Microsoft Business Solutions

Navision Security Hardening Guide

Udgivet: Oktober 2004

Microsoft

Indholdsfortegnelse

Introduktion

Microsoft® Windows® indeholder avancerede, standardbaserede sikkerhedsfunktioner. I den bredeste betydning omfatter sikkerhed planlægning og overvejelse af kompromiser. En computer kan for eksempel være låst inde i et forseglet rum, hvor kun én systemadministrator har adgang til den. Denne computer er ganske vist sikker, men den er ikke særligt nyttig, eftersom den ikke har forbindelse til andre computere. Du er nødt til at overveje, hvordan du gør netværket så sikkert som muligt, uden at det går ud over brugbarheden.

De fleste organisationer planlægger mod udefra kommende angreb og installerer firewalls, men mange virksomheder overvejer ikke, hvordan de retter op efter en sikkerhedsbrist, når først en hacker er trængt gennem firewallen. Sikkerhedsfunktionerne i kundens systemmiljø fungerer bedst, hvis brugerne ikke er nødt til at følge for mange procedurer og fremgangsmåder for at udføre deres arbejde på sikker vis. Implementering af sikkerhedspolitikker bør være så nemt som muligt for brugerne, da de ellers vil finde mindre sikre måder at udføre deres arbejdsopgaver på.

Da størrelsen af Navision-installationer kan variere kraftigt, er det vigtigt, at du omhyggeligt overvejer hver enkelt kundes behov og opvejer effektiviteten af sikkerheden mod de omkostninger, den medfører. Som kundens betroede rådgiver skal du bruge din dømmekraft og anbefale en politik, der lever op til deres sikkerhedsbehov uden at skabe en belastning, som i sidste ende får kunden til at holde op med at gennemføre politikken.

Navision-sikkerhed - bedste fremgangsmåder

Følgende generelle regler kan hjælpe med at forbedre sikkerheden i et Navision-miljø:

- Hvis du vil køre Navision Database Server som en tjeneste eller benytte kommandolinjeparameteren *installasservice*, når du starter serveren, skal du sikre dig, at tjenesten kører under kontoen NT Authority\Netværkstjeneste. Kontoen NT Authority\Netværkstjeneste findes kun i Windows™ XP og Windows Server™ 2003. Hvis du kører Windows 2000 Server, skal du oprette en konto med minimale rettigheder til tjenesten, da tjenesten ellers vil blive tildelt en lokal systemkonto. Kontoen skal højst have de samme rettigheder som en normal brugerkonto, eller det skal være en domænekonto, som hverken er administrator i domænet eller på nogen lokal computer.

  Du skal huske at tildele den NT Authority\Netværkstjeneste-konto eller den brugerkonto, som serveren kører under, læse- og skriveadgang til databasefilerne, så brugerne kan oprette forbindelse til databasen.

  Sådan giver du kontoen NT Authority\Netværkstjeneste læse- og skriveadgang til en databasefil i Windows XP:

  1. Find den mappe, der indeholder databasefilen, i Windows Stifinder.
  2. Marker databasefilen, højreklik på den, og klik på Egenskaber.
  3. Klik på fanen ***Sikkerhed*** i vinduet ***Egenskaber***, og klik på Tilføj under feltet **Gruppe- eller brugernavne**.
  4. Skriv *Netværkstjeneste* i vinduet ***Vælg Brugere, Computere eller Grupper***, og klik på OK.
  5. NETVÆRKSTJENESTE tilføjes i feltet **Gruppe- eller brugernavne** i vinduet ***Egenskaber***.
  6. Marker NETVÆRKSTJENESTE, og giv den tilladelserne *Læsning* og *Skrivning* i feltet **Tilladelser**.
- Tjenesten Navision Application Server kører som standard under kontoen NT Authority\Netværkstjeneste, hvilket giver den lokal adgang til Navision Database Server. I et netværk skal du imidlertid sikre dig, at tjenesten Navision Application Server kører under en Windows-domænekonto, som Navision Database Server genkender, hvis den skal have adgang til databaseserveren. Kontoen må hverken være en administratorkonto i domænet eller på nogen lokal computer.
- Hvis du kører SQL Server-valget til Navision, kører Microsoft SQL Server™ som en tjeneste. SQL Server-valget til Navision kræver, at SQL Server kan søge i Active Directory for at hente lister over Windows-brugergrupper med henblik på godkendelse. Du skal derfor sikre dig, at tjenesten SQL Server kører under kontoen NT Authority\Netværkstjeneste.

  Sådan sikrer du dig, at tjenesten kører under NT Authority\Netværkstjeneste:

  1. Find tjenesten MSSQLSERVER på SQL Server-computeren, højreklik på tjenesten, og klik på Egenskaber.
  2. Klik på fanen ***Log på*** i vinduet ***Egenskaber***.
  3. Klik på Denne konto under Log på som under fanen ***Log på***, skriv *NT Authority\Netværkstjeneste*, og klik på OK.

  Yderligere oplysninger om sikkerhed i SQL Server får du ved at besøge:

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

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

- Hvis du benytter et Navision-program til e-handel, for eksempel Commerce Gateway, skal du sikre dig, at Commerce Gateway Request Server er installeret korrekt med standardkontoindstillingen til tjenesterne. Standardkontoindstillingen hedder *CGRSUser* og giver Commerce Gateway Server adgang til det mindste nødvendige sæt af andre tjenester, herunder tjenesten *MSSQLSERVER* og *BizTalk Service BizTalk Group: BizTalkServerApplication*, og omfatter ikke nogen globale kontoindstillinger, som kontoen *Lokalt system* gør.
- Brug altid stærke adgangskoder. Yderligere oplysninger om stærke adgangskoder finder du i afsnittet Stærke adgangskoder.
- Benyt Windows-logon. Du kan oprette to typer logon i Navision – Databaselogon og Windows-logon. Det anbefales at benytte Windows-logon, eftersom det benytter Windows-godkendelse og gennemtvinger en effektiv adgangskodepolitik.
- Adgangskoder bør ikke genbruges. Administratorer genbruger ofte adgangskoder til flere systemer og domæner. En administrator, der er ansvarlig for to domæner, kan for eksempel oprette domæneadministratorkonti, som benytter den samme adgangskode, til begge domæner, og endda oprette lokale administratoradgangskoder på computere i domænerne, som er de samme i hele domænet. Hvis en enkelt konto eller computer bliver kompromitteret, kan det i så fald føre til, at hele domænet kompromitteres.
- Når Navision er installeret, og databaserne er oprettet eller opdateret, skal du oprette et Windows-logon og tildele det rollen SUPER i Navision. Denne SUPER-bruger skal styre databaseadministration, sikkerhed osv. Benyt en stærk adgangskode til kontoen. Adgangskoden skal holdes hemmelig. Den skal beskyttes lige så godt som SA-adgangskoden i SQL Server. Al databaseadgang administreres af denne SUPER-rolle, og den har behov for den højeste grad af beskyttelse. SUPER-brugerens adgangskode må kun være kendt af systemadministratorerne.
- Alle andre brugere, der har adgang til Navision-databasen, skal have minimale rettigheder. Det vil sige, at de skal tildeles roller i Navision, der kun giver dem adgang til de programfunktioner, som de skal bruge for at udføre deres arbejdsopgaver i virksomheden.
- Sørg for, at kun de brugere, hvis roller i virksomheden kræver det, kan importere FOB-filer, ændre objekter samt oprette og gendanne sikkerhedskopier af databasen.
- Tag regelmæssigt sikkerhedskopier af Navision-databasen, og husk at teste sikkerhedskopierne for at sikre dig, at de kan gendannes korrekt.
- Gem dine sikkerhedskopier et sikkert sted for at begrænse effekten af sikkerhedsrisici som brand, røg, støv, høje temperaturer, lynnedslag og naturkatastrofer (f.eks. jordskælv).
- Selvom Navision kan køre under mange versioner af Windows, anbefales det, at du benytter det nyeste operativsystem med de seneste sikkerhedsfunktioner. I øjeblikket er det Windows XP med Service Pack 2 og Windows Server 2003.
- Brug den Windows Update-tjeneste, der leveres sammen med Windows 2000, Windows XP og Windows Server 2003, til at anvende de seneste sikkerhedsopdateringer. Benyt funktionen Automatiske opdateringer i Windows til at holde alle klientcomputere opdateret med de seneste sikkerhedsprogramrettelser, servicepakker og opdateringer.
- Det anbefales, at du benytter den sikre TCPS-protokol til kommunikation mellem Navision-klienterne og Navision Database Server. TCPS er en sikker version af TCP/IP, der benytter SSPI (Security Support Provider Interface) med kryptering aktiveret og Kerberos-godkendelse. TCPS er standardprotokollen i Navision Database Server.

- Kunden skal have en nødplan for genoprettelse, der sikrer hurtig gendannelse af tjenesterne efter en katastrofe. Nødplanen bør omfatte følgende punkter:
  - Anskaffelse af nyt/midlertidigt udstyr.
  - Gendannelse af sikkerhedskopier til nye systemer.
  - Test af, om genoprettelsesplanen vil fungere i praksis.

Fysisk sikkerhed

Den fysiske sikkerhed er af afgørende betydning, da det ikke er muligt at erstatte den med softwaresikkerhed. Hvis en harddisk for eksempel bliver stjålet, vil dataene på disken også blive stjålet. Du skal diskutere følgende fysiske sikkerhedsemner, når du udvikler en politik sammen med kunden.

- I store installationer med dedikerede it-afdelinger skal du sørge for, at serverrum og steder, hvor softwaren opbevares, er aflåst.
- Computerne i denne kategori omfatter:
  - Microsoft SQL Server 2000-serveren
  - Den filserver, hvor Navision-programmerne er gemt.
- Sørg for, at uautoriserede brugere ikke har adgang til computerne.
- Sørg for, at der er monteret tyverialarmer, uanset hvor fortrolige dataene er.
- Sørg for, at sikkerhedskopier af vigtige data opbevares på et andet sted, og at sikkerhedskopierne opbevares i brandsikre beholdere.

Medarbejderne

Det er en god ide at begrænse administrative rettigheder for alle programmer og funktioner. Som standard bør kunderne kun give medarbejderne læseadgang til systemfunktioner, medmindre de har brug for yderligere adgang for at kunne udføre deres arbejdsopgaver. Microsoft anbefaler følgende princip for mindste rettigheder: Giv kun brugerne de minimale rettigheder, der er nødvendige for at få adgang til data og funktionalitet.
Utilfredse eller tidligere medarbejdere er en trussel mod netværkssikkerheden. Når du diskuterer sikkerhed med kunderne, skal du foreslå følgende politik vedrørende medarbejdere:

- Undersøg medarbejderens baggrund før ansættelsen.
- Forvent "hævnakter" fra utilfredse medarbejdere og tidligere medarbejdere.
- Sørg for, at kunden deaktiverer alle tilhørende Windows-konti og adgangskoder, når en medarbejder fratræder. Af hensyn til rapportering må brugere ikke slettes. Genbrug ikke kontonavne.
- Lær brugerne at være opmærksomme og rapportere mistænkelig aktivitet.
- Tildel ikke rettigheder automatisk. Hvis brugerne ikke har behov for adgang til bestemte computere, computerrum eller filsæt, skal du sørge for, at de ikke har adgang.
- Lær arbejdslederne at identificere og reagere på mulige medarbejderproblemer.
- Sørg for, at medarbejderne forstår deres roller i opretholdelsen af netværkssikkerhed.
- Uddel en kopi af firmaets politik til hver medarbejder.
- Lad ikke brugerne installere software, som ikke er godkendt af arbejdsgiveren.

Administratoren

Det anbefales, at kundens systemadministratorer holder sig orienteret om de seneste sikkerhedsrettelser fra Microsoft. Angribere er særdeles dygtige til at udnytte en kombination af mindre programfejl til at muliggøre en større kompromittering af et netværk. Administratorer skal først sikre sig, at hver enkelt computer er så sikker som muligt, og derefter tilføje sikkerhedsopdateringer og benytte antivirussoftware. Denne guide indeholder mange hyperlinks og ressourcer, hvor du kan finde værdifulde oplysninger og forslag til fremgangsmåder.

Kompleksitet udgør endnu et kompromis i beskyttelsen af dit netværk. Jo mere komplekst netværket er, desto sværere er det at beskytte det eller at reparere det, når en hacker først har fået adgang. Administratoren skal dokumentere netværkstopografien grundigt med henblik på at gøre den så enkel som muligt.

Sikkerhed er først og fremmest et spørgsmål om risikostyring. Teknologien kan ikke løse alle problemer, og sikkerhed kræver derfor en kombination af teknologi og politik. Med andre ord vil der aldrig blive udviklet et program, som du blot kan pakke ud og installere i netværket for med det samme at opnå perfekt sikkerhed. Sikkerhed er et resultat af både teknologi og politik – dvs. det er den faktiske anvendelse af teknologien, der i sidste ende bestemmer, hvor sikkert et netværk er. Microsoft leverer sikkerhedsorienterede teknologier og funktioner, men det er kun administratoren, der, under din vejledning, kan fastlægge de rette politikker for den enkelte organisation. Sørg for at planlægge sikkerhed tidligt i implementerings- og installationsprocessen. Vær opmærksom på, hvad kunden ønsker at beskytte, og hvad de er villige til at gøre for at beskytte det.

Endelig skal du udvikle nødplaner for katastrofesituationer, før de indtræffer. Hvis du kombinerer grundig planlægning med solid teknologi, opnår din kunde en høj grad af sikkerhed.

Yderligere oplysninger om generel sikkerhed finder du under "The Ten Immutable Laws of Security Administration" (De ti love for sikkerhedsadministration) på adressen:
http://www.microsoft.com/technet/archive/community/columns/security/essays/10salaws.mspx

og i artiklerne om sikkerhedsadministration på adressen:
http://www.microsoft.com/technet/community/columns/secmgmt/smarch.mspx

Beskyttelse af serveroperativsystemet

Du vil muligvis opleve, at mange mindre kunder ikke har et serveroperativsystem, men det er også vigtigt, at du forstår og kan formidle sikkerhedsmæssige anbefalinger til større kunder med mere komplekse netværksmiljøer. Du skal også være opmærksom på, at mange af de politikker og fremgangsmåder, der beskrives i dette dokument, nemt kan anvendes hos kunder, som kun har klientoperativsystemer.

Emnerne i dette afsnit gælder både for Microsoft Windows 2000 Server- og Microsoft Windows Server 2003-programmerne, selvom oplysningerne hovedsageligt er hentet i onlinehjælpen til Windows Server 2003. Windows Server 2003 indeholder et solidt sæt af sikkerhedsfunktioner. Onlinehjælpen til Windows Server 2003 indeholder komplette oplysninger om alle sikkerhedsfunktioner og -procedurer.

Yderligere oplysninger om Windows 2000 Server finder du på Windows 2000 Server Security Center på adressen http://www.microsoft.com/technet/security/prodtech/win2000/default.mspx,

og du kan læse Windows 2000 Security Hardening Guide på adressen: http://www.microsoft.com/technet/security/prodtech/win2000/win2khg/default.mspx.

Yderligere oplysninger om Windows Server 2003 finder du i *Windows Server 2003 Security Guide* på adressen http://www.microsoft.com/technet/security/prodtech/win2003/w2003hg/sgch00.mspx.

De primære funktioner i Windows Server-sikkerhedsmodellen er godkendelse, adgangskontrol og Single Sign-on:

- Godkendelse er den proces, som systemet benytter til at kontrollere brugerens identitet ved hjælp af brugerens logonoplysninger. Brugerens navn og adgangskode sammenlignes med en godkendt liste. Hvis systemet finder en tilsvarende værdi, får brugeren adgang i det omfang, der er angivet for brugeren på listen over tilladelser.
- Adgangskontrol begrænser brugerens adgang til oplysninger eller computerressourcer baseret på brugerens identitet og medlemskab af forskellige foruddefinerede grupper. Adgangskontrol benyttes normalt af systemadministratorer til at kontrollere, hvilken adgang brugerne har til netværksressourcer som f.eks. servere, mapper og filer. Det implementeres normalt ved at give brugere og grupper tilladelse til at få adgang til bestemte objekter.
- Single Sign-on gør det muligt for en bruger at logge på et Windows-domæne én gang med en enkelt adgangskode og blive godkendt på alle computere i Windows-domænet. Med Single Sign-on kan administratorer implementere adgangskodegodkendelse i hele Windows-netværket og samtidig gøre det let for slutbrugerne at få adgang.

De følgende afsnit indeholder mere detaljerede beskrivelser af disse tre nøglefunktioner.

Godkendelse

Godkendelse er en grundlæggende del af systemsikkerhed, som bruges til at kontrollere identiteten af enhver bruger, der forsøger at logge på et domæne eller få adgang til netværksressourcer. Det svageste led i de fleste godkendelsessystemer er brugerens adgangskode.

Adgangskoder er det første forsvar mod uautoriseret adgang til domænet og de lokale computere. Anbefal følgende fremgangsmåder for adgangskoder:

- Brug altid stærke adgangskoder.
- Hvis adgangskoder skal skrives ned på et stykke papir, skal papiret gemmes på et sikkert sted, og det skal destrueres, når det ikke længere behøves.
- Del aldrig adgangskoder med andre.
- Brug forskellige adgangskoder til alle brugerkonti.
- Skift adgangskoder ud med jævne mellemrum.
- Vær forsigtig med, hvor adgangskoder gemmes på computerne.

Stærke adgangskoder

Den rolle, som adgangskoder spiller ved beskyttelsen af en organisations netværk, bliver ofte undervurderet og overset. Som nævnt ovenfor er adgangskoder det første forsvar mod uautoriseret adgang til netværket. Du skal derfor sikre dig, at kunderne kræver, at deres medarbejdere benytter stærke adgangskoder.

Værktøjerne til at knække adgangskoder bliver imidlertid bedre og bedre, og de computere, der bruges til at knække adgangskoder, er kraftigere end nogensinde. Et automatisk værktøj til knækning af adgangskoder kan knække enhver adgangskode, hvis det har tid nok. Ikke desto mindre er stærke adgangskoder meget sværere at knække end svage adgangskoder.

Oplysninger om, hvordan du opretter stærke adgangskoder, som brugeren kan huske, finder du under

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

og

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

Definition af adgangskodepolitikken

Når du hjælper kunden med at definere en adgangskodepolitik, skal du sørge for at udvikle en politik, der kræver, at brugerkontiene har stærke adgangskoder. I de fleste systemer er det tilstrækkeligt at følge anbefalingerne i Windows Server 2003 Security Guide:

- Angiv politikindstillingen **Gem gamle adgangskoder**, så der gemmes flere tidligere adgangskoder. Med denne politikindstilling kan brugerne ikke benytte den gamle adgangskode, når deres adgangskoder udløber.

  Anbefalet indstilling: 24

- Angiv politikindstillingen **Maksimumperiode for adgangskode**, så adgangskoder udløber så ofte, som kundens systemmiljø kræver det.

  Anbefalet indstilling: mellem 42 (standardværdien) og 90.

- Angiv politikindstillingen **Minimumperiode for adgangskode**, så adgangskoder ikke kan ændres, før de er mere end et bestemt antal dage gamle. Denne politikindstilling fungerer sammen med politikindstillingen **Gem gamle adgangskoder**. Hvis der angives en minimumperiode for adgangskodens alder, kan brugerne ikke skifte adgangskode gentagne gange for at omgå politikindstillingen **Gem gamle adgangskoder** og derefter benytte den oprindelige adgangskode. Brugerne skal vente det angivne antal dage, før de kan skifte adgangskode.

  Anbefalet indstilling: 2.

- Angiv en politikindstilling for **Minimumlængde for adgangskode**, så adgangskoder mindst skal indeholde et bestemt antal tegn. Lange adgangskoder på syv tegn eller derover er normalt stærkere end korte adgangskoder. Med denne politikindstilling kan brugerne ikke benytte tomme adgangskoder, og de skal oprette adgangskoder med et vist mindste antal tegn.

  Anbefalet indstilling: 8.

- Aktiver politikindstillingen **Adgangskoden skal opfylde kompleksitetskravene**. Denne politikindstilling kontrollerer, at alle nye adgangskoder overholder de grundlæggende krav til stærke adgangskoder. Indstillingen sikrer, at adgangskoder indeholder mindst tre symboler fra de fire kategorier (store bogstaver, små bogstaver, tal, ikke-alfanumeriske symboler), og at de ikke indeholder en del af brugernavnet eller brugerens for- eller efternavn.

  Bemærk!
  Adgangskoder, der overholder disse krav, er ikke nødvendigvis særligt stærke.
  For eksempel overholder adgangskoden “Adgangskode1” disse krav.

  Anbefalet indstilling: Ja

- Du finder en komplet oversigt over kravene under "Adgangskoden skal opfylde kompleksitetskravene" i onlinehjælpen til Windows Server.

- Gem adgangskoder ved hjælp af reversibel kryptering – reversibel kryptering benyttes i systemer, hvor et program skal have adgang til adgangskoder i klartekstformat. Dette er ikke nødvendigt i de fleste installationer.

  Anbefalet indstilling: Nej.

Yderligere oplysninger finder du i Windows Server 2003 Security Guide (Sikkerhedsguide til Windows Server 2003):

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

Definition af en politik for kontospærring

Vær forsigtig, når du definerer politikken for kontospærring. Kontospærringspolitikken bør aldrig angives i mindre virksomheder, da der er en stor sandsynlighed for, at godkendte brugere også bliver spærret, hvilket kan være meget kostbart for kunden.

Hvis kunden bestemmer sig for at anvende kontospærringspolitikken, skal indstillingen **Tæller til spærring af konti** angives til et så højt tal, at autoriserede brugere ikke bliver spærret, fordi de skriver deres adgangskoder forkert nogle gange.

Yderligere oplysninger om politikken for kontospærring finder du under "Oversigt over kontospærringspolitik" i onlinehjælpen til Windows Server.

Oplysninger om, hvordan du anvender eller redigerer politikken for kontospærring, finder du under "Sådan anvendes eller ændres kontospærringspolitikken" i onlinehjælpen til Windows Server.

Adgangskontrol

Et Windows-netværk og ressourcerne i det (herunder Navision) kan beskyttes ved at overveje, hvilke rettigheder brugere, grupper af brugere og andre computere skal have i netværket. Du kan beskytte en eller flere computere ved at tildele brugere eller grupper bestemte brugerrettigheder. Du kan beskytte et objekt, for eksempel en fil eller mappe, ved at tildele rettigheder, der lader brugerne eller grupperne udføre bestemte handlinger på objektet. De centrale komponenter i adgangskontrol er:

- Tilladelser
- Ejerskab af objekter
- Nedarvning af tilladelser
- Brugerrettigheder
- Objektovervågning.

Tilladelser

Tilladelser definerer, hvilken type adgang en bruger eller en gruppe skal have til et objekt eller en objektegenskab som f.eks. filer, mapper og objekter i registreringsdatabasen. Tilladelser anvendes på alle beskyttede objekter, for eksempel filer eller objekter i registreringsdatabasen. Tilladelser kan gives til enhver bruger, gruppe eller computer. Det er en god praksis at give tilladelser til grupper.

Ejerskab af objekter

Der knyttes en ejer til et objekt, når objektet oprettes. I Windows 2000 Server er ejeren som standard den, der opretter objektet. I Windows Server 2003 er dette ændret for objekter, der oprettes af medlemmer af gruppen Administratorer.

Når et medlem af gruppen Administratorer opretter et objekt i Windows Server 2003, bliver gruppen Administratorer ejeren, ikke den enkelte konto, der oprettede objektet. Denne funktionalitet kan ændres i MMC-snap-in-programmet (Microsoft Management Console) Lokale sikkerhedsindstillinger ved hjælp af indstillingen **Systemobjekter: Standardejer af objekter, der er oprettet af medlemmer af gruppen Administratorer**. Uanset hvilke tilladelser der er angivet for et objekt, kan objektets ejer altid ændre tilladelserne for objektet.

Yderligere oplysninger finder du under "Ejerskab" i onlinehjælpen til Windows Server.

Nedarvning af tilladelser

Med nedarvning er det nemt for administratorer at tildele og administrere tilladelser. Med denne funktion arver alle objekter i en objektbeholder automatisk alle de af objektbeholderens tilladelser, der kan nedarves. Når du for eksempel opretter filer i en mappe, arver de mappens tilladelser. Det er kun tilladelser, der er angivet til at kunne nedarves, som arves.

Brugerrettigheder

Brugerrettigheder giver bestemte rettigheder og logonrettigheder til brugere og grupper i computermiljøet.

Oplysninger om brugerrettigheder finder du under "Brugerrettigheder" i onlinehjælpen til Windows Server.

Objektovervågning

Du kan overvåge brugernes adgang til objekter. Du kan derefter få vist disse sikkerhedsrelaterede hændelser i sikkerhedsloggen ved hjælp af Logbog.

Yderligere oplysninger finder du under "Overvågning" i onlinehjælpen til Windows Server.

Bedste fremgangsmåder for adgangskontrol

- Giv tilladelser til grupper, ikke til brugere. Det er ikke effektivt at vedligeholde brugerkonti direkte, og tildeling af tilladelser på brugerbasis bør derfor kun ske undtagelsesvist.
- Benyt Afvis tilladelser til visse specialtilfælde. Du kan for eksempel benytte Afvis tilladelser til at udelukke en del af en gruppe, som har tilladelser.

- Afvis aldrig adgang til et objekt for gruppen Alle. Hvis du nægter alle adgang til et objekt, omfatter det også administratorerne. Det er bedre at fjerne gruppen Alle og i stedet giver andre brugere, grupper eller computere tilladelser til objektet. Husk, at hvis der ikke defineres nogen tilladelser, tillades der ingen adgang.
- Giv tilladelser til et objekt så højt oppe i træet som muligt, og benyt derefter nedarvning til at overføre sikkerhedsindstillingerne i træet. Du kan hurtigt og effektivt anvende adgangskontrolindstillinger på alle underordnede objekter eller et undertræ til et overordnet objekt. Ved at gøre dette opnår du den størst mulige effekt med den mindst mulige indsats. De tilladelsesindstillinger, du angiver, bør være tilstrækkelige for de fleste brugere, grupper og computere.
- Eksplicitte tilladelser kan undertiden tilsidesætte nedarvede tilladelser. En nedarvet afvisning af tilladelser forhindrer ikke adgang til et objekt, hvis objektet har en eksplicit indgang for Giv tilladelse. Eksplicitte tilladelser går forud for nedarvede tilladelser, også nedarvet afvisning af tilladelser.
- For tilladelser til Active Directory®-objekter skal du være sikker på, at du forstår de specifikke bedste fremgangsmåder for Active Directory-objekter.

Yderligere oplysninger finder du under "Bedste fremgangsmåder for tildeling af tilladelser til Active Directory-objekter" i onlinehjælpen til Windows Server 2003.

Firewall til ekstern sikkerhed

En firewall er en hardwarekomponent eller et softwareprogram, der forhindrer datapakker i enten at komme ind i eller ud fra et bestemt netværk. For at kontrollere trafikken åbnes eller lukkes porte i firewallen for informationspakker. Firewallen undersøger flere typer oplysninger i hver datapakke: Den protokol, der benyttes til at levere pakken, pakkens destination eller afsender, typen af indhold i pakken og det portnummer, den sendes til. Hvis firewallen er indstillet til at acceptere den angivne protokol gennem målporten, lukkes pakken igennem. Microsoft Windows Small Business Server 2003 Premium Edition leveres med Microsoft Internet Security and Acceleration (ISA) Server 2000 som firewallløsning. Small Business Server Standard Edition omfatter også en firewall.

ISA Server 2004

Internet Security and Acceleration (ISA) Server 2000 omdirigerer på sikker vis anmodninger og svar mellem internettet og klientcomputerne i det interne netværk.

ISA Server fungerer som en sikker gateway til internettet for klienterne i det lokale netværk. ISA Server-computeren fungerer usynligt for de andre parter i kommunikationsstien. Internetbrugeren bør ikke kunne mærke, at der er en firewallserver, medmindre brugeren forsøger at få adgang til en tjeneste eller et websted, som ISA Server-computeren ikke tillader adgang til. Den internetserver, der søges adgang til, fortolker anmodningerne fra ISA Server-computeren, som om anmodningerne kommer fra klientprogrammet.

Når du vælger IP-fragmentfiltrering (Internet Protocol), aktiverer du webproxyserver- og firewalltjenesterne for at filtrere fragmenter. Når pakkefragmenter filtreres, bliver alle fragmenterede IP-pakker slettet. En almindelig angrebsform består i at sende fragmenterede pakker og derefter sætte dem sammen på en måde, der kan beskadige systemet.

ISA Server har en funktion til sporing af kompromittering, som identificerer det tidspunkt, hvor der gøres forsøg på at angribe et netværk, og udfører en række konfigurerede handlinger (eller alarmer) i tilfælde af angreb.

Hvis IIS (Internet Information Services) er installeret på ISA Server-computeren, skal du konfigurere programmet til ikke at benytte de porte, som ISA Server bruger til udgående webanmodninger (som standard 8080) og indkommende webanmodninger (som standard 80). Du kan for eksempel indstille IIS til at overvåge port 81 og derefter konfigurere ISA Server-computeren til at omdirigere indkommende webanmodninger til port 81 på den lokale computer, der kører IIS.

Hvis der er konflikt mellem de porte, som ISA Server og IIS benytter, stopper installationsprogrammet IIS Publishing Service. Du kan derefter indstille IIS til at overvåge en anden port og genstarte IIS Publishing Service.

ISA Server-politikker

Du kan definere en ISA Server-politik, der fastsætter indgående og udgående adgang. Websteds- og indholdsregler angiver, hvilke websteder og hvilket indhold der er adgang til. Protokolregler angiver, om en bestemt protokol kan benyttes til indgående og udgående kommunikation.

Du kan oprette websteds- og indholdsregler, protokolregler, webudgivelsesregler og IP-pakkefiltre. Disse politikker bestemmer, hvordan ISA Server-klienterne kommunikerer med internettet, og hvilken kommunikation der er tilladt.

Virusbeskyttelse

En computervirus er en eksekverbar fil, der er udviklet til at kopiere sig selv, slette eller beskadige datafiler og programmer og undgå at blive opdaget. Virus omskrives og ændres ofte, så de ikke kan opdages. Virus sendes ofte som vedhæftede filer i e-mail. Antivirusprogrammer skal hele tiden opdateres, så de kan finde nye og ændrede virus. Virus er den hyppigst forekommende form for computervandalisme.

Antivirussoftware er specielt udviklet til at finde og forebygge virusprogrammer. Eftersom der hele tiden udvikles nye virusprogrammer, tilbyder mange udviklere af antivirusprogrammer jævnlige opdateringer af deres programmer til kunderne. Microsoft anbefaler kraftigt, at der implementeres antivirussoftware i kundens systemmiljø.

Virussoftware installeres normalt på følgende tre steder: brugernes arbejdsstationer, servere og det netværk, hvor e-mail modtages i (og i nogle tilfælde sendes fra) organisationen.

Virustyper

Der findes tre hovedtyper af virus, som inficerer computersystemer: startsektorvirus, filinficerende virus og trojanske heste.

Startsektorvirus

Når en computer startes, søger den i startsektoren på harddisken, før den indlæser operativsystemet eller andre startfiler. En startsektorvirus er udviklet til at overskrive oplysningerne i startsektoren på harddisken med sin egen kode. Når en computer er inficeret med en startsektorvirus, bliver virussens kode indlæst i hukommelsen før noget andet. Når virussen er indlæst i hukommelsen, kan den kopiere sig selv til andre diske, der benyttes på den inficerede computer.

Filinficerende virus

Filinficerende virus er den mest almindelige form for virus. De vedhæfter sig selv til eksekverbare programfiler ved at føje deres egen kode til den eksekverbare fil. Viruskoden tilføjes normalt på en måde, så den ikke bliver sporet. Når den inficerede fil køres, kan virussen vedhæfte sig selv til andre eksekverbare filer. Filer, der inficeres af denne type virus, har normalt filtypenavnene .com, .exe eller .sys.

Nogle filinficerende virus er udviklet til bestemte programmer. Programtyper, der ofte angribes, er .ovl-filer (overlay) og .dll-filer (Dynamic-Link Library). Disse filer bliver ikke udført, men eksekverbare filer kalder dem. Virussen overføres, når kaldet udføres.

Data beskadiges, når virussen udløses. En virus kan udløses, når en inficeret fil køres, eller når en miljøindstilling har en bestemt værdi (f.eks. en bestemt systemdato).

Trojanske heste

En trojansk hest er ikke et egentligt virusprogram. Den væsentligste forskel mellem en virus og en trojansk hest er, at den trojanske hest ikke kopierer sig selv, den ødelægger kun oplysninger på harddisken. En trojansk hest ligner et legitimt program, for eksempel et spil eller et hjælpeprogram. Men når programmet udføres, kan det ødelægge eller beskadige data.

Bedste fremgangsmåder for virusbeskyttelse

Udspredning af makrovirus kan forhindres. Her er nogle tip, som du bør dele med kunderne, til at undgå infektion.

- Installer et antivirusprogram, der scanner indkommende meddelelser fra internettet for virus, før meddelelserne passerer routeren. Dette sikrer dig, at e-mails bliver scannet for kendte virus.
- Kend kilden til de dokumenter, du modtager. Dokumenter bør ikke åbnes, medmindre de kommer fra en person, som kunden har tillid til.

- Tal med den person, der har oprettet dokumentet. Hvis brugerne ikke er sikre på, om et dokument er sikkert, skal de kontakte den person, der har oprettet dokumentet.
- Benyt beskyttelsen mod makrovirus i Microsoft Office. Office-programmerne giver brugeren besked, hvis et dokument indeholder makroer. Denne funktion gør det muligt for brugeren at aktivere eller deaktivere makroerne, når dokumentet åbnes.
- Brug et antivirusprogram til at søge efter og fjerne makrovirus. Antivirusprogrammer kan finde og ofte fjerne makrovirus fra dokumenter. Microsoft anbefaler, at der benyttes et antivirusprogram, som er certificeret af ICSA (International Computer Security Association).

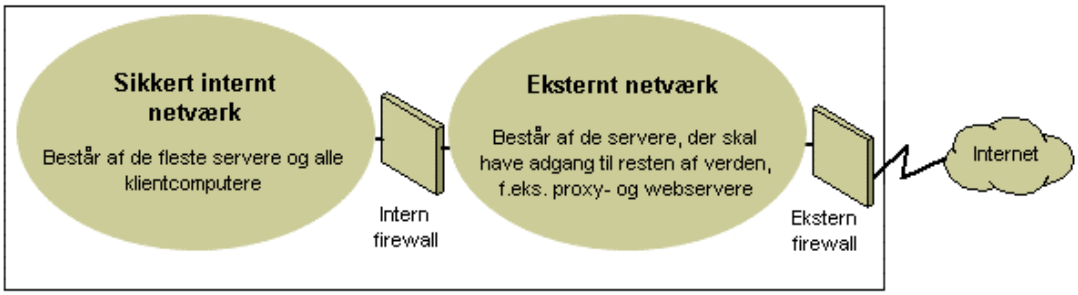
Yderligere generelle oplysninger om virus og computersikkerhed finder du på følgende Microsoft-websteder om sikkerhed:

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

Strategier for netværkssikkerhed

Da design og implementering af et IP-internetmiljø kræver afbalancering af private og offentlige netværkskrav, er firewallen blevet en vigtig delkomponent i beskyttelsen af netværkets integritet. En firewall er ikke en enkelt komponent. NCSA (National Computer Security Association) definerer en firewall som "et system eller en kombination af systemer, der fastlægger en grænse mellem to eller flere netværk". Selvom der benyttes forskellige begreber, kaldes grænsen ofte for et afskærmet netværk. Det afskærmede netværk beskytter intranettet eller virksomhedens lokale netværk (LAN – Local Area Network) mod indtrængen ved at kontrollere adgangen fra internettet eller andre større netværk.

Følgende diagram viser et afskærmet netværk, der er afgrænset med firewalls og placeret mellem et privat netværk og internettet for at beskytte det private netværk:



Grundlæggende afskærmet netværk

Organisationer benytter firewalls til at give sikkerhed på forskellige måder. IP-pakkefiltrering giver dårlig sikkerhed, er svær at administrere og let at kompromittere. Programgateways er mere sikre end pakkefiltre og lettere at administrere, fordi de kun gælder for nogle få, bestemte programmer, for eksempel et bestemt e-mail-system. Gateways på kredsløbsniveau er mest effektive, når brugeren af et netværksprogram udgør en større trussel end de data, som programmet overfører. En proxyserver er et omfattende sikkerhedsværktøj, der indeholder en programgateway, sikker adgang for anonyme brugere og andre tjenester. Her er nogle oplysninger om de forskellige muligheder:

- **IP-pakkefiltrering**
  IP-pakkefiltrering var den første implementering af firewallteknologi. Pakkeheaders undersøges for kilde- og destinationsadresser, TCP- og UDP-portnumre (Transmission Control Protocol og User Datagram Protocol) og andre oplysninger. Pakkefiltrering er en begrænset teknologi, der fungerer bedst i overskuelige sikkerhedsmiljøer, for eksempel hvis der ikke er tillid til noget uden for det afskærmede netværk, men der er tillid til alt inden for det afskærmede netværk. Nogle forhandlere har inden for de seneste år forbedret pakkefiltreringsmetoden ved at føje funktioner til intelligente beslutninger til pakkefiltreringskernen. Dette har skabt en ny form for pakkefiltrering kaldet *stateful protocol inspection*. Du kan konfigurere pakkefiltrering til enten at acceptere visse typer pakker og afvise alle andre eller til at afvise visse typer pakker og acceptere alle andre.
- **Programgateways**
  Programgateways bruges, når et programs egentlige indhold udgør den største trussel. Det, at de er programspecifikke, er både deres styrke og begrænsning, eftersom de er svære at tilpasse til teknologiske ændringer.
- **Kredsløbsgateways**
  Kredsløbsgateways er tunneler, der er bygget gennem en firewall, og som skaber forbindelse mellem bestemte processer eller systemer på den ene side med bestemte processer eller systemer på den anden side. Kredsløbsgateways er mest nyttige i de tilfælde, hvor den person, der bruger et program, udgør en større potentiel trussel end de oplysninger, som programmet overfører. Forskellen mellem en kredsløbsgateway og et pakkefilter er, at gatewayen kan oprette forbindelse til et eksternt programskema, der kan tilføre yderligere oplysninger.
- **Proxyservere**
  Proxyservere er omfattende sikkerhedsværktøjer, der indeholder firewall- og programgatewayfunktioner, som administrerer internettrafik til og fra et lokalnetværk. Proxyservere stiller også cachelagring af dokumenter og adgangskontrol til rådighed. En proxyserver kan forbedre ydeevnen ved at cachelagre data, der ofte forespørges efter, for eksempel populære websider, og stille dem direkte til rådighed. En proxyserver kan også filtrere og slette anmodninger, som ejeren finder upassende, for eksempel anmodninger om uautoriseret adgang til fortrolige filer.

Sørg for, at kunden benytter de firewallsikkerhedsfunktioner, der kan hjælpe dem. Placer et afskærmet netværk i netværkstopologien på et sted, hvor al trafik fra uden for virksomhedens netværk skal passere gennem afskærmningen, som opretholdes af en ekstern firewall. Du kan finindstille firewallens adgangskontrol, så den imødekommer kundens behov, og du kan konfigurere firewalls til at rapportere alle forsøg på uautoriseret adgang.

Hvis du vil minimere det antal porte, som du skal åbne på den indre firewall, kan du bruge en firewall på programniveau, for eksempel ISA Server 2000.

Yderligere oplysninger om TCP/IP finder du under "Designing a TCP/IP Network" (Design af et TCP/IP-netværk) på adressen http://www.microsoft.com/resources/documentation/WindowsServ/2003/all/deployguide/en-us/dnsbb_tcp_overview.asp.

Trådløse netværk

Trådløse netværk er som standard konfigureret, så det er muligt at lytte til de trådløse signaler. De kan være sårbare, hvis en hacker får adgang til dem, på grund af standardindstillingerne på noget trådløst hardware, den nemme adgang i trådløse netværk og de aktuelle krypteringsmetoder. Der er konfigurationsindstillinger og værktøjer, som kan beskytte mod aflytning, men husk, at de ikke beskytter computerne mod hackere og virus, der kommer ind via internetforbindelsen. Det er derfor ekstremt vigtigt at inkludere en firewall for at beskytte computerne mod uønsket indtrængen fra internettet.

Yderligere oplysninger om at beskytte et trådløst netværk finder du under "How to Make Your 802.11b Wireless Home Network More Secure" (Sådan gør du dit trådløse 802.11b-hjemmenetværk mere sikkert) på adressen http://support.microsoft.com/default.aspx?scid=kb;en-us;309369.

Netværkssikkerhedsscenarier

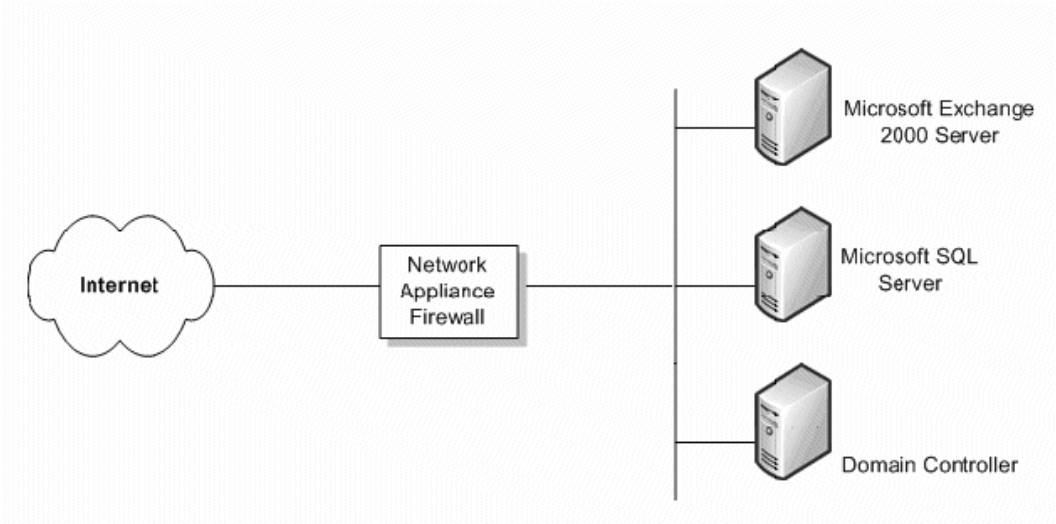
Den grad af sikkerhed, som kundens organisation har brug for, afhænger af flere faktorer. Det er som regel et kompromis mellem budgettet og behovet for at beskytte virksomhedens data. Det er muligt for en mindre virksomhed at have en meget kompleks sikkerhedsstruktur, der giver den bedst mulige netværkssikkerhed, men mindre virksomheder har muligvis ikke råd til denne grad af sikkerhed. I dette afsnit undersøger vi fire scenarier, og for hvert scenarie stiller vi forslag, der giver forskellige grader af sikkerhed.

Ingen firewall

Hvis kunden har forbindelse til internettet, men ingen firewall, skal der implementeres en form for netværkssikkerhed. Der findes enkle netværksfirewallkomponenter, som giver tilstrækkelig sikkerhed til at holde de fleste hackere ude.

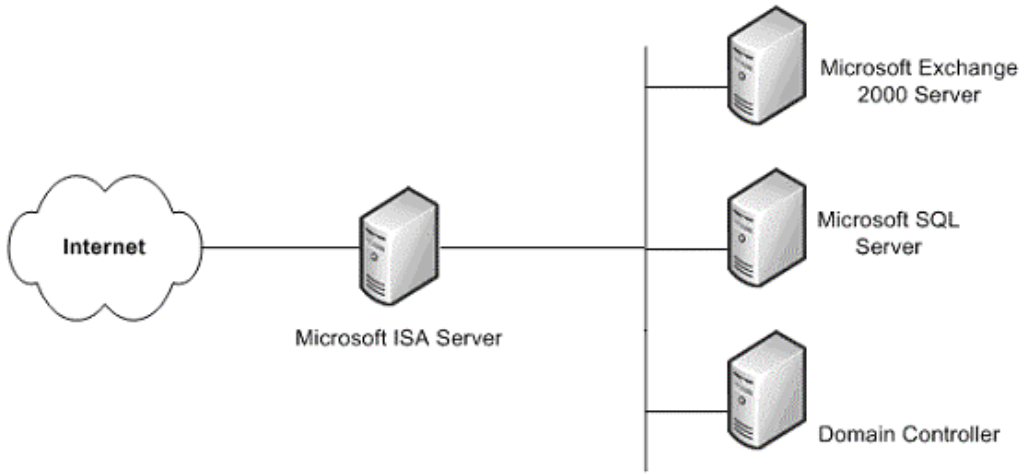
En enkel firewall

Den mindste grad af sikkerhed, der kan anbefales, er at have en enkel firewall mellem internettet og kundens data. Firewallen giver muligvis ikke nogen avanceret sikkerhed og må ikke antages for at være særligt sikker. Men den er bedre end ingenting.



Enkel firewall

Kundens budget tillader forhåbentlig en mere sikker løsning, der kan beskytte deres virksomhedsdata. ISA Server er en sådan løsning. Den forøgede omkostning til den ekstra server giver en langt bedre sikkerhed end en normal forbrugerfirewall, eftersom de kun stiller NAT (Network Address Translation) og pakkefiltrering til rådighed.



ISA Server-firewall

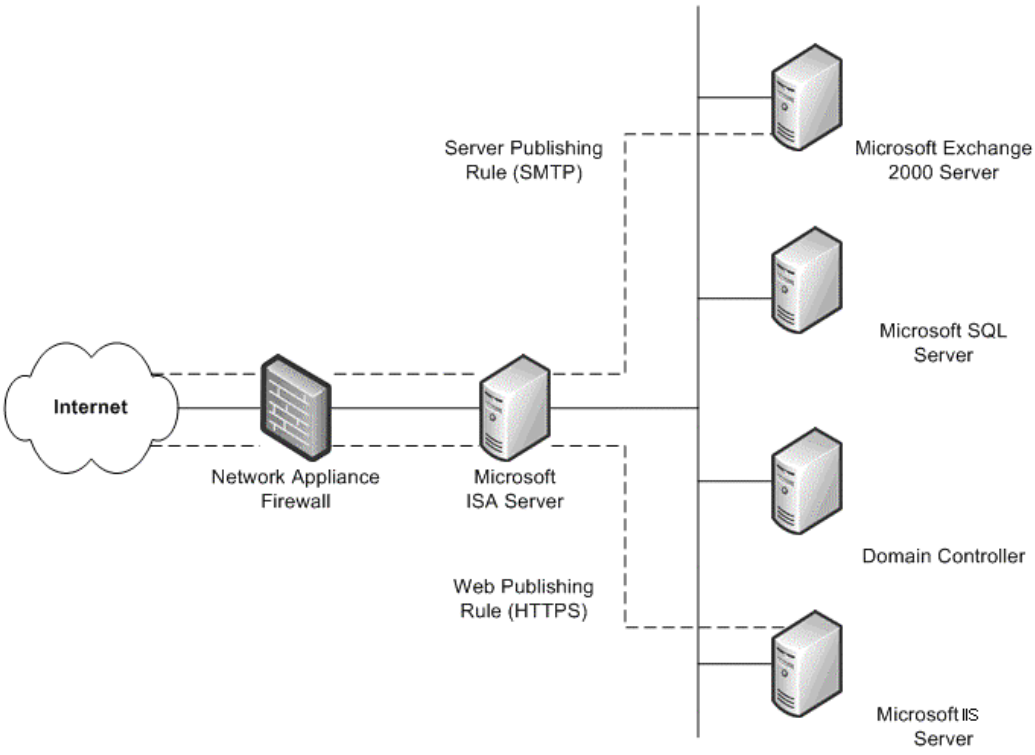
Denne løsning med én firewall er mere sikker end en simpel firewall og indeholder Windows-specifikke sikkerhedstjenester.

Én eksisterende firewall

Hvis kunden har én eksisterende firewall, der adskiller kundens intranet fra internettet, bør du muligvis overveje en ekstra firewall, der giver flere måder at konfigurere interne ressourcer til internettet på.

Webudgivelse er en af disse måder. Dette er, når der installeres en ISA Server foran organisationens webserver, der giver adgang for internetbrugere. Med indkommende webforespørgsler kan ISA Server fungere som en webserver over for verden udenfor, der opfylder klientanmodninger om webindhold fra dens cachelager. ISA Server videresender kun anmodninger til webserveren, når anmodningerne ikke kan efterkommes fra dens cachelager.

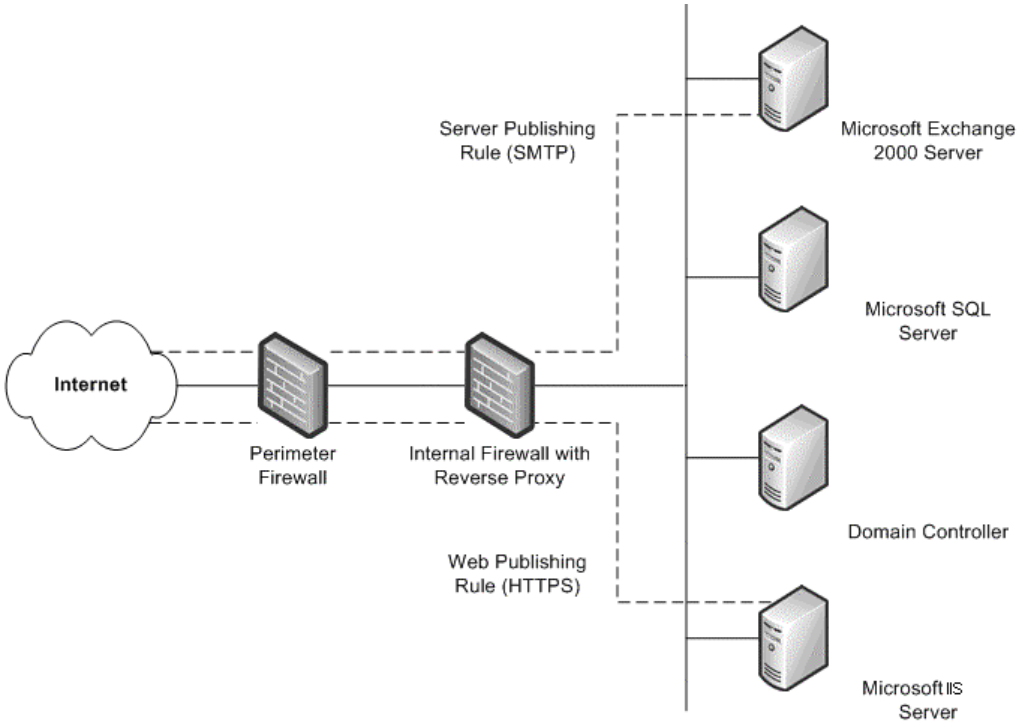
En anden metode er serverudgivelse. ISA Server gør det muligt at udgive interne servere til internettet uden at slække på det interne netværks sikkerhed. Du kan konfigurere regler for webudgivelse og serverudgivelse, der bestemmer, hvilke anmodninger der skal sendes til en server på det lokale netværk, for at skabe en højere grad af sikkerhed for de interne servere.



Eksisterende firewall med tilføjet ISA Server

To eksisterende firewalls

Det fjerde scenarie er, at organisationen har to firewalls installeret med et etableret afskærmet netværk (DMZ – demilitariseret zone). En eller flere af disse servere stiller omvendte proxytjenester til rådighed, så internetklienter ikke har direkte adgang til servere på intranettet. I stedet opfanger en af firewallene, helst den interne firewall, netværksanmodninger til interne servere, kontrollerer pakkerne og videresender dem på vegne af internetværten.



To eksisterende firewalls

Dette scenarie svarer til det foregående scenarie efter tilføjelsen af den anden firewall. Den eneste forskel er, at den interne firewall, der understøtter omvendt proxy, ikke er en ISA-server. I dette scenarie skal du arbejde tæt sammen med administratorerne af de to firewalls for at definere serverudgivelsesregler, som overholder sikkerhedspolitikken.

Administration af sikkerhedsrettelser

Operativsystemer og programmer er ofte meget komplekse. De kan bestå af millioner af kodelinjer, der er skrevet af mange forskellige programmører. Det er vigtigt, at softwaren fungerer pålideligt, og at den ikke kompromitterer sikkerheden eller stabiliteten i it-miljøet. Programmer afprøves grundigt, før de offentliggøres, for at minimere problemer. Imidlertid finder hackere hele tiden svagheder i software, hvorfor det er ikke er muligt at forudse alle fremtidige angreb.

I mange organisationer er administration af programrettelser en del af deres overordnede strategi for ændrings- og konfigurationsstyring. Uanset organisationens type og størrelse er det imidlertid af afgørende betydning at have en god strategi for administration af programrettelser, også selvom organisationen endnu ikke har etableret effektiv ændrings- og konfigurationsstyring. Langt de fleste gennemførte angreb mod computersystemer sker mod systemer, hvor sikkerhedsrettelser ikke er blevet installeret.

Sikkerhedsrettelser udgør en væsentlig udfordring for de fleste organisationer. Når der er fundet en svaghed i et program, spredes oplysningerne om den hurtigt i hackerkredse. Når der bliver opdaget en svaghed i Microsofts programmer, prøver vi at udgive en sikkerhedsrettelse så hurtigt som muligt. Indtil programrettelsen er installeret, kan den sikkerhed, som kunden forlader sig på, være alvorligt reduceret.

I Navision-miljøet skal du sikre dig, at kunderne installerer de nyeste sikkerhedsrettelser i hele systemet. Sørg for, at kunderne benytter de teknologier, som Microsoft har gjort tilgængelige. De omfatter:

- **Microsoft Security Notification Service**
  Security Notification Service er en liste over e-mail-adresser, der modtager beskeder, hver gang en opdatering bliver tilgængelig. Beskederne er en værdifuld del af en forebyggende sikkerhedsstrategi. De er også tilgængelige på TechNet-webstedet Product Security Notification: http://www.microsoft.com/technet/security/bulletin/notify.mspx.
- **Microsoft Automatiske opdateringer**
  Windows kan installere sikkerhedsopdateringer på dine computere automatisk.
- **Microsoft Security Bulletin-søgeværktøj**
  Security Bulletin-søgeværktøjet er tilgængeligt på webstedet for Security Bulletin Service: http://www.microsoft.com/technet/security/current.aspx. Kunden kan bestemme, hvilke opdateringer de har behov for, afhængigt af hvilket operativsystem, hvilke programmer og hvilke servicepakker de kører i øjeblikket.
- **MBSA (Microsoft Baseline Security Analyzer)**
  Dette grafiske værktøj er tilgængeligt fra webstedet til Microsoft Baseline Security Analyzer: http://www.microsoft.com/technet/security/tools/mbsahome.mspx. Værktøjet fungerer ved at sammenligne en computers aktuelle status med en liste over opdateringer, som Microsoft vedligeholder. MBSA udfører også grundlæggende sikkerhedstjek for indstillinger for adgangskodestyrke og -udløb, politikker for gæstekonto og en række andre punkter. MBSA søger desuden efter svagheder i Microsoft IIS (Internet Information Services), SQL Server™ 2000, Exchange 5.5, Exchange 2000 og Exchange Server 2003.
- **Microsoft SUS (Software Update Services)**
  Tidligere kaldt Windows Update Corporate Edition. Dette værktøj gør det muligt for virksomheder at placere alle kritiske opdateringer og SRP'er (Security Rollup Packages), som er tilgængelige på det offentlige Windows Update-websted, på lokale computere. Værktøjet arbejder sammen med en ny version af klienter til automatisk opdatering om at skabe rammen for en effektiv strategi for automatisk overførsel og installation. Det nye klientprogram til automatisk opdatering omfatter en klient til operativsystemerne Windows 2000 og Windows Server 2003 og kan installere de overførte opdateringer automatisk. Yderligere oplysninger om Microsoft SUS finder du på adressen http://www.microsoft.com/windows2000/windowsupdate/sus/default.asp.

- **SUS-funktionspakke (Software Update Services) til Microsoft SMS (Systems Management Server)**
  SUS-funktionspakken til SMS indeholder et antal værktøjer til at lette arbejdet med at installere softwareopdateringer i virksomheden. Værktøjerne omfatter Security Update Inventory Tool, Microsoft Office Inventory Tool for Updates, Distribute Software Updates Wizard og SMS Web Reporting Tool med Web Reports Add-in for Software Updates. Yderligere oplysninger om de enkelte værktøjer finder du på adressen http://www.microsoft.com/smserver/downloads/20/featurepacks/suspack/.

Tal med kunderne om hvert af disse værktøjer, og anbefal kunderne at benytte dem. Det er meget vigtigt, at sikkerhedsproblemer håndteres så hurtigt som muligt uden at kompromittere systemmiljøets stabilitet.

Sikkerhedsindstillinger i SQL Server 2000

Eftersom Navision også kører på SQL Server 2000, er det vigtigt, at du tager skridt til at forøge sikkerheden i kundens SQL Server 2000-installation. De følgende fremgangsmåder hjælper med at forbedre sikkerheden i SQL Server:

- Sørg for, at de seneste servicepakker og opdateringer er installeret til operativsystemet og SQL Server 2000. Du finder de seneste oplysninger på webstedet Microsoft Security http://www.microsoft.com/security/default.asp.
- For sikkerhed på filsystemniveau skal du sikre dig, at alle SQL Server 2000-data og -systemfiler er installeret på NTFS-partitioner. Gør kun filerne tilgængelige for administratorer eller brugere på systemniveau vha. NTFS-tilladelser. Dette forhindrer, at brugerne åbner filerne, når tjenesten MSSQLSERVER ikke kører.
- Benyt en domænekonto med få rettigheder, for eksempel NT Authority\Netværkstjeneste eller kontoen LocalSystem (anbefales) til SQL Server 2000-tjenesten (MSSQLSERVER). Denne konto bør have færrest muligt rettigheder i domænet og skal hjælpe med at begrænse (men ikke stoppe) et angreb på serveren i tilfælde af kompromittering. Kontoen skal med andre ord kun have rettigheder på lokalbrugerniveau i domænet. Hvis SQL Server 2000 bruger en domæneadministratorkonto til at køre tjenesterne, vil en kompromittering af serveren føre til kompromittering af hele domænet. Hvis du vil ændre denne indstilling, skal du benytte SQL Server Enterprise Manager til at foretage ændringen. Adgangskontrollisterne til filer, registreringsdatabasen og brugerrettigheder bliver automatisk ændret.
- De fleste udgaver af SQL Server 2000 installeres med to standarddatabaser, **Northwind** og **pubs**. Begge databaserne er eksempeldatabaser, der benyttes til test, oplæring og som generelle eksempler. De bør ikke installeres i et produktionssystem. Hvis databaserne er til stede, kan det få en angriber til at udnytte svagheder, der involverer standardindstillinger og standardkonfiguration. Hvis **Northwind** og **pubs** findes på SQL Server 2000-produktionscomputeren, bør de slettes.
- Overvågning af SQL Server 2000-systemet er som standard deaktiveret, så ingen betingelser overvåges. Dette gør det svært at opdage indtrængen og hjælper angribere med at dække deres spor. Du bør som minimum aktivere overvågning af mislykkede forsøg på logon.

De senest opdaterede sikkerhedsoplysninger til SQL Server 2000 finder du på adressen http://www.microsoft.com/sql/techinfo/administration/2000/security/default.asp.

Om Microsoft Business Solutions

Microsoft Business Solutions er en underafdeling af Microsoft, der tilbyder et stort udvalg af integrerede, komplette virksomhedsprogrammer og tjenester, som er beregnet til at hjælpe mindre, mellemstore og store virksomheder med at skabe forbindelse mellem kunder, medarbejdere, partnere og leverandører. Microsoft Business Solutions' programmer optimerer de strategiske virksomhedsprocesser på tværs af økonomistyring, virksomhedsanalyse, personaleadministration, projektstyring, kundeadministration, administration af udstationeringer, administration af forsyningskæder, e-commerce, produktion og salgsadministration. Programmerne er udviklet til at skabe den nødvendige indsigt for at hjælpe kundernes virksomheder med at opnå succes. Yderligere oplysninger om Microsoft Business Solutions finder du på adressen http://www.microsoft.com/BusinessSolutions/