Windows-inloggning och tilldela den rollen SUPER i Navision. Den här SUPER-användaren sköter databasadministration och säkerhet med mera. Ge den här inloggningen ett starkt lösenord. Det här lösenordet bör vara konfidentiellt. Det ska ha samma skydd som du ger SA-lösenordet i SQL Server. All databasåtkomst hanteras av SUPER-rollen och den kräver den högsta skyddsnivån. Systemadministratörer bör endast känna till SUPER-användarens lösenord.
- Alla andra användare som har åtkomst till Navision-databasen bör ha så få privilegier som möjligt. Detta innebär att de tilldelas roller i Navision som endast ger dem åtkomst till funktioner och funktionalitet som de behöver för att utföra sina uppgifter i företaget.
- Se till att endast de användare vars roll i företaget kräver det kan importera FOB-filer, designa om objekt samt skapa och återställa databassäkerhetskopior.
- Skapa regelbundet säkerhetskopior av Navision-databasen och kom ihåg att testa säkerhetskopiorna så att de kan återställas.
- Lagra säkerhetskopiorna på en säker plats så att du begränsar effekterna av t.ex. eldsvåda, rök, damm, hög temperatur eller blixtnedslag.
- Även om Navision kan köras på flera versioner av Windows rekommenderas du att använda de senaste operativsystemen med de senaste säkerhetsfunktionerna. För närvarande är det Windows XP med Service Pack 2 och Windows Server 2003.
- Använd Windows Update-tjänsten som ingår i Windows 2000, Windows XP och Windows Server 2003 om du vill installera de senaste säkerhetsuppdateringarna. Använd funktionen Automatiska uppdateringar i Windows om du vill hålla alla klientdatorer uppdaterade med de senaste säkerhetskorrigeringarna, uppdateringarna och Service Pack.
- Du rekommenderas att använda det säkra TCPS-protokollet för kommunikation mellan Navision-klienter och Navision-databasservern. TCPS är en säker version av TCP/IP och den använder SSPI (Security Support Provider Interface) med kryptering aktiverat och Kerberos-autentisering. TCPS är standardprotokollet för Navision-databasservern.
- Kunden bör ha en återställningsplan i händelse av en olycka som garanterar att tjänsterna snabbt kommer igång igen. En återställningsplan bör omfatta frågor som:
    - Anskaffning av ny/tillfällig utrustning.
    - Återställning av säkerhetskopior på nya system.
    - Testning av säkerhetsplanen så att den fungerar.

Fysisk säkerhet

Den fysiska säkerheten är absolut nödvändig eftersom det inte finns något sätt att ersätta den med programvarusäkerhet. Om till exempel en hårddisk blir stulen, stjäls även hårddiskens data. Diskutera följande frågor om fysisk säkerhet när du utvecklar en princip med kunden:

- Se till att serverrum och platser där programvara lagras är låsta för stora installationer med IT-avdelningar.
- Datorer i den här kategorin omfattar:
  - Microsoft SQL Server 2000
  - Filservern som innehåller Navisions körbara filer.
- Håll obehöriga användare borta från datorerna.
- Se till att inbrottslarm installeras, oavsett hur känsliga data är.
- Se till att säkerhetskopior av känsliga data lagras på en extern plats, och att säkerhetskopior lagras i brandsäkra behållare.

Anställda

Det är en bra idé att begränsa administrativa rättigheter för alla produkter och funktioner. Som standard bör de anställda endast få läsbehörighet till systemfunktioner, såvida de inte behöver ytterligare behörighet för att kunna utföra sitt arbete. Microsoft föreslår principen med så få privilegier som möjligt: ge användare endast de privilegier som krävs för åtkomst av data och funktionalitet.
Missnöjda anställda och före detta anställda är ett hot mot nätverkssäkerheten. Föreslå följande princip angående anställda när du diskuterar säkerhet med dina kunder:

- Ta reda på de anställdas bakgrund och tidigare anställningar.
- Tänk på att anställda och tidigare anställda som är missnöjda kan ställa till med besvär.
- Se till att alla anställdas associerade Windows-konton och lösenord inaktiveras när de slutar. Av rapporteringsskäl bör inte användare tas bort. Återanvänd inte konton.
- Instruera användarna att vara vaksamma och rapportera misstänkt aktivitet.
- Tilldela inte privilegier automatiskt. Se till att användare som inte behöver åtkomst till särskilda datorer, datorrum eller filuppsättningar inte har åtkomst.
- Instruera och utbilda arbetsledare så att de kan identifiera och agera mot eventuella problem med anställda.
- Se till att anställda förstår sin roll när det gäller att bevara säkerheten i nätverket.
- Dela ut ett exemplar av företagets principer till alla anställda.
- Låt inte användare installera programvara som inte godkänts av arbetsgivaren.

Administratör

Vi rekommenderar att kundens systemadministratörer kontinuerligt installerar nya säkerhetskorrigeringar från Microsoft. Inkräktare och hackare är skickliga på att utnyttja små säkerhetsluckor för att genomföra stora attacker i ett nätverk. Administratörer ska först se till att varje enskild dator är så säker som möjligt, och sedan installera säkerhetsuppdateringar och använda antivirusprogram. Många länkar och resurser tillhandahålls i den här handboken så att du enkelt kan hitta användbar information och metodtips.

Komplexitet innebär en annan kompromiss när nätverket ska säkras. Ju mer komplext nätverket är, desto svårare är det att säkra det, eller åtgärda problem när en inkräktare väl kommit in i nätverket. Administratören bör göra en fullständig dokumentation av nätverkets topografi och hålla den så enkel som möjligt.

Säkerhet innebär huvudsakligen skyddsåtgärder. Eftersom tekniken inte löser alla problem kräver säkerhet en kombination av teknik och principer. Med andra ord kommer det aldrig att finnas en produkt som du kan installera i nätverket som direkt ger fullständig säkerhet. Säkerhet är ett resultat av både teknik och principer – det är *hur* tekniken används som avgör säkerhetsnivån i nätverket. Microsoft levererar teknik och funktioner för säkerhet, men det är administratören, med din vägledning, som avgör vilka principer som ska användas i företaget. Planera för säkerhet tidigt i implementerings- och distributionsprocessen. Sätt dig in i vad kunden vill skydda och vilka åtgärder de är villiga att vidta.

Utveckla slutligen beredskapsplaner för oförutsedda händelser. Om du kombinerar en genomtänkt plan med bra teknik, får din kund en utmärkt säkerhet.

Om du vill ha mer allmän information om säkerhet kan du läsa "The Ten Immutable Laws of Security Administration" på:
http://www.microsoft.com/technet/archive/community/columns/security/essays/10salaws.mspx.

och artiklarna om säkerhetshantering på:
http://www.microsoft.com/technet/community/columns/secmgmt/smarch.mspx

Säkra serveroperativsystem

Även om du finner att många små kunder inte har ett serveroperativsystem är det viktigt att du förstår och kan ge metodtips om säkerhet till större kunder med mer komplexa nätverksmiljöer. Du bör också vara medveten om att många av principerna och tipsen i det här dokumentet enkelt kan tillämpas för de kunder som endast har klientoperativsystem.

Begreppen i det här avsnittet gäller både Microsoft Windows 2000 Server- och Microsoft Windows Server 2003-produkter även om den här informationen huvudsakligen hämtats från direkthjälpen i Windows Server 2003. Windows Server 2003 ger en kraftfull uppsättning av säkerhetsfunktioner. Direkthjälpen i Windows Server 2003 innehåller fullständig information om alla säkerhetsfunktioner och procedurer.

Om du vill ha mer information om Windows 2000 Server kan du gå till Windows 2000 Server Security Center på
http://www.microsoft.com/technet/security/prodtech/win2000/default.mspx.

och läsa Windows 2000 Security Hardening Guide på:
http://www.microsoft.com/technet/security/prodtech/win2000/win2khg/default.mspx

Om du vill ha mer information om Windows 2003 Server kan du gå till Windows 2003 Server Security Center på
http://www.microsoft.com/technet/security/prodtech/win2003/w2003hg/sgch00.mspx

Huvudfunktionerna för Windows-servrars säkerhetsmodell är autentisering, åtkomstkontroll och enkel inloggning:

- Autentisering är den process som systemet använder för att verifiera en användares identitet genom inloggningsreferensen. Användarnamnet och lösenordet jämförs med en lista över behöriga användare. Om systemet hittar användarnamnet och lösenordet beviljas användaren åtkomst enligt behörighetslistan för den aktuella användaren.
- Åtkomstkontroll begränsar användaråtkomsten av information eller resurser baserat på användarnas identitet och medlemskap i olika fördefinierade grupper. Åtkomstkontroll används av systemadministratörer för att styra vilken åtkomst användare ska ha till nätverksresurser, t.ex. servrar, kataloger och filer. Detta implementeras vanligtvis genom att tilldela användare och grupper behörighet för specifika objekt.
- Med enkel inloggning (Single Sign-on) kan en användare logga in i Windows-domänen med ett lösenord och sedan autentiseras på alla datorer i Windows-domänen. Enkel inloggning gör att administratörer kan använda lösenordsautentisering över Windows-nätverket samtidigt som användarna enkelt kan logga in.

Följande avsnitt innehåller mer detaljerade beskrivningar av dessa tre viktiga funktioner.

Autentisering

Autentisering är en grundläggande beståndsdel i systemsäkerheten och används för att verifiera identiteten för alla användare som försöker logga in på en domän eller komma åt nätverksresurser. Den svaga länken i de flesta autentiseringssystem är användarens lösenord.

Lösenord utgör den första försvarslinjen mot obehörig åtkomst av domänen och lokala datorer. Rekommendera följande för lösenord:

- Använd alltid starka lösenord.
- Om lösenord måste skrivas ner på papper, förvara papperet på en säker plats och förstör det när det inte längre behövs.
- Dela aldrig lösenord med någon.

- Använd olika lösenord för alla användarkonton.
- Byt lösenord med jämna mellanrum.
- Var försiktig med att spara lösenord på datorer.

Starka lösenord

Den roll som lösenord har när det gäller att säkra ett nätverk är ofta underskattad och förbisedd. Som nämnts tidigare utgör lösenordet den första försvarslinjen mot obehörig åtkomst i nätverket. Du bör därför se till att dina kunder instruerar sina anställda att använda starka lösenord.

Verktygen för att knäcka lösenord förbättras ständigt, och de datorer som används för att knäcka lösenorden blir alltmer kraftfulla. Om de automatiserade verktygen får tillräckligt med tid kan de knäcka vilket lösenord som helst, men starka lösenord är mycket svårare att knäcka än svaga lösenord.

Om du vill ha information om hur du skapar starka lösenord som användaren kan komma ihåg går du till

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

och

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

Definiera en lösenordsprincip

När du hjälper kunden att definiera en lösenordsprincip ser du till att skapa en princip som kräver att alla användarkonton har starka lösenord. För de flesta system är följande rekommendationer i Windows Server 2003 Security Guide tillräckliga:

- Definiera principinställningen **Nyligen använda lösenord får inte användas** så att flera tidigare lösenord sparas. Med den här principinställningen kan inte användare använda samma lösenord när deras lösenord förfaller.

  Rekommenderad inställning: 24

- Definiera principinställningen **Högsta ålder för lösenord** så att lösenorden förfaller så ofta som det behövs i kundens miljö.

  Rekommenderad inställning: mellan 42 (standard) och 90.

- Definiera principinställningen **Lägsta ålder på lösenord** så att lösenorden inte kan ändras förrän efter ett visst antal dagar. Den här principinställningen används i kombination med principinställningen **Nyligen använda lösenord får inte användas**. Om lägsta ålder på lösenord definieras kan inte användare upprepat ändra sina lösenord för att kringgå principinställningen **Nyligen använda lösenord får inte användas**, och sedan använda det ursprungliga lösenordet. Användare måste vänta angivet antal dagar innan de kan ändra sina lösenord.

  Rekommenderad inställning: 2.

- Definiera principinställningen **Minsta längd på lösenord** så att lösenorden måste bestå minst av ett visst antal tecken. Långa lösenord, sju eller fler tecken, är oftast starkare än kortare lösenord. Med den här principinställningen kan inte användare använda tomma lösenord, utan de måste skapa lösenord som innehåller minst ett visst antal tecken.

  Rekommenderad inställning: 8.

- Aktivera principinställningen **Lösenord måste uppfylla krav på komplexitet**. Den här principinställningen kontrollerar alla nya lösenord och ser till att de uppfyller grundläggande krav för starka lösenord. Den kontrollerar att lösenorden innehåller minst tre tecken från de fyra kategorierna (versaler, gemener, siffror och icke-alfanumeriska tecken), och att de inte innehåller någon del av användarnamnet eller användarens för- eller efternamn.

  Obs!
  Lösenord som uppfyller dessa krav är inte nödvändigtvis starka. Lösenordet "Exempel1" uppfyller till exempel dessa krav.

  Rekommenderad inställning: Ja

- En lista över kraven finns i avsnittet "Lösenord måste uppfylla krav på komplexitet" i direkthjälpen i Windows Server.

- Principinställningen Lagra lösenord med omvändbar kryptering används i system när program behöver åtkomst till lösenord i klartext. Den behövs inte i de flesta konfigurationer.

  Rekommenderad inställning: Nej.

Mer information finns i Windows Server 2003 Security Guide:

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

Definiera en princip för kontoutelåsning

Var försiktig när du definierar en princip för kontoutelåsning. Principen för kontoutelåsning bör aldrig användas i små företag eftersom risken är stor att behöriga användare utelåses, vilket kan vara kostsamt för kunden.

Om kunden beslutar sig för att använda en princip för kontoutelåsning, ställer du in principinställningen **Tröskelvärde för kontoutelåsning** till ett högt värde så att behöriga användare inte blir utelåsta från sina användarkonton om de råkar skriva fel lösenord flera gånger.

Mer information om principen för kontoutelåsning finns i avsnittet Översikt över princip för kontoutelåsning i direkthjälpen i Windows Server.

Mer information om hur du tillämpar eller ändrar principen för kontoutelåsning finns i avsnittet Tillämpa eller ändra princip för kontoutelåsning i direkthjälpen i Windows Server.

Åtkomstkontroll

Ett Windows-nätverk och dess resurser (inklusive Navision) kan säkras genom att se över vilka rättigheter användare, användargrupper och andra datorer har i nätverket. Du kan säkra en dator eller flera datorer genom att tilldela användare eller användargrupper särskilda användarrättigheter. Du kan säkra ett objekt, till exempel en fil eller mapp, genom att tilldela behörigheter som låter användare eller användargrupper utföra specifika åtgärder i det. Viktiga begrepp för åtkomstkontroll är:

- Behörigheter
- Ägarskap för objekt
- Arv av behörigheter
- Användarrättigheter
- Objektgranskning

Behörigheter

Behörigheter definierar typen av åtkomst som tilldelas en användare eller grupp för ett objekt eller objektegenskap, t.ex. filer, mappar och registerobjekt. Behörigheter tillämpas på alla säkra objekt, till exempel filer eller registerobjekt. Behörigheter kan tilldelas användare, grupper eller datorer. Det bästa är att tilldela dem till grupper.

Ägarskap för objekt

En ägare associeras till ett objekt när det skapas. Som standard är den som skapar objektet ägare i Windows 2000 Server. Detta har ändrats i Windows Server 2003 för objekt som skapas av medlemmar i gruppen **Administratörer**.

När en medlem i gruppen **Administratörer** skapar ett objekt i Windows Server 2003 blir gruppen **Administratörer** ägare istället för det individuella konto som användes när objektet skapades. Det här beteendet kan ändras i snapin-modulen Lokala säkerhetsinställningar i MMC (Microsoft Management Console) genom inställningen **Systemobjekt: Standardägare för objekt som skapas av medlemmar i gruppen Administratörer**. Oavsett vilka behörigheter ett objekt har så kan ägaren alltid ändra behörigheterna för objektet.

Mer information finns i avsnittet "Ägarskap" i direkthjälpen i Windows Server.

Arv av behörigheter

Med arv kan administratörer enkelt tilldela och hantera behörigheter. Den här funktionen gör att objekt i en behållare automatiskt ärver alla ärftliga behörigheter för behållaren. När du till exempel skapar filer i en mapp, ärver de mappens behörigheter. Endast de behörigheter som markerats som ärftliga ärvs.

Användarrättigheter

Med användarrättigheter beviljas specifika privilegier och inloggningsrättigheter till användare och grupper i datormiljön.

Mer information om användarrättigheter finns i avsnittet "Användarrättigheter" i direkthjälpen i Windows Server.

Objektgranskning

Du kan granska användarnas åtkomst till objekt. Därefter kan du se dessa säkerhetsrelaterade händelser i säkerhetsloggen i Loggboken.

Mer information finns i avsnitten om granskning i direkthjälpen i Windows Server.

Metodtips om åtkomstkontroll

- Tilldela behörigheter till grupper i stället för till användare. Eftersom det inte är effektivt att underhålla användarkonton direkt, bör du bara i undantagsfall tilldela behörigheter per användare.
- Behörigheter av typen Neka använder du i vissa specialfall. Du använder till exempel Neka om du vill utelämna en delmängd av en grupp som har behörigheter av typen Tillåts.
- Neka aldrig gruppen **Alla** åtkomst till ett objekt. Om du nekar alla behörighet till ett objekt gäller det även administratörer. En bättre lösning är att ta bort gruppen **Alla** om du ger andra användare, grupper eller datorer behörigheter till det objektet. Kom ihåg att om inga behörigheter har angetts, tillåts ingen åtkomst.
- Tilldela behörigheter till ett objekt så högt upp i trädet som möjligt och sprid sedan säkerhetsinställningarna i trädet genom arv. Du kan snabbt och effektivt tillämpa behörighetsinställningar på alla underordnade objekt eller ett delträd till ett överordnat objekt. På så sätt får du största möjliga effekt med minsta möjliga arbetsinsats. Behörighetsinställningarna som du anger bör vara tillräckliga för de flesta av användarna, grupperna och datorerna.
- Explicita behörigheter kan ibland åsidosätta ärvda behörigheter. Ärvda nekade behörigheter förhindrar inte åtkomst till ett objekt om objektet har den explicita behörighetsposten Tillåt. Explicita behörigheter går före ärvda behörigheter, till och med ärvda nekade behörigheter.
- Försäkra dig om att du förstår metodtipsen som särskilt gäller behörigheter för Active Directory®-objekt.

Mer information finns i "Metodtips för tilldelning av behörigheter till Active Directory-objekt" i direkthjälpen i Windows Server 2003.

Extern säkerhetsbrandvägg

En brandvägg är en maskin- eller programvarukomponent som förhindrar datapaket från att komma in i eller lämna ett specifikt nätverk. Trafikflödet styrs genom att portar i brandväggen öppnas eller stängs för informationspaket. Brandväggen kontrollerar flera informationsbitar i varje datapaket: protokollet som paketet levereras genom, paketets mål eller avsändare, typen av innehåll

i paketet och det portnummer som det skickas till. Om brandväggen är konfigurerad till att acceptera angivet protokoll genom målporten, tillåts paketet att komma igenom. Microsoft Windows Small Business Server 2003 Premium Edition levereras med Microsoft Internet Security and Acceleration (ISA) Server 2000 som brandväggslösning. I Small Business Server Standard Edition ingår också en brandvägg.

ISA Server 2004

Internet Security and Acceleration (ISA) Server 2000 dirigerar begäranden och svar på ett säkert sätt mellan Internet och klientdatorer i det interna nätverket.

ISA Server fungerar som en säker gateway mot Internet för klienter i det lokala nätverket. Andra parter i kommunikationsvägen märker inte av ISA Server-datorn (den är transparent). Internetanvändaren ska inte märka om det finns en brandvägg eller inte, såvida inte användaren försöker komma åt en tjänst eller gå till en webbplats som ISA Server-datorn nekar åtkomst till. Internetservern som ansluts tolkar begärandena från ISA Server-datorn som om de kommer från klientprogrammet.

När du väljer IP-fragmentfiltrering (Internet Protocol) aktiverar du webbproxy och brandväggstjänster för filtrering av paketfragment. Alla fragmenterade IP-paket ignoreras vid filtrering av paketfragment. En välkänd attack innebär att fragmenterade paket skickas och sedan sätts ihop på ett sådant sätt att systemet kan skadas.

ISA Server har en funktion för intrångsidentifiering som identifierar när någon försöker genomföra en attack i ett nätverk, och utför konfigurerade åtgärder (eller varningar) i händelse av en attack.

Om IIS (Internet Information Services) är installerat på ISA Server-datorn måste du konfigurera det till att inte använda portar som ISA Server använder för utgående webbegäranden (standard är 8080) och inkommande webbegäranden (standard är 80). Du kan till exempel ändra IIS till att övervaka port 81, och sedan konfigurera ISA Server-datorn till att dirigera inkommande webbegäranden till port 81 på den lokala datorn som kör IIS.

Om det finns en konflikt mellan portar som ISA Server och IIS använder, stoppar installationsprogrammet publiceringstjänsten för IIS. Du kan sedan ändra IIS till att övervaka en annan port och starta om publiceringstjänsten för IIS.

Principer för ISA Server

Du kan definiera en princip för ISA Server som styr inkommande och utgående trafik. Webbplats- och innehållsregler anger vilka webbplatser och vilket innehåll som kan nås. Protokollregler anger om ett särskilt protokoll kan användas för inkommande och utgående trafik.

Du kan skapa webbplats- och innehållsregler, protokollregler, webbpubliceringsregler och filter för IP-paket. De här principerna avgör hur ISA Server-klienter kommunicerar med Internet och vilken trafik som tillåts.

Virusskydd

Ett datorvirus är en körbar fil som utformats för att replikera sig själv eller skada datafiler och program, och undvika upptäckt. I själva verket skrivs virus ofta om och justeras så att de inte kan upptäckas. Virus skickas ofta som e-postbilagor. Antivirusprogram måste kontinuerligt uppdateras för att kunna hitta nya och modifierade virus. Virus utgör den värsta formen av skadegörelse mot datorer.

Antivirusprogram utformas särskilt för att upptäcka och stoppa virus. Många tillverkare av antivirusprodukter erbjuder kunderna periodiska uppdateringar av programvaran eftersom nya virus hela tiden utvecklas. Microsoft rekommenderar starkt att kunden använder antivirusprogram i sin miljö.

Virusprogramvara installeras vanligtvis på var och en av dessa platser: arbetsstationer, servrar och nätverket dit e-posten kommer (och i vissa fall förgreningar) i företaget.

Typer av virus

Det finns tre huvudtyper av virus som angriper datorsystem: startsektorvirus, filvirus och trojanska hästar.

Startsektorvirus

När en dator startas söker den igenom startsektorn på hårddisken innan den läser in operativsystemet eller andra startfiler. Ett startsektorvirus byter ut informationen i hårddiskens startsektorer mot sin egna kod. När en dator smittas av ett startsektorvirus läses virusets kod först in i minnet. När viruset har kommit in i minnet kan det replikera sig självt till andra diskar på den smittade datorn.

Filvirus

Filvirus är den vanligaste typen av virus, och det fäster sig självt i ett körbart program genom att lägga till sin egna kod i den körbara filen. Viruskoden läggs vanligtvis till på sådant sätt att det undgår upptäckt. När en smittad fil körs kan viruset sprida sig till andra körbara filer. Filer som smittas av den här typen av virus har vanligtvis filtillägget .com, .exe eller .sys.

Vissa filvirus är utformade för specifika program. Programtyper som ofta är måltavlor är OVL-filer (överläggsfiler; overlays) och DLL-filer (Dynamic Link Library). Även om dessa filer inte körs, anropas de av körbara filer. Viruset överförs när anropet görs.

Data skadas när viruset utlöses. Ett virus kan utlösas när en smittad fil körs eller när en specifik miljöinställning uppfylls (till exempel ett visst systemdatum).

Trojanska hästar

En trojansk häst är egentligen inte ett virus. Den viktiga skillnaden mellan ett virus och en trojansk häst är att den trojanska hästen inte replikerar sig själv utan förstör informationen på hårddisken. En trojansk häst framställs som ett legitimt program, till exempel ett spel eller ett verktyg, men när programmet körs kan det förstöra eller ändra data.

Metodtips om virus

Det går att förhindra spridning av makrovirus. Här är några tips om hur du kan undvika virusangrepp, som du kan dela med dig av till dina kunder:

- Installera en virusskyddslösning som söker efter virus i inkommande meddelanden från Internet innan de passerar routern. Detta garanterar att e-postmeddelandena genomsöks efter kända virus.
- Ta reda på källan till de dokument som tas emot. Dokument bör inte öppnas om de inte är från någon som kunden har förtroende för.
- Kontakta personen som skapade dokumentet. Om användarna är det minsta osäkra på om ett dokument är säkert eller inte bör de kontakta den som skapade dokumentet.
- Använd makrovirusskyddet i Microsoft Office. I Office varnar programmen användaren om ett dokument innehåller makron. Den här funktionen tillåter användaren att aktivera eller inaktivera makrona i dokumentet när det öppnas.
- Använd antivirusprogram för att hitta och ta bort makrovirus. Antivirusprogram kan identifiera och ofta även ta bort makrovirus från dokument. Microsoft rekommenderar att du använder antivirusprogramvara som certifierats av ICSA (International Computer Security Association).

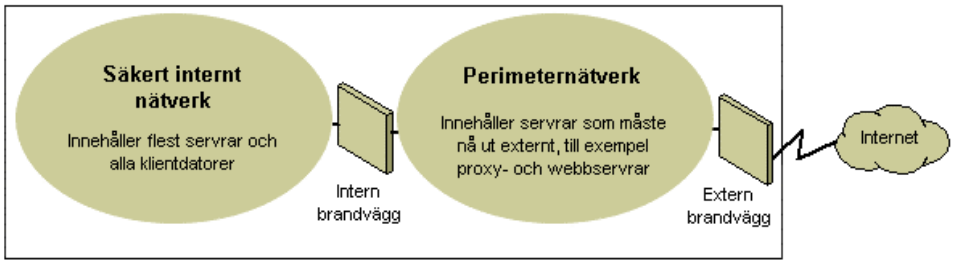
Mer information om virus och datorsäkerhet i allmänhet finns på följande Microsoft-webbplatser:

- Microsoft Security på http://www.microsoft.com/security/default.asp.
- Säkerhetsdokumentation på Microsoft TechNet http://www.microsoft.com/technet/security/Default.mspx.

Säkerhetsstrategier för nätverk

Eftersom utformningen och distributionen av en IP-internätverksmiljö kräver en balans mellan privata och offentliga nätverksaspekter, har brandväggen blivit en viktig beståndsdel i skyddet av nätverksintegriteten. En brandvägg är inte någon enskild komponent. NCSA (National Computer Security Association) definierar en brandvägg som "ett system eller en kombination av system som utgör en gräns mellan två eller flera nätverk." Olika termer används, men ofta kallas denna gräns för perimeternätverk. Perimeternätverket skyddar intranätet eller företagets lokala nätverk (LAN) från intrång genom att styra åtkomsten från Internet- eller andra stora nätverk.

Följande diagram visar ett perimeternätverk som är avgränsat med brandväggar och placerat mellan ett privat nätverk och Internet för att skydda det privata nätverket:



Grundläggande perimeternätverk

Företag och organisationer använder brandväggar på olika sätt för att få säkerhet. IP-paketfiltrering ger svag säkerhet, är besvärlig att hantera och enkel att åsidosätta. Programgateways är säkrare än paketfiltrering och är enklare att hantera eftersom de endast passar ett fåtal specifika tillämpningar, till exempel ett särskilt e-postsystem. Gateways på kretsnivå är mest effektiva när användaren av ett nätverksprogram är en viktigare aspekt än de data som passerar genom programmet. Proxyservern är ett omfattande säkerhetsverktyg som omfattar en programgateway, säker åtkomst för anonyma användare och andra tjänster. Här följer information om de olika alternativen:

- **IP-paketfiltrering**
  IP-paketfiltrering var den första implementeringen av brandväggsteknik. I pakethuvudena kontrolleras käll- och måladresser, TCP- (Transmission Control Protocol) och UDP-portnummer (User Datagram Protocol) och annan information. Paketfiltrering är en begränsad teknik som fungerar bäst i tydligt definierade säkerhetsmiljöer där till exempel allt utanför perimeternätverket inte är betrott, men allt innanför är det. På senare år har paketfiltreringsmetoden förbättrats. Nya funktioner för intelligent beslutsfattande har lagts till i kärnan för paketfiltrering, dvs en ny form av paketfiltrering har skapats som kallas *dynamisk paketfiltrering (SPI)*. Du kan konfigurera paketfiltreringen så att vissa typer av paket godkänns medan alla andra nekas, eller så att vissa typer av paket nekas medan alla andra godkänns.
- **Programgateways**
  Programgateways används när det aktuella innehållet i ett program är den viktigaste aspekten. Att de är programspecifika är både en styrka och en svaghet eftersom de inte är så lätta att anpassa till ny teknik.
- **Gateways på kretsnivå**
  Gateways på kretsnivå är tunnlar som byggts genom en brandvägg och som ansluter till specifika processer eller system på den ena sidan och specifika processer eller system på den andra sidan. Gateways på kretsnivå lämpar sig bäst i miljöer där programanvändaren utgör en potentiellt större risk än den information som överförs i programmet. Gateway på kretsnivå skiljer sig från paketfiltrering genom sin förmåga att ansluta till ett out-of-band-programschema som kan lägga till ytterligare information.
- **Proxyservrar**
  Proxyservrar är omfattande säkerhetsverktyg med brandväggs- och programgatewayfunktionalitet som hanterar Internettrafik till och från ett lokalt nätverk (LAN). Proxyservrar tillhandahåller också åtkomstkontroll och mellanlagring (cachelagring) av dokument. En proxyserver kan ge högre prestanda eftersom ofta efterfrågade data (till exempel populära webbsidor) lagras i cacheminnet och kan tas fram direkt vid behov. En proxyserver kan också filtrera och ignorera begäranden som ägaren inte godkänner, till exempel begäranden om obehörig åtkomst till skyddade filer.

Se till att kunden använder de funktioner för brandväggssäkerhet som kan hjälpa dem. Placera ett perimeternätverk i nätverkstopologin i en punkt där all trafik från utsidan av företagsnätverket måste passera igenom perimetern som hanteras av den externa brandväggen. Du kan finjustera åtkomstkontrollen för brandväggen enligt kundens behov, och konfigurera brandväggar så att de rapporterar alla försök till obehörig åtkomst.

Om du vill minimera antalet portar som du behöver öppna i den inre brandväggen kan du använda en programnivåbrandvägg, till exempel ISA Server 2000.

Mer information om TCP/IP finns i "Designing a TCP/IP Network" på http://www.microsoft.com/resources/documentation/WindowsServ/2003/all/deployguide/en-us/dnsbb_tcp_overview.asp.

Trådlösa nätverk

Trådlösa nätverk konfigureras som standard på ett sätt som tillåter avlyssning av trådlösa signaler. De kan vara sårbara eftersom standardinställningarna i viss trådlös maskinvara, tillgängligheten i det trådlösa nätverket och krypteringsmetoderna som används gör att obehöriga personer kan komma in i nätverket. Det finns konfigurationsalternativ och verktyg som kan skydda mot avlyssning, men tänk på att de inte skyddar datorerna från hackare och virus som tar sig in via Internetanslutningen. Det är därför mycket viktigt att använda en brandvägg för att skydda datorerna från inkräktare som kommer in via Internet.

Mer information om hur du kan skydda ett trådlöst nätverk finns i artikeln "How to Make Your 802.11b Wireless Home Network More Secure" på http://support.microsoft.com/default.aspx?scid=kb;en-us;309369.

Scenarier för nätverkssäkerhet

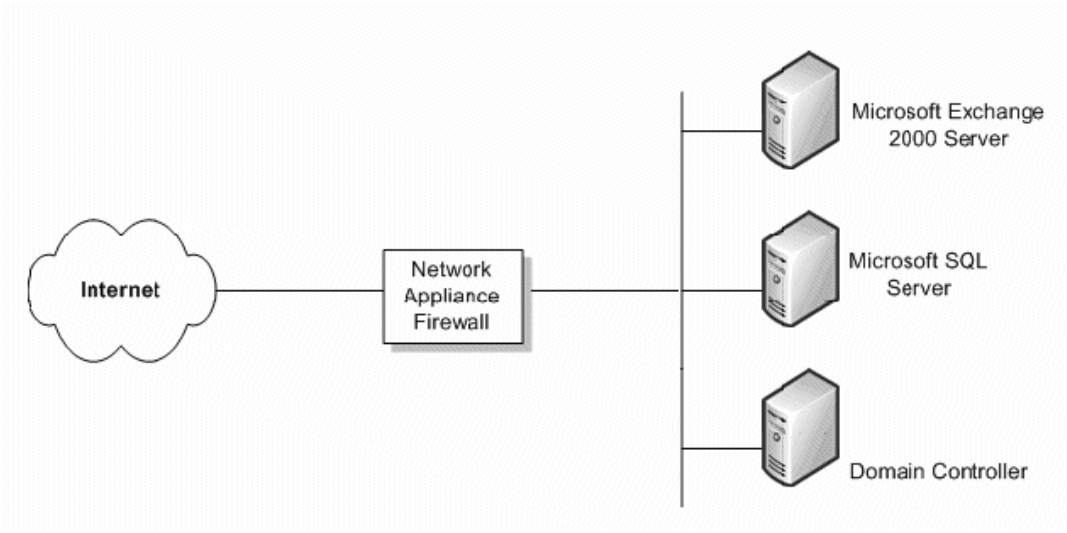
Vilken nivå av nätverkssäkerhet som kunden behöver beror på flera faktorer. Ofta blir det en kompromiss mellan budget och datasäkerhetsbehov. Det är fullt möjligt för ett litet företag att få en komplex säkerhetsstruktur som ger högsta möjliga nätverkssäkerhet, men det kanske innebär för stora kostnader att skaffa den säkerhetsnivån. I det här avsnittet studerar vi fyra scenarier och ger rekommendationer med olika säkerhetsnivåer.

Ingen brandvägg

Om kunden har en Internetanslutning men ingen brandvägg behövs vissa säkerhetsåtgärder vidtas för nätverket. Det finns enkla brandväggsprogram för nätverk som ger tillräcklig säkerhet och stoppar de flesta hackare.

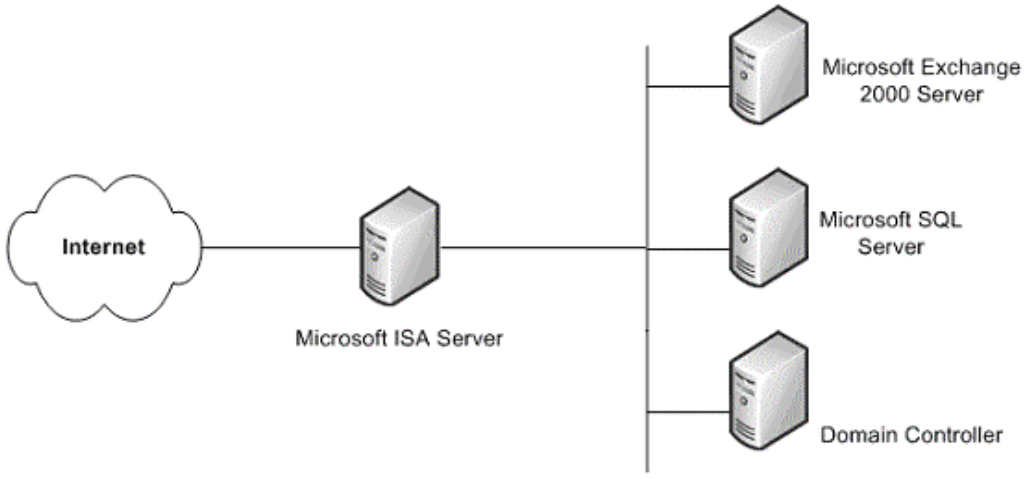
En enkel brandvägg

Den lägsta säkerhetsnivå som rekommenderas är en enkel brandvägg mellan Internet och kundens data. Den här brandväggen ger kanske inte någon avancerad eller hög säkerhetsnivå, men det är bättre än ingenting.



Enkel brandvägg

Förhoppningsvis räcker kundens budget till en säkrare lösning som skyddar deras företagsdata. En sådan lösning är ISA Server. Den högre kostnaden för den här extra servern ger betydligt högre säkerhet än genomsnittliga konsumentbrandväggar eftersom de vanligtvis endast tillhandahåller nätverksadressöversättning (NAT) och paketfiltrering.



ISA Server-brandvägg

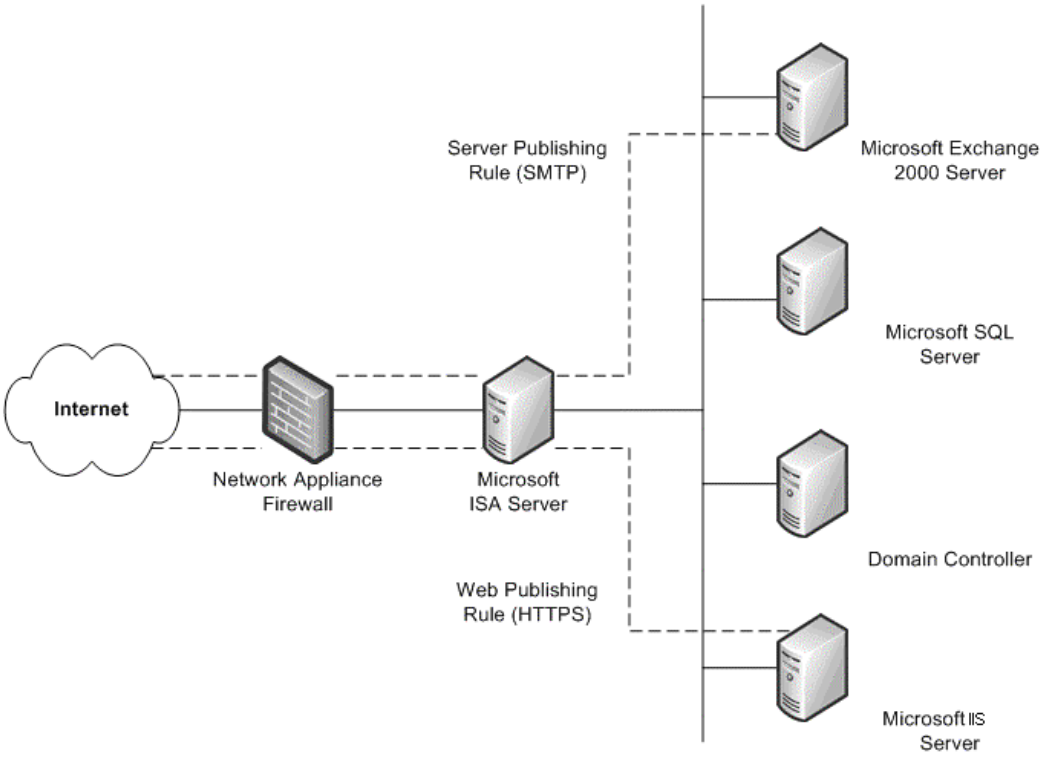
Den här enkla brandväggslösningen är säkrare än en brandsväggslösning på ingångsnivå (entry-level) och tillhandahåller Windows-specifika säkerhetstjänster.

En befintlig brandvägg

Om kunden redan har en brandvägg som avgränsar deras intranät från Internet, kan du överväga om kunden behöver ytterligare en brandvägg som ger fler möjligheter att konfigurera interna resurser till Internet.

En sådan metod är webbpublicering. Det är när en ISA Server används framför en företagswebbserver som ger åtkomst till Internetanvändare. ISA Server kan framställas som en webbserver vid inkommande begäranden, och behandla klientbegäranden om webbinnehåll från sitt cacheminne. ISA Server vidarebefordrar endast begäranden till webbservern när de inte kan behandlas från cacheminnet.

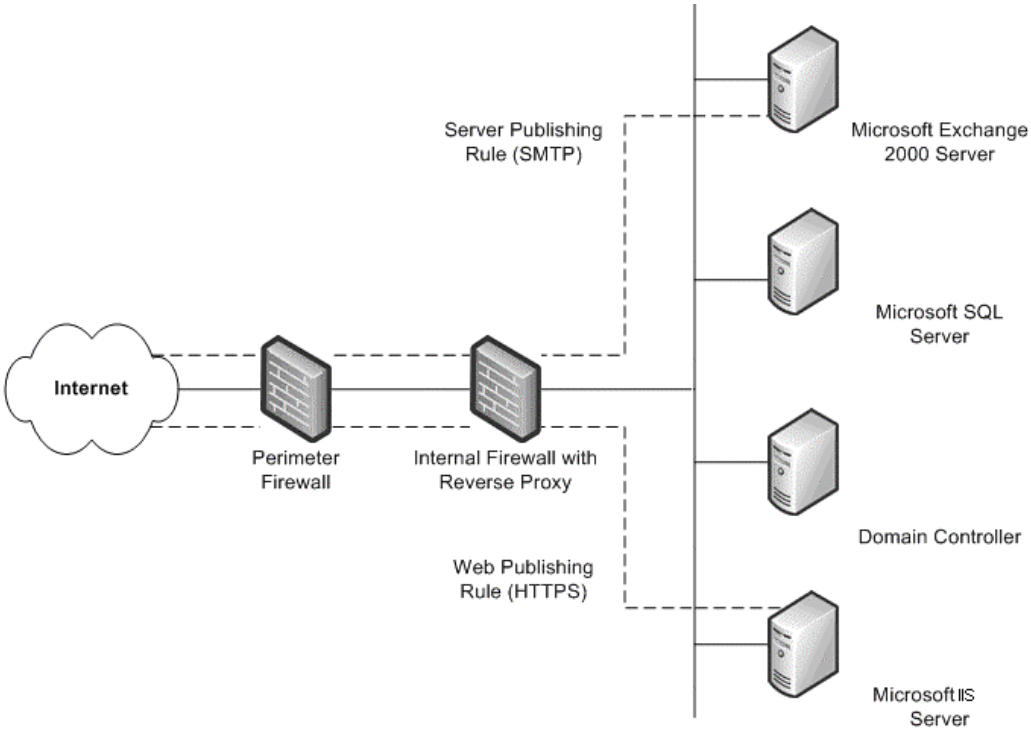
En annan metod är serverpublicering. ISA Server tillåter att interna servrar publiceras till Internet utan att säkerheten försämras i det interna nätverket. Du kan konfigurera regler för webbpublicering och serverpublicering som styr vilka begäranden som ska skickas till en server i det lokala nätverket, vilket ger bättre säkerhet för de interna servrarna.



Befintlig brandvägg tillsammans med ISA Server

Två befintliga brandväggar

Det fjärde scenariot är när företaget har två brandväggar och ett perimeternätverk (DMZ). En eller flera av dessa servrar tillhandahåller omvända proxytjänster så att Internetklienter inte ansluter direkt till servrar i intranätet. I stället fångar en av brandväggarna, lämpligen den interna brandväggen, upp nätverksbegäranden för interna servrar och undersöker dessa paket för att sedan vidarebefordra dem till Internetvärden.



Två befintliga brandväggar

Det här scenariot liknar föregående scenario efter att den andra brandväggen lagts till. Enda skillnaden är att den interna brandväggen som stöder omvänd proxy inte är en ISA Server. I det här scenariot bör du ha ett nära samarbete med dem som ansvarar för varje brandvägg, och definiera regler för serverpublicering som följer säkerhetsprincipen.

Hantering av säkerhetskorrigeringar

Operativsystem och program är ofta mycket komplexa. De kan bestå av miljontals rader med kod som skrivits av många olika programmerare. Det är viktigt att programvaran fungerar korrekt och inte försämrar säkerheten eller stabiliteten i IT-miljön. För att minimera eventuella problem utsätts program för omfattande tester innan de släpps på marknaden, men hackare fortsätter oavbrutet att leta efter svagheter i programvaran vilket gör det omöjligt att förutse alla framtida attacker.

I många företag utgör hanteringen av säkerhetskorrigeringar en del av strategin för övergripande ändringar och konfigurationshantering, men oavsett vilken typ av eller storlek företaget har, är det viktigt ha en bra strategi för hantering av säkerhetskorrigeringar även om företaget inte ännu har någon strategi för ändringar och konfigurationshantering. Det stora flertalet lyckade attacker mot datorsystem görs i system där inga säkerhetskorrigeringar har installerats.

Säkerhetskorrigeringar är en viktig utmaning för de flesta företag. När en svaghet väl har blottats i en programvara, sprids den informationen i allmänhet snabbt mellan hackare. Microsoft strävar efter att ge ut säkerhetskorrigeringar så snabbt som möjligt när svagheter i programvaran hittas. Fram tills korrigeringen släpps kan den säkerhet som kunden förlitar sig på vara allvarligt försvagad.

I Navision-miljön måste du se till att dina kunder har installerat de senaste säkerhetskorrigeringarna i sina system. Se till att kunden använder någon av de tekniker som Microsoft tillhandahåller. Dessa är:

- **Microsoft Security Notification Service**
  Security Notification Service är en tjänst som skickar meddelanden enligt en e-postlista när nya uppdateringar blir tillgängliga. Meddelandena tjänar ett viktigt syfte i strategin att ha framförhållning i säkerhetshanteringen. De finns också på TechNet-webbplatsen Product Security Notification: http://www.microsoft.com/technet/security/bulletin/notify.mspx.
- **Microsoft Automatiska uppdateringar**
  Windows kan automatiskt installera säkerhetsuppdateringar på datorerna.
- **Microsoft Security Bulletin-sökverktyg**
  Security Bulletin-sökverktyget finns tillgängligt på Security Bulletin Service-webbplatsen: http://www.microsoft.com/technet/security/current.aspx. Kunden kan bestämma vilka uppdateringar som behövs utifrån de operativsystem, program och Service Pack som körs för närvarande.
- **Microsoft Baseline Security Analyzer (MBSA)**
  Det här grafiska verktyget finns tillgängligt på Microsoft Baseline Security Analyzer-webbplatsen: http://www.microsoft.com/technet/security/tools/mbsahome.mspx. Det här verktyget jämför aktuell status för en dator med en lista över uppdateringar hos Microsoft. MBSA utför också grundläggande säkerhetskontroller av lösenordsstyrka och förfallotidsinställningar, principer för gästkonton och ett antal andra områden. MBSA letar också efter svagheter i Microsoft Internet Information Services (IIS), SQL Server™ 2000, Exchange 5.5, Exchange 2000 och Exchange Server 2003.
- **Microsoft Software Update Services (SUS)**
  Det här verktyget kallades tidigare Windows Update Corporate Edition och det gör att företag kan distribuera alla viktiga uppdateringar och SRP:er (Security Rollup Packages) som finns på den offentliga webbplatsen Windows Update. Verktyget använder en ny AU-klientuppsättning (automatisk uppdatering) och utgör grunden för en effektiv och kraftfull strategi för automatisk hämtning och installation. Med den nya AU-klientuppsättningen, som inkluderar en klient för Windows 2000- och Windows Server 2003-operativsystemen, kan uppdateringar hämtas och installeras automatiskt. Mer information om Microsoft SUS finns på http://www.microsoft.com/windows2000/windowsupdate/sus/default.asp.

- **Microsoft Systems Management Server (SMS) Software Update Services Feature Pack**
  SMS Software Update Services Feature Pack innehåller ett antal verktyg som kan användas för att förenkla processen med att distribuera programvaruuppdateringar I företaget. I verktygen ingår Security Update Inventory Tool, ett Microsoft Office-inventeringsverktyg för uppdateringar, Distribute Software Updates Wizard och SMS Web Reporting Tool med tillägget Web Reports Add-in for Software Updates. Mer information om varje verktyg finns på http://www.microsoft.com/smserver/downloads/20/featurepacks/suspack/.

Diskutera vart och ett av de här verktygen med dina kunder och uppmuntra dem att använda verktygen. Det är viktigt att säkerhetsfrågor hanteras så snabbt som möjligt för att bevara stabiliteten i miljön.

Säkerhetsinställningar för SQL Server 2000

Eftersom Navision också körs på SQL Server 2000 är det viktigt att du vidtar åtgärder för att öka säkerheten i kundens SQL Server 2000-installation. Följande steg hjälper dig att öka säkerheten för SQL Server:

- Se till att senaste Service Pack och uppdateringar för operativsystem och SQL Server 2000 är installerade. Den senaste informationen hittar du på Microsoft Security-webbplatsen http://www.microsoft.com/security/default.asp.
- För säkerhet på filsystemsnivå ser du till att alla data- och systemfiler för SQL Server 2000 är installerade på NTFS-partitioner. Du bör göra filerna tillgängliga endast för användare på administratörs- eller systemnivå med hjälp av NTFS-behörigheter. Detta skyddar mot användare som använder filerna när MSSQLSERVER-tjänsten inte körs.
- Använd ett domänkonto med få privilegier, till exempel NT INSTANS\Network Service eller LocalSystem-kontot (rekommenderas), för SQL Server 2000-tjänsten (MSSQLSERVER). Det här kontot ska ha så få rättigheter som möjligt i domänen och det bör hjälpa till att begränsa, men inte stoppa, en attack mot servern. Det här kontot ska med andra ord endast ha behörigheter på lokal användarnivå i domänen. Om SQL Server 2000 använder ett domänadministratörskonto för att köra tjänsterna innebär en attack på servern en attack på hela domänen. Använd SQL Server Enterprise Manager om du vill ändra den här inställningen. Åtkomstkontrollistor (ACL) för filer, registret och användarättigheter ändras automatiskt.
- Det flesta utgåvor av SQL Server 2000 installeras med två standarddatabaser, **Northwind** och **pubs**. Båda databaserna är exempeldatabaser som används för testning, utbildning och som allmänna exempel. De bör inte distribueras inom ett produktionssystem. Hackare kan utnyttja att de här databaserna finns och försöka komma in i systemet med hjälp av standardinställningarna och -konfigurationen. **Northwind** och **pubs** bör tas bort om de finns på produktionsdatorn med SQL Server 2000.
- Granskning av SQL Server 2000-system är inaktiverad som standard, så inga händelser granskas. Detta gör det svårt att upptäcka intrång och hjälper inkräktare genom att dölja deras spår. Som en minsta säkerhetsåtgärd bör du aktivera granskning av misslyckade inloggningar.

Den senaste säkerhetsinformationen om SQL Server 2000 finns på http://www.microsoft.com/sql/techinfo/administration/2000/security/default.asp.

Om Microsoft Business Solutions

Microsoft Business Solutions, en avdelning inom Microsoft, erbjuder ett flertal integrerade affärsprogram och tjänster (slutpunkt till slutpunkt) som utformats för att hjälpa små, medelstora och större företag att bättre kommunicera med kunder, anställda, partners och leverantörer. Microsoft Business Solutions-program optimerar strategiska affärsprocesser inom hantering av finans, analys, personal, projekt, kundrelationer, fältservice, leverantörskedja, e-handel, tillverkning och återförsäljning. Programmen är utformade för att hjälpa kunderna nå sina affärsmål. Mer information om Microsoft Business Solutions finns på http://www.microsoft.com/BusinessSolutions/