Microsoft Business Solutions

Navision Security Hardening Guide

Gepubliceerd: oktober 2004

Microsoft

Inhoudsopgave

Inleiding

Microsoft® Windows® biedt geavanceerde, op standaarden gebaseerde netwerkbeveiliging. In het algemeen heeft beveiliging te maken met het incalculeren van risico's en het sluiten van compromissen. Een computer kan bijvoorbeeld in een afgesloten ruimte worden geplaatst die alleen toegankelijk is voor de systeembeheerder. Zo loopt de computer weliswaar geen gevaar, maar erg nuttig is het ook niet. De computer is namelijk niet verbonden met andere computers. U moet het netwerk zo veilig mogelijk proberen te maken zonder dat u de bruikbaarheid ervan beperkt.

De meeste organisaties plaatsen ter afwering van externe aanvallen een firewall. Veel bedrijven hebben echter geen procedure voor het beperken van de schade zodra een kwaadwillende gebruiker de firewall heeft omzeild. Beveiligingsmaatregelen in de netwerkomgeving van uw klant vormen een goede oplossing als gebruikers niet te veel stappen hoeven uit te voeren om op een veilige manier zaken te kunnen doen. De implementatie van beveiligingsbeleid moet voor gebruikers zo eenvoudig mogelijk zijn, anders vinden ze meestal wel minder veilige manieren om hun doel te bereiken.

Aangezien de omvang van Navision-installaties erg varieert, is het belangrijk dat er goed wordt nagedacht over de behoeften van iedere klant. De effectiviteit van de beveiliging moet worden afgewogen tegen de bijbehorende kosten. Raad, als vertrouwde adviseur van uw klant, een beleid aan dat zo goed mogelijk voldoet aan diens beveiligingsbehoeften, maar dat uiteindelijk niet zo’n grote belasting vormt dat de klant het beleid gaat negeren.

Aanbevolen procedures voor Navision-beveiliging

De volgende algemene richtlijnen kunnen u helpen bij de beveiliging van de Navision-omgeving:

- Als u Navision Database Server als een service wilt uitvoeren of de opdrachtregelparameter *installasservice* wilt gebruiken wanneer u de server start, moet u ervoor zorgen dat de service wordt uitgevoerd als de NT Authoriteit\Netwerkservice-account. De NT Authoriteit\Netwerkservice-account bestaat alleen op Windows™ XP en Windows Server™ 2003. Als u Windows 2000 Server hebt, moet u een account maken met minimale rechten voor de service, anders wordt aan de service een lokale systeemaccount toegewezen. Deze account mag maximaal dezelfde rechten hebben als de normale gebruikersaccount of een domeinaccount die noch in het domein, noch op een lokale computer beheerder is.

  U moet de NT Authoriteit\Netwerkservice-account of de gebruikersaccount waaronder de server wordt uitgevoerd, lees- en schrijfrechten geven voor de databasebestanden om ervoor te zorgen dat de gebruikers verbinding kunnen maken met de database.

  Als u de NT Authoriteit\Netwerkservice-account lees- en schrijftoegang wilt geven tot een databasebestand op Windows XP, gaat u als volgt te werk:

  1. Navigeer in Windows Verkenner naar de map die het databasebestand bevat.
  2. Selecteer het databasebestand, klik er met de rechtermuisknop op en klik vervolgens op Eigenschappen.
  3. Klik op het tabblad ***Beveiliging*** van het venster ***Eigenschappen*** en klik vervolgens op Toevoegen bij het veld **Namen van groepen of gebruikers**.
  4. Geef *Netwerkservice* op in het venster ***Gebruikers, computers of groepen selecteren*** en klik op OK.
  5. NETWERKSERVICE is toegevoegd aan het veld **Namen van groepen of gebruikers** in het venster ***Eigenschappen***.
  6. Selecteer NETWERKSERVICE in het veld **Machtigingen** en wijs hieraan *lees*- en *schrijf*rechten toe.
- De Navision Application Server-service wordt standaard uitgevoerd als de NT Authoriteit\Netwerkservice-account, waardoor er lokaal toegang kan worden verkregen tot Navision Database Server. Op een netwerk moet u er echter voor zorgen dat de Navision Application Server-service wordt uitgevoerd als een Windows-domeinaccount die wordt herkend door Navision Database Server, als u wilt dat deze toegang heeft tot de databaseserver. Deze account mag noch in het domein, noch op een lokale computer beheerder zijn.
- Als u SQL Server Option voor Navision uitvoert, wordt Microsoft SQL Server™ uitgevoerd als een service. Voor SQL Server Option voor Navision is vereist dat via SQL Server uit Active Directory lijsten van Windows-gebruikersgroepen kunnen worden opgehaald voor verificatiedoeleinden. U moet er daarom voor zorgen dat de SQL Server-service wordt uitgevoerd als de NT Authoriteit\Netwerkservice-account.

  Als u de service wilt uitvoeren als NT Authoriteit\Netwerkservice, gaat u als volgt te werk:

  1. Zoek op de SQL Server-computer de MSSQLSERVER-service, klik hierop met de rechtermuisknop en klik vervolgens op Eigenschappen.
  2. Klik op het tabblad ***Aanmelden*** in het venster ***Eigenschappen***.
  3. Klik op Deze account onder Aanmelden op het tabblad ***Aanmelden***, geef *NT Authoriteit\Netwerkservice* op en klik op OK.

Voor meer informatie over SQL Server-beveiliging gaat u naar:
http://www.microsoft.com/security/guidance/prodtech/SQLServer.mspx
en http://www.microsoft.com/technet/security/prodtech/dbsql/default.mspx

- Als u een e-businessproduct van Navision, zoals Commerce Gateway, hebt geïnstalleerd, moet u ervoor zorgen dat Commerce Gateway Request Server correct is geïnstalleerd, met de standaardaccountinstelling voor de services. De standaardaccountinstelling heet *CGRSUser* en geeft Commerce Gateway Server toegang tot een minimaal aantal andere vereiste services, waaronder de *MSSQLSERVER*-service en *BizTalk-service BizTalk-groep: BizTalkServerApplication*. Er worden geen globale-accountinstellingen toegewezen, zoals bij de account *Lokaal systeem*.
- Gebruik altijd sterke wachtwoorden. Voor meer informatie over sterke wachtwoorden gaat u naar het gedeelte Sterke wachtwoorden.
- Meld u aan via Windows. Navision staat twee soorten aanmeldingen toe: databaseaanmeldingen en Windows-aanmeldingen. We raden u aan u aan te melden via Windows omdat hierbij wordt gebruikgemaakt van Windows-verificatie en u in staat wordt gesteld een veilig wachtwoordbeleid te voeren.
- Voorkom hergebruik van wachtwoorden. Vaak wordt voor verschillende systemen en domeinen hetzelfde wachtwoord gebruikt. Een beheerder die verantwoordelijk is voor twee domeinen kan bijvoorbeeld in elk domein beheerdersaccounts maken die gebruikmaken van hetzelfde wachtwoord. Deze beheerder kan voor lokale beheerders op domeincomputers zelfs in het hele domein dezelfde wachtwoorden instellen. Als er in dit geval op één account of computer wordt ingebroken, kan het hele domein gevaar lopen.
- Nadat Navision is geïnstalleerd en de databases zijn gemaakt of bijgewerkt, moet u een Windows-aanmelding maken en deze toewijzen aan de SUPER-rol in Navision. Deze SUPER-gebruiker regelt het databasebeheer, de beveiliging, enzovoort. Geef deze aanmelding een sterk wachtwoord. Dit wachtwoord moet vertrouwelijk blijven. Hierop moet dezelfde beveiliging van toepassing zijn als op het SA-wachtwoord in SQL Server. Alle databasetoegang wordt beheerd door de SUPER-rol. Hiervoor is het hoogste beveiligingsniveau vereist. Het wachtwoord van de SUPER-gebruiker mag alleen bekend zijn bij de systeembeheerders.
- Aan alle andere gebruikers met toegang tot de Navision-database moeten zo min mogelijk machtigingen worden toegewezen. Dit houdt in dat aan hen in Navision rollen worden toegewezen waarmee zij alleen toegang krijgen tot de functies die ze nodig hebben om hun taken te kunnen uitvoeren binnen het bedrijf.
- Zorg ervoor dat alleen de gebruikers voor wie dit vereist is vanwege hun rol binnen het bedrijf FOB-bestanden kunnen importeren, objecten kunnen wijzigen en reservekopieën van databases kunnen maken en terugzetten.
- Maak regelmatig een reservekopie van de Navision-database en test de reservekopieën om te controleren of ze kunnen worden teruggezet.
- Bewaar de reservekopieën op een veilige plek om beschadiging door brand, rook, stof, hoge temperaturen, bliksem en milieurampen (bijvoorbeeld een aardbeving) tot een minimum te beperken.
- Hoewel Navision kan worden uitgevoerd op verschillende versies van Windows, is het aan te raden het nieuwste besturingssysteem te gebruiken, met de nieuwste beveiligingsvoorzieningen. Op dit moment zijn dat Windows XP (Service Pack 2) en Windows Server 2003.

- Gebruik de service Windows Update die wordt meegeleverd bij Windows 2000, Windows XP en Windows Server 2003 om de meest recente beveiligingsupdates toe te passen. Gebruik de functie Automatische updates van Windows om ervoor te zorgen dat op al uw clientcomputers de meest recente beveiligingspatches, service packs en updates zijn geïnstalleerd.
- Het is aan te raden om het beveiligde TCPS-protocol te gebruiken voor de communicatie tussen de Navision-clients en Navision Database Server. TCPS is een beveiligde versie van TCP/IP en maakt gebruik van SSPI (Security Support Provider Interface) met ingeschakelde codering en Kerberos-verificatie. TCPS is het standaardprotocol voor Navision Database Server.
- De klant moet een noodplan hebben om de services na een ramp snel te kunnen hervatten. Een noodplan moet het volgende omvatten:
  - Het verkrijgen van nieuwe/tijdelijke apparatuur.
  - Het terugzetten van reservekopieën op nieuwe systemen.
  - Testen of het noodplan echt werkt.

Fysieke beveiliging

Fysieke beveiliging is een absolute must, omdat deze niet kan worden vervangen door softwarebeveiliging. Als er bijvoorbeeld een vaste-schijfstation wordt gestolen, worden de gegevens op dat station uiteindelijk ook gestolen. Bespreek met uw klant de volgende fysieke-beveiligingskwesties bij het ontwikkelen van een beleid:

- Grote bedrijven met een eigen IT-afdeling moeten ervoor zorgen dat de serverruimtes en de locaties waar software wordt bewaard, worden afgesloten.
- Tot deze categorie behoren de volgende computers:
  - De Microsoft SQL Server 2000-server
  - De bestandsserver waarop de uitvoerbare Navision-bestanden zijn opgeslagen.
- Houd onbevoegde gebruikers uit de buurt van de computers.
- Installeer een inbraakalarm, ongeacht de gevoeligheid van de gegevens.
- Bewaar reservekopieën van kritieke gegevens in brandvrije containers op een andere locatie.

De werknemers

Het is een goed idee om de beheerdersrechten voor alle producten en functies te beperken. Klanten zouden hun werknemers standaard alleen leesrechten moeten geven voor systeemfuncties, tenzij de werknemers meer toegangsrechten nodig hebben om hun werk te kunnen doen. Microsoft raadt u aan het volgende principe te hanteren: geef gebruikers zo min mogelijk toegangsrechten tot gegevens en functies.
Ontevreden werknemers en ex-werknemers vormen een potentiële bedreiging voor de netwerkbeveiliging. Wanneer u de beveiliging bespreekt met uw klanten, kunt u het beste het volgende beleid aanbevelen ten aanzien van werknemers:

- Voer een antecedentenonderzoek uit voordat u iemand in dienst neemt.
- Houd er rekening mee dat ontevreden werknemers en ex-werknemers 'wraak' kunnen nemen.

- Controleer of alle bijbehorende Windows-accounts en -wachtwoorden zijn gedeactiveerd wanneer een werknemer de organisatie verlaat. U moet gebruikers, voor rapportagedoeleinden, niet verwijderen. Gebruik de accounts niet opnieuw.
- Leer gebruikers alert te zijn en verdachte activiteiten te melden.
- Wijs niet automatisch rechten toe. Als gebruikers geen toegang hoeven te hebben tot bepaalde computers, computerruimtes of reeksen bestanden, moet u ervoor zorgen dat dit ook niet het geval is.
- Leer supervisors potentiële problemen met werknemers te herkennen en hierop te reageren.
- Zorg ervoor dat werknemers hun rol begrijpen met betrekking tot de netwerkbeveiliging.
- Geef alle werknemers een kopie van het bedrijfsbeleid.
- Zorg ervoor dat gebruikers geen software kunnen installeren die niet is goedgekeurd door de werkgever.

De beheerder

We raden de systeembeheerders van uw klanten aan de nieuwste beveiligingsoplossingen te installeren die beschikbaar zijn via Microsoft. Kwaadwillenden zijn heel handig in het combineren van kleine fouten om op grote schaal te kunnen binnendringen in een netwerk. Beheerders moeten er eerst voor zorgen dat elke afzonderlijke computer zo veilig mogelijk is, en vervolgens beveiligingsupdates toevoegen en antivirussoftware gebruiken. In deze handleiding treft u veel koppelingen en bronnen aan die u helpen nuttige informatie en aanbevolen procedures te vinden.

Complexiteit is een ander gevaar voor de beveiliging van uw netwerk. Hoe complexer een netwerk is, hoe moeilijker het is om het te beveiligen of te repareren nadat een onbevoegde er toegang toe heeft verkregen. De beheerder moet de netwerktopografie zorgvuldig documenteren met als doel deze zo eenvoudig mogelijk te houden.

Beveiliging is hoofdzakelijk gericht op risicobeheer. Aangezien technologie niet zaligmakend is, is voor beveiliging een combinatie van technologie en beleid vereist. Met andere woorden: er zal nooit een product komen dat u alleen maar hoeft uit te pakken en te installeren op het netwerk, en dat onmiddellijk zorgt voor een perfecte beveiliging. Beveiliging is het resultaat van zowel technologie als beleid. Het beveiligingsniveau van een netwerk wordt uiteindelijk bepaald door de manier waarop de technologie wordt gebruikt. Microsoft levert technologie en functionaliteit waarbij rekening is gehouden met de beveiliging, maar alleen de beheerder kan, met uw hulp, het juiste beleid bepalen voor een organisatie. Zorg ervoor dat u tijdens het implementatieproces in een vroeg stadium de beveiliging meeneemt. Vraag wat uw cliënt wil beveiligen en wat deze bereid is hiervoor te doen.

Stel tot slot een plan op voor noodgevallen voordat deze optreden. Als u een gedegen planning combineert met solide technologie, heeft uw klant een uitstekend beveiligingssysteem.

Zie voor meer informatie over beveiliging in het algemeen 'The Ten Immutable Laws of Security Administration' op:
http://www.microsoft.com/technet/archive/community/columns/security/essays/10salaws.mspx.

en de artikelen over beveiligingsbeheer op:
http://www.microsoft.com/technet/community/columns/secmgmt/smarch.mspx

Het serverbesturingssysteem beveiligen

Hoewel veel kleinere klanten waarschijnlijk geen serverbesturingssysteem zullen hebben, is het belangrijk dat u de aanbevolen beveiligingsprocedures begrijpt en deze kunt uitleggen aan grotere klanten met complexere netwerkomgevingen. U moet zich er ook van bewust zijn dat grote delen van het beleid en de procedures uit dit document eenvoudig kunnen worden toegepast op klanten die enkel clientbesturingssystemen hebben.

De concepten in dit gedeelte zijn van toepassing op zowel Microsoft Windows 2000 Server- als Microsoft Windows Server 2003-producten, hoewel deze informatie hoofdzakelijk is gehaald uit de on line Help van Windows Server 2003. Windows Server 2003 biedt een degelijke set beveiligingsfuncties. De on line Help van Windows Server 2003 bevat uitgebreide informatie over alle beveiligingsfuncties en -procedures.

Ga voor meer informatie over Windows 2000 Server naar het Windows 2000 Server Security Center op
http://www.microsoft.com/technet/security/prodtech/win2000/default.mspx.

en lees de Windows 2000 Security Hardening Guide op:
http://www.microsoft.com/technet/security/prodtech/win2000/win2khg/default.mspx

Zie voor meer informatie over Windows Server 2003 de *Windows Server 2003 Security Guide* op
http://www.microsoft.com/technet/security/prodtech/win2003/w2003hg/sgch00.mspx

De primaire functies van het beveiligingsmodel van de Windows-server zijn verificatie, toegangsbeheer en eenmalige aanmelding:

- Verificatie is het proces waarbij de identiteit van een gebruiker wordt geverifieerd aan de hand van diens aanmeldingsreferenties. De naam en het wachtwoord van de gebruiker worden vergeleken met die in een goedgekeurde lijst. Als de referenties worden herkend, krijgt de gebruiker in zoverre toegang als is aangegeven in de machtigingslijst voor de desbetreffende gebruiker.
- Toegangsbeheer beperkt de toegang van gebruikers tot gegevens of computerbronnen op basis van de identiteit van gebruikers en hun lidmaatschap van verschillende vooraf gedefinieerde groepen. Toegangsbeheer wordt normaal gesproken door systeembeheerders gebruikt voor het regelen van de toegang die gebruikers hebben tot netwerkbronnen, zoals servers, mappen en bestanden. Dit gebeurt meestal door gebruikers en groepen toegangsrechten te geven voor bepaalde objecten.

- Dankzij eenmalige aanmelding hoeft een gebruiker zich maar eenmaal aan te melden bij het Windows-domein, met één wachtwoord, om te worden geverifieerd voor alle computers in het Windows-domein. Dankzij eenmalige aanmelding kunnen beheerders wachtwoordverificatie implementeren in het hele Windows-netwerk, terwijl eindgebruikers eenvoudig toegang kunnen verkrijgen.

De volgende gedeelten bevatten uitgebreidere beschrijvingen van deze drie kernfuncties.

Verificatie

Verificatie is een essentieel onderdeel van de systeembeveiliging. Het wordt gebruikt om de identiteit te bevestigen van elke gebruiker die probeert zich aan te melden bij een domein of toegang te krijgen tot netwerkbronnen. De zwakke schakel in de meeste verificatiesystemen is het wachtwoord van de gebruiker.

Wachtwoorden vormen de eerste verdedigingslinie tegen toegang van onbevoegden tot het domein en lokale computers. Beveel de volgende procedures voor wachtwoorden aan:

- Gebruik altijd sterke wachtwoorden.
- Als wachtwoorden op een stuk papier moeten worden geschreven, bewaar het papier dan op een veilige plek en vernietig het als het niet meer nodig is.
- Vertel een wachtwoord nooit aan iemand anders.
- Gebruik voor elke gebruikersaccount een ander wachtwoord.
- Wijzig wachtwoorden regelmatig.
- Let op waar wachtwoorden worden opgeslagen op computers.

Sterke wachtwoorden

De rol die wachtwoorden spelen in de beveiliging van het netwerk van een organisatie wordt vaak onderschat of over het hoofd gezien. Zoals eerder al is gezegd, vormen wachtwoorden de eerste verdedigingslinie tegen toegang van onbevoegden tot het netwerk. Zorg er dus voor dat uw klanten hun werknemers verplichten sterke wachtwoorden te gebruiken.

De hulpprogramma's die worden gebruikt voor het kraken van wachtwoorden, worden echter steeds beter en de computers die hiervoor worden gebruikt, zijn krachtiger dan ooit. Een geautomatiseerd hulpprogramma voor het kraken van wachtwoorden kan elk wachtwoord kraken, als er maar genoeg tijd is. Toch zijn sterke wachtwoorden moeilijker te kraken dan zwakke wachtwoorden.

Voor richtlijnen voor het maken van sterke wachtwoorden die de gebruiker kan onthouden, gaat u naar

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

en

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

Het wachtwoordbeleid definiëren

Wanneer u samen met uw klant het wachtwoordbeleid definieert, moet u zorgen dat het gebruik van sterke wachtwoorden verplicht wordt gesteld voor alle gebruikersaccounts. Voor de meeste systemen is het voldoende als u de aanbevelingen in de Windows Server 2003 Security Guide ter harte neemt:

- Definieer de beleidsinstelling **Uniekheid van wachtwoorden forceren door laatste wachtwoord(en) te onthouden** zodanig dat meerdere oude wachtwoorden worden onthouden. Als deze beleidsinstelling is ingeschakeld, kunnen gebruikers niet hetzelfde wachtwoord gebruiken wanneer het vervalt.

  Aanbevolen instelling: 24

- Definieer de beleidsinstelling **Maximale wachtwoordduur** zodanig dat wachtwoorden zo vaak als nodig voor de omgeving van de klant vervallen.

  Aanbevolen instelling: tussen 42 (de standaardinstelling) en 90.

- Definieer de beleidsinstelling **Minimale wachtwoordduur** zodanig dat wachtwoorden niet kunnen worden gewijzigd voordat ze meer dan een bepaald aantal dagen oud zijn. Deze beleidsinstelling werkt samen met de beleidsinstelling **Uniekheid van wachtwoorden forceren door laatste wachtwoord(en) te onthouden**. Als er een minimale wachtwoordduur is gedefinieerd, kunnen gebruikers hun wachtwoord niet herhaaldelijk wijzigen om de beleidsinstelling **Uniekheid van wachtwoorden forceren door laatste wachtwoord(en) te onthouden** te omzeilen en vervolgens hun oorspronkelijke wachtwoord te gebruiken. Gebruikers moeten het opgegeven aantal dagen wachten voordat ze hun wachtwoord kunnen wijzigen.

  Aanbevolen instelling: 2.

- Definieer de beleidsinstelling **Minimale wachtwoordlengte** zodanig dat wachtwoorden minimaal een bepaald aantal tekens moeten bevatten. Lange wachtwoorden, van zeven of meer tekens, zijn normaal gesproken sterker dan korte. Als u deze beleidsinstelling inschakelt, kunnen gebruikers geen lege wachtwoorden gebruiken en moeten ze wachtwoorden maken die minimaal een bepaald aantal tekens lang zijn.

  Aanbevolen instelling: 8.

- Schakel de beleidsinstelling **Wachtwoorden moeten voldoen aan complexiteitsvereisten** in. Als u dit doet, wordt er gecontroleerd of alle nieuwe wachtwoorden voldoen aan de basisvereisten voor sterke wachtwoorden. Met deze instelling zorgt u ervoor dat wachtwoorden minimaal drie symbolen hebben uit de vier categorieën (hoofdletters, kleine letters, cijfers, niet-alfanumerieke symbolen) en niet een deel van de gebruikersnaam of de voor- of achternaam van de gebruiker bevatten.

  Opmerking
  Wachtwoorden die aan deze vereisten voldoen, hoeven nog niet heel sterk te zijn. Het wachtwoord 'Wachtwoord1' voldoet bijvoorbeeld aan deze vereisten.

  Aanbevolen instelling: Ja

- Zie voor een volledige lijst met deze vereisten 'Wachtwoorden moeten voldoen aan complexiteitsvereisten' in de on line Help van Windows Server.

- Sla wachtwoorden op met behulp van omkeerbare codering. Omkeerbare codering wordt gebruikt in systemen waarbij een toepassing toegang nodig heeft tot leesbare wachtwoorden. Voor de meeste implementaties is deze codering niet nodig.

  Aanbevolen instelling: Nee.

Zie voor meer informatie de Windows Server 2003 Security Guide:

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

Een accountvergrendelingsbeleid definiëren

Wees voorzichtig bij het definiëren van het accountvergrendelingsbeleid. In een klein bedrijf moet nooit een accountvergrendelingsbeleid worden ingesteld, omdat daardoor hoogstwaarschijnlijk ook bevoegde gebruikers worden uitgesloten. Dit kan uw klant veel geld kosten.

Als de klant besluit een accountvergrendelingsbeleid toe te passen, stelt u de beleidsinstelling **Drempel voor accountvergrendelingen** in op een getal dat hoog genoeg is om bevoegde gebruikers niet uit te sluiten van hun gebruikersaccounts omdat ze hun wachtwoord een paar keer verkeerd typen.

Zie voor meer informatie over het accountvergrendelingsbeleid 'Accountvergrendelingsbeleid - overzicht' in de on line Help van Windows Server.

Zie voor informatie over het toepassen of wijzigen van het accountvergrendelingsbeleid 'Accountvergrendelingsbeleid toepassen of aanpassen' in de on line Help van Windows Server.

Toegangsbeheer

Een Windows-netwerk en de bijbehorende bronnen (waaronder Navision) kunnen worden beveiligd door zorgvuldig om te gaan met de rechten van gebruikers, gebruikersgroepen en andere computers op het netwerk. U kunt een of meer computers beveiligen door specifieke gebruikersrechten te verlenen aan gebruikers of groepen. U kunt een object, zoals een bestand of map, beveiligen door machtigingen toe te wijzen die gebruikers of groepen toestaan bepaalde acties uit te voeren op dat object. De belangrijkste concepten in verband met toegangsbeheer zijn:

- Machtigingen
- Eigendom van objecten
- Overname van machtigingen
- Gebruikersrechten
- Objectcontrole

Machtigingen

Met machtigingen definieert u het type toegang dat wordt verleend aan een gebruiker of groep tot een object of objecteigenschap, zoals bestanden, mappen en registerobjecten. U kunt machtigingen verlenen voor elk beveiligd object, zoals een bestand of een registerobject. Machtigingen kunnen worden verleend aan elke gebruiker, groep of computer. Het is aan te raden om machtigingen te verlenen aan groepen.

Eigendom van objecten

Wanneer een object wordt gemaakt, wordt hieraan een eigenaar toegewezen. In Windows 2000 Server is de maker van het object automatisch de eigenaar. Dit geldt in Windows Server 2003 niet meer voor objecten die worden gemaakt door leden van de groep Beheerders.

Wanneer een lid van de groep Beheerders een object maakt in Windows Server 2003, is de groep Beheerders de eigenaar in plaats van de account die het object heeft gemaakt. U kunt deze instelling wijzigen in de MMC-module Lokale beveiligingsinstellingen (Microsoft Management Console) via **Systeemobjecten: de standaardeigenaar van objecten wordt gemaakt door leden van de groep Beheerders**. De eigenaar van een object kan de machtigingen voor dat object altijd wijzigen, ongeacht de machtigingen die op dat moment zijn ingesteld voor het object.

Zie voor meer informatie 'Eigendom' in de on line Help van Windows Server.

Overname van machtigingen

De overnamefunctie stelt beheerders in staat machtigingen eenvoudig toe te wijzen en te beheren. Door deze functie nemen objecten in een container automatisch alle hiertoe ingestelde machtigingen van die container over. Bijvoorbeeld: wanneer u bestanden maakt in een map, nemen deze de machtigingen van die map over. Alleen de machtigingen die zijn gemarkeerd voor overname, worden overgenomen.

Gebruikersrechten

Gebruikersrechten zijn bepaalde machtigingen en aanmeldingsrechten voor gebruikers en groepen in uw computeromgeving.

Zie voor meer informatie over gebruikersrechten het gedeelte 'Gebruikersrechten' in de on line Help van Windows Server.

Objectcontrole

U kunt de toegang van gebruikers tot objecten controleren. Vervolgens kunt u deze beveiligingsgebeurtenissen bekijken in het beveiligingslogboek met behulp van Logboeken.

Zie voor meer informatie 'Controlebeleid' in de on line Help van Windows Server.

Aanbevolen procedures voor toegangsbeheer

- Wijs machtigingen toe aan groepen in plaats van gebruikers. Aangezien het rechtstreekse onderhoud van gebruikersaccounts geen efficiënte manier van werken is, moet u alleen in uitzonderlijke gevallen machtigingen toewijzen aan gebruikers.
- Gebruik Weigeren-machtigingen voor speciale gevallen. U kunt Weigeren-machtigingen bijvoorbeeld gebruiken om een subset of een groep uit te sluiten waarvoor Toestaan-machtigingen zijn ingesteld.
- Weiger de groep Iedereen nooit de toegang tot een object. Als u iedereen de toegang weigert tot een object, geldt dit ook voor de beheerders. U kunt de groep Iedereen beter verwijderen en andere gebruikers, groepen of computers machtigingen verlenen voor het object. Als er geen machtigingen zijn gedefinieerd, is toegang niet toegestaan.
- Wijs machtigingen toe aan een object dat zo hoog mogelijk staat in de structuur en pas hierop vervolgens overname toe om de beveiligingsinstellingen door te geven aan alle onderliggende objecten in de structuur. U kunt snel en effectief toegangsbeheerinstellingen toepassen op alle onderliggende objecten of op de substructuur van een bovenliggend object. Op deze manier sorteert u met een minimale inspanning een zo groot mogelijk effect. De machtigingsinstellingen die u configureert, moeten geschikt zijn voor het merendeel van de gebruikers, groepen en computers.
- Specifieke machtigingen hebben soms voorrang op overgenomen machtigingen. Overgenomen Weigeren-machtigingen verhinderen de toegang tot een object niet als het object een specifieke Toestaan-machtiging heeft. Specifieke machtigingen hebben voorrang op overgenomen machtigingen, zelfs op overgenomen Weigeren-machtigingen.
- Als u machtigingen voor Active Directory®-objecten wilt gebruiken, moet u de aanbevolen procedures voor Active Directory-objecten kennen.

Zie voor meer informatie 'Aanbevolen procedures voor het toewijzen van machtigingen voor Active Directory-objecten' in de on line Help van Windows Server 2003.

Externe beveiligingsfirewall

Een firewall is hardware of software die voorkomt dat gegevenspakketten een bepaald netwerk binnengaan of verlaten. Om het verkeer te kunnen regelen worden poorten in de firewall geopend of gesloten voor informatiepakketten. Er wordt gekeken naar verschillende zaken in elk gegevenspakket: Het protocol waarmee het pakket wordt geleverd, de bestemming of de afzender van het pakket, het type inhoud van het pakket en het poortnummer waarnaar het wordt verzonden. Als de firewall zo is ingesteld dat het opgegeven protocol is toegestaan voor de gewenste poort, mag het pakket erdoor. Bij Microsoft Windows Small Business Server 2003 Premium Edition wordt Microsoft Internet Security and Acceleration (ISA) Server 2000 meegeleverd als firewalloplossing. Small Business Server Standard Edition bevat ook een firewall.

ISA Server 2004

Internet Security and Acceleration (ISA) Server 2000 regelt op een veilige manier het verkeer tussen internet en clientcomputers op het interne netwerk.

ISA Server fungeert als een beveiligde gateway naar internet voor clients op het lokale netwerk. De ISA Server-computer is transparant voor de andere partijen in het communicatiepad. Internetgebruikers moeten niet kunnen zien dat er een firewallserver aanwezig is, tenzij de gebruiker probeert toegang te krijgen tot een service of naar een site te gaan waartoe de ISA Server-computer de toegang weigert. De internetserver waartoe wordt geprobeerd toegang te verkrijgen, interpreteert de verzoeken van de ISA Server-computer alsof ze afkomstig zijn van de clienttoepassing.

Wanneer u IP-fragmentfiltering (Internet Protocol) kiest, schakelt u de webproxy- en firewallservices in voor het filteren van pakketfragmenten. Door pakketfragmenten te filteren worden alle gefragmenteerde IP-pakketten geweigerd. Het verzenden van gefragmenteerde pakketten om deze vervolgens weer zodanig samen te voegen dat ze het systeem kunnen beschadigen, is een bekende aanvalstechniek.

ISA Server heeft een mechanisme voor het opsporen van indringers waarmee het tijdstip wordt geregistreerd waarop een aanval op een netwerk wordt uitgevoerd, en waarmee een reeks geconfigureerde acties (of waarschuwingen) wordt uitgevoerd in geval van een aanval.

Als IIS (Internet Information Services) is geïnstalleerd op de ISA Server-computer, moet u IIS zodanig configureren dat deze niet de poorten gebruikt die ISA Server gebruikt voor uitgaande (standaard 8080) en binnenkomende webverzoeken (standaard 80). U kunt IIS bijvoorbeeld poort 81 laten controleren en de ISA Server-computer vervolgens zodanig configureren dat de binnenkomende webverzoeken worden gestuurd naar poort 81 op de lokale computer met IIS.

Als er een conflict optreedt tussen poorten die ISA Server en IIS gebruiken, wordt de IIS-publicatieservice beëindigd. Vervolgens kunt u IIS een andere poort laten controleren en de IIS-publicatieservice opnieuw starten.

ISA Server-beleid

U kunt een ISA Server-beleid definiëren dat de toegang van binnenkomend en uitgaand verkeer regelt. Site- en inhoudsregels geven aan tot welke sites en inhoud toegang is toegestaan. Protocolregels geven aan of een bepaald protocol toegankelijk is voor binnenkomende en uitgaande communicatie.

U kunt site- en inhoudsregels, protocolregels, webpublicatieregels en IP-pakketfilters maken. Dit beleid bepaalt hoe de ISA Server-clients communiceren met internet en welke communicatie is toegestaan.

Virusbeveiliging

Een computervirus is een uitvoerbaar bestand dat is ontworpen om zichzelf te vermenigvuldigen, gegevensbestanden en programma's te wissen of te beschadigen, en opsporing te verhinderen. Virussen worden vaak herschreven en aangepast om opsporing te voorkomen. Virussen worden vaak verzonden als e-mailbijlage. Antivirusprogramma's moeten voortdurend worden bijgewerkt om nieuwe en aangepaste virussen te kunnen opsporen. Virussen zijn de belangrijkste vorm van computercriminaliteit.

Antivirussoftware is speciaal ontworpen voor de opsporing van en beveiliging tegen virusprogramma's. Aangezien er continu nieuwe virusprogramma's worden gemaakt, bieden veel makers van antivirusproducten hun klanten periodieke updates voor hun software aan. Microsoft beveelt u ten zeerste aan antivirussoftware te implementeren in de netwerkomgeving van uw klant.

Antivirussoftware wordt meestal op de volgende drie locaties geïnstalleerd: werkstations van gebruikers, servers en de netwerklocatie waar e-mail de organisatie binnenkomt (en, in sommige gevallen, verlaat).

Soorten virussen

Er zijn drie belangrijke soorten virussen die computersystemen kunnen infecteren: opstartsectorvirussen, virussen die bestanden infecteren, en Trojaanse paarden.

Opstartsectorvirussen

Wanneer u een computer opstart, wordt de opstartsector van de vaste schijf gescand voordat het besturingssysteem of andere opstartbestanden worden geladen. Een opstartsectorvirus is ontworpen om de informatie in de opstartsectoren van de vaste schijf te vervangen door eigen code. Wanneer een computer is geïnfecteerd met een opstartsectorvirus, wordt de viruscode als eerste in het geheugen gelezen. Zodra het virus in het geheugen is opgeslagen, kan het zich verspreiden naar andere schijven die de geïnfecteerde computer gebruikt.

Virussen die bestanden infecteren

Het meestvoorkomende type virus, dat bestanden infecteert, hecht zichzelf aan een uitvoerbaar programmabestand door hieraan eigen code toe te voegen. De viruscode wordt meestal zodanig toegevoegd dat deze niet kan worden opgespoord. Wanneer het geïnfecteerde bestand wordt uitgevoerd, kan het virus zich hechten aan andere uitvoerbare bestanden. Bestanden die worden geïnfecteerd door dit type virus, hebben meestal de extensie .COM, .EXE of .SYS.

Sommige virussen die bestanden infecteren, zijn ontworpen voor specifieke programma's. OVL- en DLL-bestanden zijn programmatypen die hiervan vaak het slachtoffer zijn. Hoewel deze bestanden niet worden uitgevoerd, worden ze wel aangeroepen door uitvoerbare bestanden. Het virus wordt overgebracht wanneer de aanroep plaatsvindt.

Gegevens raken beschadigd wanneer het virus wordt geactiveerd. Een virus kan worden geactiveerd wanneer een geïnfecteerd bestand wordt uitgevoerd of er aan een bepaalde omgevingsinstelling wordt voldaan (bijvoorbeeld een bepaalde systeemdatum).

Trojaanse paarden

Een Trojaans paard is eigenlijk geen virus. Het belangrijkste verschil tussen een virus en een Trojaans paard is dat deze laatste zichzelf niet vermenigvuldigt. Een Trojaans paard vernietigt alleen gegevens op de vaste schijf. Een Trojaans paard doet zich voor als een onschuldig programma, zoals een spelletje of een hulpprogramma. Wanneer het wordt uitgevoerd, kan het echter gegevens vernietigen of coderen.

Aanbevolen procedures voor virusbeveiliging

U kunt de verspreiding van een macrovirus voorkomen. Hier volgt een aantal tips ter voorkoming van infectie, die u met uw klanten kunt delen:

- Installeer een virusbeveiligingsoplossing die binnenkomende berichten van internet scant op virussen voordat de berichten langs de router mogen. Zo zorgt u ervoor dat e-mails worden gescand op bekende virussen.
- Let op de bron van de documenten die u ontvangt. Documenten mogen alleen worden geopend als ze afkomstig zijn van personen die door de klant worden vertrouwd.
- Neem contact op met de persoon die het document heeft gemaakt. Als gebruikers niet helemaal zeker weten of het document veilig is, moeten ze contact opnemen met de persoon die het document heeft gemaakt.
- Gebruik de macrovirusbeveiliging van Microsoft Office. In Office wordt de gebruiker gewaarschuwd als een document macro's bevat. Dankzij deze functie kunnen gebruikers de macro's in- of uitschakelen als het document wordt geopend.
- Gebruik virusscansoftware om macrovirussen op te sporen en te verwijderen. Met virusscansoftware kunt u macrovirussen opsporen in en vaak ook verwijderen uit documenten. Microsoft beveelt het gebruik van antivirussoftware aan die is gecertificeerd door het ICSA, een internationale vereniging voor computerbeveiliging.

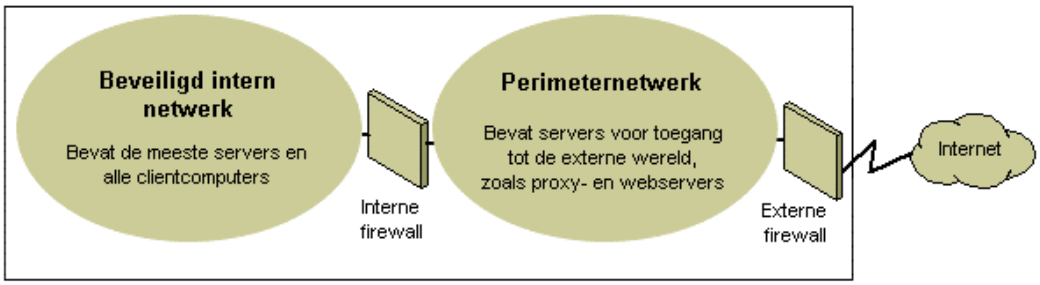
Voor meer informatie over virussen en computerbeveiliging in het algemeen gaat u naar de volgende Microsoft Security-websites:

- Microsoft Security op http://www.microsoft.com/security/default.asp.
- Documentatie over beveiliging op Microsoft TechNet http://www.microsoft.com/technet/security/Default.mspx.

Strategieën voor netwerkbeveiliging

Aangezien voor het ontwerp en de implementatie van een IP-internetwerkomgeving een balans moet worden gevonden tussen openbare en privé-netwerkkwesties, is de firewall een belangrijk onderdeel geworden van de bescherming van de netwerkintegriteit. Een firewall bestaat niet uit één onderdeel. De NCSA, een vereniging voor computerbeveiliging, definieert een firewall als 'een systeem (of combinatie van systemen) dat een grens vormt tussen twee of meer netwerken'. Hoewel er verschillende termen in gebruik zijn, wordt deze grens meestal een perimeternetwerk genoemd. Het perimeternetwerk beveiligt het intranet of LAN-netwerk van een bedrijf tegen indringers door de toegang vanaf internet of andere grote netwerken te regelen.

In het volgende diagram wordt een perimeternetwerk weergegeven dat is begrensd door firewalls en dat tussen een privé-netwerk en internet is geplaatst om het privé-netwerk te beschermen:



Eenvoudig perimeternetwerk

Binnen verschillende organisaties wordt er op verschillende manieren gebruikgemaakt van firewalls voor de beveiliging. IP-pakketfiltering vormt een zwakke beveiliging, is lastig te beheren en eenvoudig te omzeilen. Toepassingsgateways zijn veiliger dan pakketfilters en eenvoudiger te beheren, omdat ze maar bij een paar specifieke toepassingen horen, zoals een bepaald e-mailsysteem. Circuitgateways zijn effectiever wanneer de gebruiker van een netwerktoepassing van groter belang is dan de gegevens die worden doorgegeven door die toepassing. De proxyserver is een uitgebreid beveiligingshulpmiddel dat een toepassingsgateway, veilige toegang voor anonieme gebruikers en andere services biedt. Hier volgt wat informatie over deze verschillende opties:

- **IP-pakketfiltering**
  IP-pakketfiltering was de eerste implementatie van firewalltechnologie. Kopteksten van pakketten worden gecontroleerd op bron- en doeladressen, TCP- (Transmission Control Protocol) en UDP-poortnummers (User Datagram Protocol), en andere informatie. Pakketfiltering is een beperkte technologie die het beste werkt in duidelijke beveiligingsomgevingen, waarbij bijvoorbeeld niets van buiten het perimeternetwerk wordt vertrouwd en alles van binnen het netwerk wel. De laatste jaren hebben verschillende leveranciers de pakketfilteringsmethode verbeterd door intelligente beslissingsfuncties aan de pakketfilteringskern toe te voegen. Zo ontstond een nieuwe vorm van pakketfiltering, die *stateful protocol inspection* wordt genoemd. U kunt pakketfiltering zodanig configureren dat specifieke typen pakketten worden geaccepteerd terwijl alle andere worden geweigerd, of dat specifieke typen pakketten worden geweigerd en alle andere worden geaccepteerd.

- **Toepassingsgateways**
  Toepassingsgateways worden gebruikt wanneer de werkelijke inhoud van een toepassing het belangrijkste element is. Dat ze toepassingsspecifiek zijn is zowel een voordeel als een nadeel, omdat ze niet eenvoudig kunnen worden aangepast aan technologische wijzigingen.
- **Circuitgateways**
  Circuitgateways zijn tunnels die zijn aangebracht in een firewall en bepaalde processen of systemen aan de ene kant verbinden met processen of systemen aan de andere kant. Circuitgateways zijn vooral geschikt voor situaties waarbij de persoon die een toepassing gebruikt een groter potentieel risico vormt dan de gegevens die de toepassing bevat. De circuitgateway verschilt van een pakketfilter omdat deze wél verbinding kan maken met een OOB-toepassingsschema (Out-Of-Band), dat extra informatie kan toevoegen.
- **Proxyservers**
  Proxyservers zijn uitgebreide beveiligingshulpmiddelen die een firewall en toepassingsgateway-functionaliteit hebben waarmee het internetverkeer van en naar een LAN-netwerk wordt geregeld. Proxyservers bieden ook functies voor het in het cachegeheugen plaatsen van documenten, en voor toegangsbeheer. Een proxyserver kan tot betere prestaties leiden door veelgevraagde gegevens, bijvoorbeeld een populaire webpagina, in het cachegeheugen te plaatsen zodat deze onmiddellijk beschikbaar zijn. Een proxyserver kan verzoeken ook filteren en ongewenste verzoeken verwijderen, zoals verzoeken voor onbevoegde toegang tot bedrijfsbestanden.

Controleer of de klant gebruikmaakt van de firewallbeveiligingsfuncties die hem kunnen helpen. Plaats een perimeternetwerk in de netwerktopologie op een punt waar al het verkeer van buiten het bedrijfsnetwerk door de grens heen moet die wordt gevormd door de externe firewall. U kunt het toegangsbeheer voor de firewall precies afstemmen op de behoeften van de klant, en u kunt firewalls zodanig configureren dat alle pogingen door onbevoegden tot het verkrijgen van toegang worden gemeld.

Als u het aantal poorten dat u moet openen voor de binnenste firewall wilt minimaliseren, kunt u een toepassingslaagfirewall gebruiken, bijvoorbeeld ISA Server 2000.

Zie voor meer informatie over TCP/IP 'Designing a TCP/IP Network' op http://www.microsoft.com/resources/documentation/WindowsServ/2003/all/deployguide/en-us/dnsbb_tcp_overview.asp.

Draadloze netwerken

Draadloze netwerken worden standaard zodanig geconfigureerd dat afluisteren van de draadloze signalen mogelijk is. De standaardinstellingen van sommige draadloze hardware, de toegankelijkheid die draadloze netwerken bieden en de huidige coderingsmethoden bieden kwaadwillende onbevoegden de mogelijkheid zicht toegang tot het draadloze netwerk te verschaffen. Er zijn configuratieopties en -hulpmiddelen die u kunnen beschermen tegen afluisteren. Hiermee worden computers echter niet beschermd tegen hackers en virussen die binnendringen via de internetverbinding. Het is daarom van zeer groot belang dat er een firewall wordt gebruikt om de computers te beveiligen tegen ongewenste indringers op internet.

Zie voor meer informatie over het beveiligen van een draadloos netwerk 'How to Make Your 802.11b Wireless Home Network More Secure' op http://support.microsoft.com/default.aspx?scid=kb;en-us;309369.

Netwerkbeveiligingsscenario's

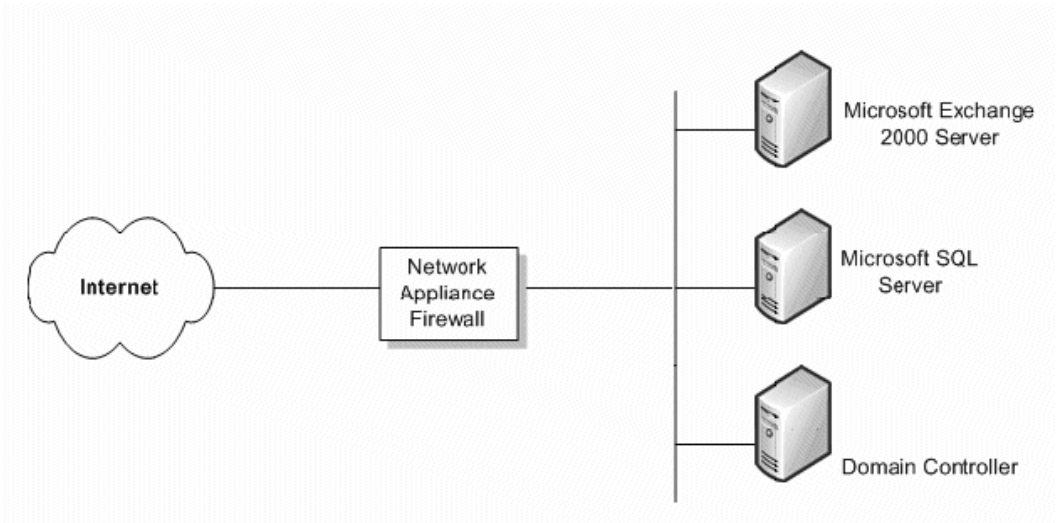
Welk netwerkbeveiligingsniveau vereist is voor de organisatie van een klant, is afhankelijk van verschillende factoren. Meestal wordt er een compromis gesloten tussen budget enerzijds en het gewenste beveiligingsniveau voor bedrijfsgegevens anderzijds. Een klein bedrijf kan een heel complexe beveiligingsstructuur hebben die een optimaal netwerkbeveiligingsniveau biedt, maar waarschijnlijk kan dat kleine bedrijf een dergelijk beveiligingsniveau niet betalen. In dit gedeelte bekijken we vier scenario's en doen we in elk scenario aanbevelingen die een verschillend beveiligingsniveau bieden.

Geen firewall

Als uw klant wel verbinding heeft met internet maar niet over een firewall beschikt, moet er een bepaald netwerkbeveiligingsniveau worden geïmplementeerd. Er zijn eenvoudige netwerkfirewallapparaten die voldoende bescherming bieden om de meeste potentiële hackers af te schrikken.

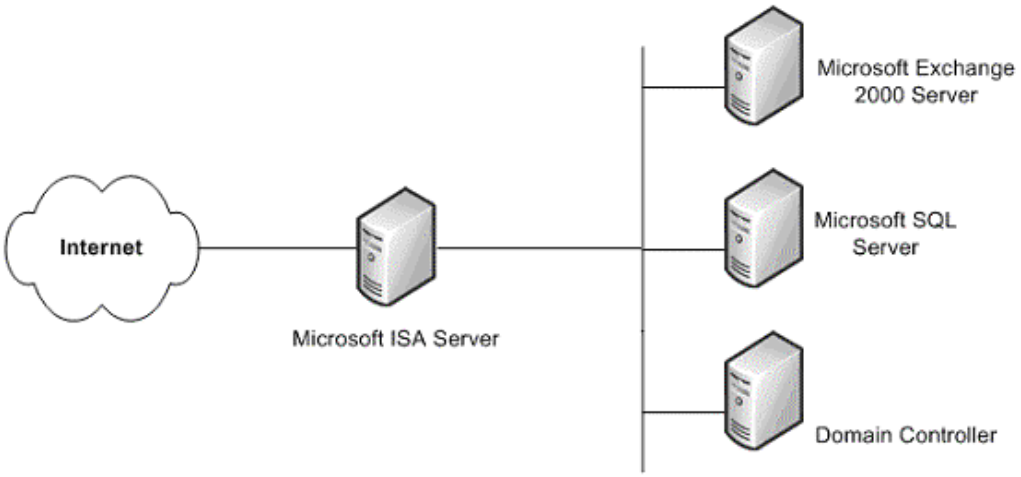
Eén eenvoudige firewall

Het minimaal aanbevolen beveiligingsniveau bestaat uit één firewall tussen internet en de gegevens van uw cliënt. Deze firewall biedt mogelijk geen geavanceerde beveiliging en kan niet als heel veilig worden beschouwd. Het is echter beter dan niks.



Eenvoudige firewall

Hopelijk staat het budget van de klant de aanschaf van een veiligere oplossing toe, die de bedrijfsgegevens beter kan beschermen. Een mogelijke oplossing is ISA Server. Deze aanvullende server, die hogere kosten met zich meebrengt, biedt veel meer zekerheid dan de gemiddelde firewall voor eindgebruikers, omdat deze laatste meestal alleen NAT (netwerkadresvertaling) en pakketfiltering biedt.



ISA Server-firewall

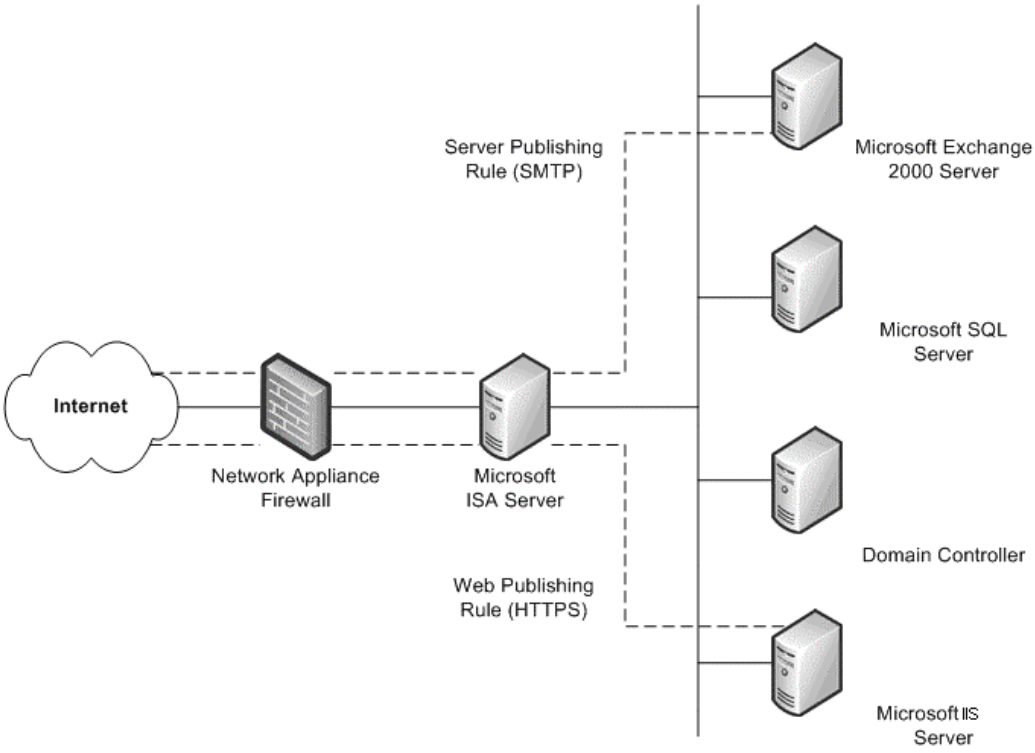
Deze oplossing met één firewall is veiliger dan een firewallapparaat op binnenkomstniveau en biedt Windows-specifieke beveiligingsservices.

Eén bestaande firewall

Als de klant een bestaande firewall heeft die het intranet van internet scheidt, is het verstandig een aanvullende firewall te overwegen die verschillende manieren biedt om interne bronnen te verbinden met internet.

Een mogelijke methode is webpublicatie. Dit is wanneer een ISA Server wordt geïmplementeerd vóór de webserver van een organisatie, die toegang biedt voor internetgebruikers. Als er webverzoeken binnenkomen, kan ISA Server ten opzichte van de buitenwereld als webserver fungeren. Clientverzoeken om webinhoud worden dan vanuit het cachegeheugen van de ISA Server ingewilligd. ISA Server stuurt verzoeken alleen door naar de webserver wanneer de verzoeken niet kunnen worden ingewilligd vanuit het cachegeheugen.

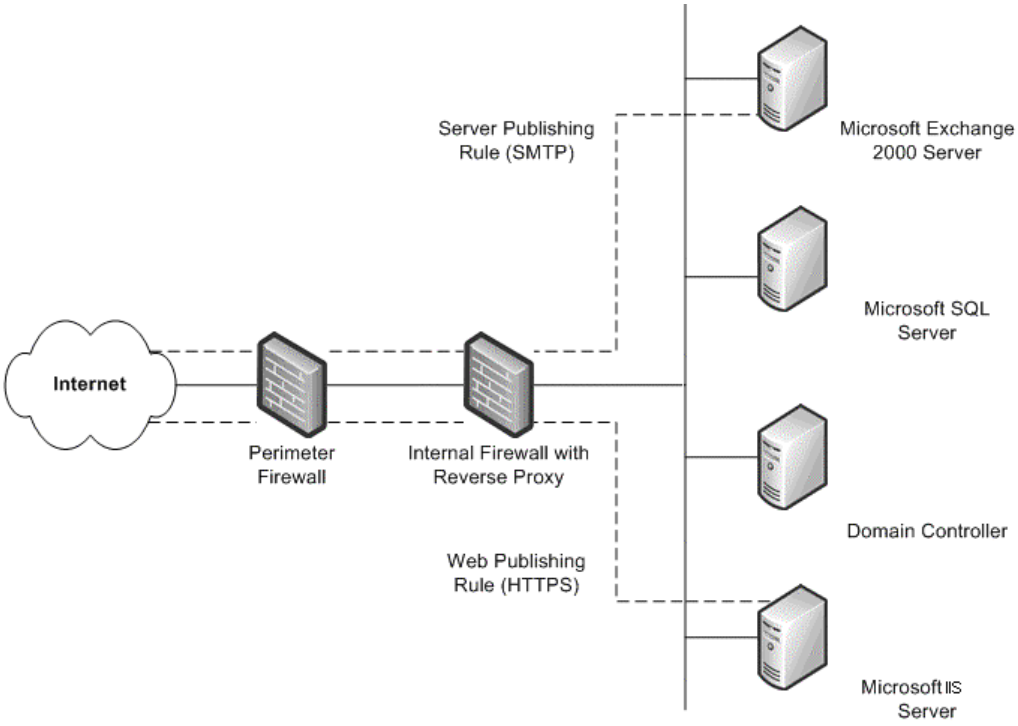
Een andere methode is serverpublicatie. ISA Server staat het publiceren van interne servers op internet toe zonder de beveiliging van het interne netwerk in gevaar te brengen. U kunt webpublicatie- en serverpublicatieregels configureren aan de hand waarvan wordt bepaald welke verzoeken moeten worden verzonden naar een server op het lokale netwerk, zodat er een extra beveiligingslaag wordt toegevoegd voor de interne servers.



Bestaande firewall plus een ISA Server

Twee bestaande firewalls

Bij het vierde scenario gaat het om een organisatie die twee firewalls heeft en een perimeternetwerk (DMZ). Een of meer van deze servers levert omgekeerde proxyservices zodat internetclients niet rechtstreeks toegang krijgen tot het intranet. In plaats hiervan moet een van de firewalls, het liefst de interne firewall, netwerkverzoeken voor interne servers onderscheppen, die pakketten controleren en ze vervolgens doorsturen namens de internethost.



Twee bestaande firewalls

Dit scenario komt ongeveer overeen met het vorige, nadat de tweede firewall is toegevoegd. Het enige verschil is dat de interne firewall die omgekeerde proxy ondersteunt, geen ISA Server is. In dit scenario moet u nauw samenwerken met de beheerders van elke firewall om serverpublicatieregels te definiëren die voldoen aan het beveiligingsbeleid.

Beheer van beveiligingspatches

Besturingssystemen en toepassingen zijn vaak enorm complex. Ze kunnen bestaan uit miljoenen regels code, geschreven door veel verschillende programmeurs. Het is cruciaal dat de software op betrouwbare wijze functioneert en de beveiliging of stabiliteit van de IT-omgeving niet in gevaar brengt. Om problemen te voorkomen worden programma's uitgebreid getest voordat ze worden uitgebracht. Kwaadwillenden zoeken echter continu naar zwakke plekken in software. Het is ondoenlijk om te anticiperen op alle mogelijke toekomstige aanvallen.

Voor veel organisaties is patchbeheer deel van de algemene strategie ten aanzien van het beheer van wijzigingen en configuraties. Het is echter van groot belang om een aparte strategie ten aanzien van patchbeheer te hebben, ongeacht de aard en de omvang van de organisatie, zelfs als er binnen de organisatie nog geen effectief beleid ten aanzien van het beheer van wijzigingen en configuraties van kracht is. Het merendeel van de succesvolle aanvallen op computersystemen vindt plaats op systemen waarop beveiligingspatches niet zijn geïnstalleerd.

Beveiligingspatches zijn voor de meeste organisaties een heikel punt. Zodra er een zwakke plek is ontdekt in software, verspreiden kwaadwillenden de informatie hierover meestal snel in de hackersgemeenschap. Wanneer er een zwakke plek is ontdekt in software van Microsoft, streeft Microsoft ernaar zo snel mogelijk een beveiligingspatch uit te brengen. Totdat de patch is geïmplementeerd, is het beveiligingsniveau waarop de klant vertrouwt en dat deze verwacht mogelijk aanzienlijk lager.

In de Navision-omgeving moet u controleren of uw klanten de meest recente beveiligingspatches op het hele systeem hebben geïnstalleerd. Controleer of de klant de technologieën gebruikt die Microsoft beschikbaar heeft gesteld. Hiertoe behoren:

- **Microsoft Security Notification Service**
  Dit is een e-maillijst die meldingen verzendt zodra er een update beschikbaar wordt gesteld. Deze meldingen dragen in belangrijke mate bij aan een proactieve beveiligingsstrategie. Ze zijn ook beschikbaar via de TechNet Product Security Notification-website: http://www.microsoft.com/technet/security/bulletin/notify.mspx.
- **Automatische updates van Microsoft**
  Windows kan automatisch beveiligingsupdates toepassen op uw computers.
- **Zoekprogramma voor Microsoft-beveiligingsbulletins**
  Het zoekprogramma voor beveiligingsbulletins is beschikbaar via de Security Bulletin Service-website: http://www.microsoft.com/technet/security/current.aspx. De klant kan bepalen welke updates nodig zijn op basis van het besturingssysteem, de toepassingen en de service packs die op dat moment zijn geïnstalleerd.
- **Microsoft Baseline Security Analyzer (MBSA)**
  Dit grafische hulpprogramma is beschikbaar via de Microsoft Baseline Security Analyzer-website: http://www.microsoft.com/technet/security/tools/mbsahome.mspx. Het hulpprogramma vergelijkt de huidige status van een computer met een lijst van updates die wordt onderhouden door Microsoft. MBSA voert ook een aantal basisbeveiligingscontroles uit met betrekking tot wachtwoordsterkte- en verloopinstellingen, gastaccountbeleid en een aantal andere zaken. MBSA zoekt ook naar zwakke plekken in Microsoft Internet Information Services (IIS), SQL Server™ 2000, Exchange 5.5, Exchange 2000 en Exchange Server 2003.
- **Microsoft Software Update Services (SUS)**
  Met dit hulpprogramma (voorheen Windows Update Corporate Edition) kunnen bedrijven lokale computers als host laten fungeren voor alle kritieke updates en SRP's (beveiligingssamenvoegingspakketten) die beschikbaar zijn via de openbare Windows Update-site. Samen met een nieuwe versie van AU-clients (automatische update) vormt dit hulpprogramma de basis voor een krachtige, automatische download- en installatiestrategie. De nieuwe AU-client bevat een client voor de besturingssystemen Windows 2000 en Windows Server 2003 en heeft de mogelijkheid gedownloade updates automatisch te installeren. Zie voor meer informatie over Microsoft SUS http://www.microsoft.com/windows2000/windowsupdate/sus/default.asp.
- **Microsoft Systems Management Server (SMS) Software Update Services Feature Pack**
  Dit pakket bevat een aantal hulpmiddelen die bedoeld zijn om het distributieproces voor software-updates over de hele onderneming te vereenvoudigen. Tot deze hulpmiddelen behoren: Security Update Inventory Tool, Microsoft Office Inventory Tool for Updates, Distribute Software Updates Wizard en SMS Web Reporting Tool with Web Reports Add-in for Software Updates. Zie voor meer informatie over de afzonderlijke hulpmiddelen http://www.microsoft.com/smserver/downloads/20/featurepacks/suspack/.

Bespreek al deze hulpmiddelen met uw klanten en raad ze aan deze te gebruiken. Het is van groot belang dat beveiligingsproblemen zo snel mogelijk worden opgelost zonder de stabiliteit van de omgeving in gevaar te brengen.

SQL Server 2000-beveiligingsinstellingen

Aangezien Navision ook kan worden uitgevoerd onder SQL Server 2000, is het van belang dat u maatregelen neemt om de beveiliging van de SQL Server 2000-installatie van de klant te verbeteren. Met de volgende stappen kunt u de SQL Server-beveiliging verbeteren:

- Controleer of de meest recente service packs en updates voor het besturingssysteem en SQL Server 2000 zijn geïnstalleerd. Voor het laatste nieuws gaat u naar de Microsoft Security-website http://www.microsoft.com/security/default.asp.
- Voor de beveiliging op bestandssysteemniveau controleert u of alle SQL Server 2000-gegevens en -systeembestanden zijn geïnstalleerd op NTFS-partities. U moet de bestanden alleen beschikbaar maken voor beheerders of systeemniveaugebruikers via NTFS-machtigingen. Zo bent u beschermd tegen gebruikers die toegang tot die bestanden proberen te krijgen wanneer de MSSQLSERVER-service niet actief is.
- Gebruik een domeinaccount waarvoor weinig rechten nodig zijn, zoals NT Authoriteit\Netwerkservice of de account Lokaal systeem (aanbevolen) voor SQL Server 2000-service (MSSQLSERVER). Deze account hoort minimale rechten te hebben in het domein en moet helpen de schade te beperken (maar niet te voorkomen) in geval van een aanval op de server. Met andere woorden: deze account mag alleen machtigingen voor lokale gebruikers hebben in het domein. Als SQL Server 2000 een domeinbeheerdersaccount gebruikt om de services uit te voeren, leidt een inbraak op de server tot gevaar voor het volledige domein. U kunt deze instellingen wijzigen via SQL Server Enterprise Manager. De ACL's (toegangsbeheerlijsten) voor bestanden, het register en gebruikersrechten worden automatisch gewijzigd.
- De meeste edities van SQL Server 2000 worden geïnstalleerd met twee standaarddatabases: **Noordenwind** en **pubs**. Beide databases zijn voorbeelddatabases die worden gebruikt voor tests, trainingen en algemene voorbeelden. Ze moeten niet worden geïmplementeerd in een productiesysteem. Als een kwaadwillende weet dat deze databases aanwezig zijn, kan hij/zij proberen misbruik te maken van de bijbehorende standaardinstellingen en -configuratie. Als **Noordenwind** en **pubs** aanwezig zijn op de SQL Server 2000-productiecomputer, moeten ze worden verwijderd.
- De functie voor het controleren van het SQL Server 2000-systeem is standaard uitgeschakeld, zodat er geen voorwaarden worden gecontroleerd. Deze functie bemoeilijkt de opsporing van indringers en helpt kwaadwillenden bij het wissen van hun sporen. U moet minimaal de functie voor het controleren van mislukte aanmeldingen inschakelen.

Voor de meest recente informatie over SQL Server 2000-beveiliging gaat u naar http://www.microsoft.com/sql/techinfo/administration/2000/security/default.asp.

Over Microsoft Business Solutions

Microsoft Business Solutions, een divisie van Microsoft, biedt een breed scala geïntegreerde, end-to-end-bedrijfstoepassingen en -services die zijn ontworpen om de communicatie te verbeteren van kleine, middelgrote en grote bedrijven met klanten, werknemers, partners en leveranciers. Met de toepassingen van Microsoft Business Solutions kunt u de strategische bedrijfsprocessen optimaliseren op het gebied van financieel management, analyse, personeelsbeheer, projectmanagement, CRM, veldservicemanagement, Supply Chain Management, e-commerce en productie- en detailhandelmanagement. De toepassingen zijn ontworpen om klanten inzicht te bieden en met succes zaken te kunnen doen. Meer informatie over Microsoft Business Solutions vindt u op http://www.microsoft.com/BusinessSolutions/

Dit is een voorlopig document dat aanzienlijk kan worden gewijzigd voordat de software die in dit document wordt beschreven, daadwerkelijk wordt uitgebracht.

De informatie in dit document vertegenwoordigt de huidige visie van Microsoft Corporation op de besproken kwesties vanaf de publicatiedatum. Aangezien Microsoft moet reageren op veranderende marktomstandigheden, mag deze informatie niet worden beschouwd als een belofte van Microsoft en kan Microsoft de juistheid niet garanderen van informatie die na de publicatiedatum wordt gepresenteerd.

Dit document is alleen bedoeld ter informatie. MICROSOFT GEEFT GEEN EXPLICIETE OF IMPLICIETE GARANTIES IN DIT DOCUMENT.

Het is de verantwoordelijkheid van de gebruiker te voldoen aan alle toepasselijke auteursrechten. Zonder de rechten onder het auteursrecht te beperken, mag niets uit dit document worden gereproduceerd, opgeslagen of opgenomen in een ophaalsysteem, of in enigerlei vorm of op enigerlei wijze worden verzonden (elektronisch, mechanisch, via fotokopieën, opname of anderszins), of voor enigerlei doel, zonder de uitdrukkelijke, schriftelijke toestemming van Microsoft Corporation.

Microsoft beschikt mogelijk over patenten, aanvragen voor patenten, merken, auteursrechten of andere intellectuele eigendomsrechten met betrekking tot de materie in dit document. Tenzij uitdrukkelijk vermeld in een schriftelijke licentieovereenkomst van Microsoft, geeft dit document u geen licentie voor deze patenten, merken, auteursrechten of andere intellectuele eigendomsrechten.

© 2003 Microsoft Business Solutions ApS, Denemarken. Alle rechten voorbehouden.

Microsoft, Great Plains, Navision zijn gedeponeerde merken of merken van Microsoft Corporation, Great Plains Software, Inc of Microsoft Business Solutions ApS of hun dochterbedrijven. Great Plains Software, Inc. en Microsoft Business Solutions ApS zijn dochterbedrijven van Microsoft Corporation. De namen van bestaande bedrijven en producten die in dit document worden genoemd, kunnen de merken zijn van hun respectieve eigenaren. De voorbeeldbedrijven, -organisaties, -producten, -domeinnamen, -e-mailadressen, -logo´s, -personen en -gebeurtenissen in dit document zijn fictief. Elke overeenkomst met echte bedrijven, organisaties, producten, domeinnamen, e-mailadressen, logo's, personen of gebeurtenissen berust op louter toeval.