Microsoft Business Solutions

Navision Security Hardening Guide

Birt: Október 2004

Microsoft

Efnisyfirlit

Kynning

Með Microsoft® Windows® fylgir háþróað netöryggi sem byggt er á stöðlum. Í grófum dráttum snúast öryggismál um skipulagningu og málamiðlanir. Til dæmis er hægt að læsa tölvu inni í öryggishvelfingu og veita aðeins einum kerfisstjóra aðgang að henni. Þessi tölva kann að vera örugg en hún er ekki mjög gagnleg þar sem hún er ekki tengd við aðrar tölvur. Finna þarf leið til þess að netið sé eins öruggt og hægt er án þess að fórna notkunarmöguleikum.

Flest fyrirtæki gera ráð fyrir utanaðkomandi árásum og setja upp eldveggi en mörg fyrirtæki gera ekki ráðstafanir til að bregðast við öryggisrofi þegar meinfýsinn notandi kemst inn fyrir eldvegginn. Öryggisráðstafanir í umhverfi viðskiptavinarins skila árangri ef notendur þurfa ekki að ljúka of mörgum ferlum og þrepum til að stunda viðskipti með öruggum hætti. Innleiðing öryggisreglna ætti að vera eins auðveld og hægt er fyrir notendur, annars finna þeir óöruggari leiðir til að vinna.

Þar sem stærð Navision-uppsetninga getur verið mjög mismunandi er mikilvægt að fara vandlega yfir þarfir einstakra viðskiptavina og vega virkni öryggisráðstafana á móti kostnaðinum sem kann að felast í þeim. Sem traustur ráðgjafi viðskiptavinarins skaltu nota þína bestu dómgreind og mæla með reglum sem uppfylla öryggisþarfir þeirra án þess að íþyngja þeim svo að viðskiptavinurinn hætti að lokum að fylgja reglunum.

Bestu venjur um öryggi Navision

Eftirfarandi almennar reglur geta aukið öryggi Navision-umhverfisins:

- Ef keyra á Navision Database Server sem þjónustu eða nota skipanalínufæribreytuna *installasservice* þegar þjónninn er ræstur skal tryggja að þjónustan keyri sem reikningurinn NT Authority\Network Service. Reikningurinn NT Authority\Network Service er aðeins til í Windows™ XP og Windows Server™ 2003. Ef Windows 2000 Server er keyrður skal stofna reikning með minnstu heimildum fyrir þjónustuna því annars fær þjónustan Local System reikning. Þessi reikningur ætti í mesta lagi að hafa sömu heimildir og reikningur fyrir venjulega notendur eða vera lénsreikningur sem er ekki kerfisstjóri í léninu eða á nokkurri staðbundinni tölvu.

  Það þarf að muna að gefa reikningnum NT Authority\Network Service eða notandareikningnum sem þjónninn keyrir undir les- og skrifaðgang að gagnagrunnskránum til að tryggja að notendur geti tengst gagnagrunninum.

  Reikningnum NT Authority\Network Service gefinn les- og skrifaðgangur að gagnagrunnskrá í Windows XP:

  1. Í Windows Explorer er flett að möppunni þar sem gagnagrunnsskráin er geymd.
  2. Hægrismellt er á gagnagrunnsskrána og smellt á Properties.
  3. Í glugganum ***Properties*** er hægrismellt á flipann ***Security*** og undir reitnum **Group and user names** er smellt á Add.
  4. Í glugganum ***Select Users, Computers, or Groups*** er ritað *Network Service* og smellt á OK.
  5. NETWORK SERVICE hefur verið bætt við reitinn **Group and user names** í glugganum ***Properties***.
  6. NETWORK SERVICE er valið og í reitnum **Permissions** eru lestrar- og skrifheimildir gefnar.
- Þjónustan Navision Application Server keyrir sjálfgefið sem reikningurinn NT Authority\Network Service og það gerir henni kleift að fá staðbundinn aðgang að Navision Database Server. Á neti þarf hins vegar að tryggja að þjónustan Navision Application Server keyri sem lénsreikningur í Windows sem þekkist í Navision Database Server ef hún á að hafa aðgang að gagnagrunnsþjóni. Þessi reikningur ætti ekki að vera kerfisstjóri í léninu eða á neinni staðbundinni tölvu.
- Ef SQL Server Option fyrir Navision er keyrt er Microsoft SQL Server™ keyrt sem þjónusta. SQL Server Option fyrir Navision krefst þess að SQL Server geti flett upp í Active Directory til að fá lista yfir notendahópa í Windows vegna sannvottunar. Því þarf að tryggja að þjónustan SQL Server keyri sem reikningurinn NT Authority\Network Service.

  Til að tryggja að þjónustan keyri sem NT Authority\Network Service:

  1. Í tölvunni með SQL Server er þjónustan MSSQLSERVER fundin, hægrismellt á hana og smellt á Properties.
  2. Í glugganum ***Properties*** er smellt á flipann ***Log On***.
  3. Á flipanum ***Log On***, undir Log on as er smellt á This Account og ritað *NT Authority\NetworkService* og smellt á OK.

  Nánari upplýsingar um öryggi SQL Server eru á:

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

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

- Ef Navision netverslunarvara eins og Commerce Gateway er keyrð skal tryggja að Commerce Gateway Request Server hafi verið rétt upp settur með sjálfgefnum reikningsstillingum fyrir þjónusturnar. Sjálfgefna reikningsstillingin kallast *CGRSUser* og veitir Commerce Gateway Server aðgang að lágmarkssafni annara þjónusta sem hann þarfnast, þar á meðal *MSSQLSERVER* og *BizTalk Service BizTalk Group : BizTalkServerApplication* og inniheldur engar altækar reikningsstillingar eins og reikningurinn *Local System*.
- Alltaf skal nota traust aðgangsorð. Nánari upplýsingar um traust aðgangsorð eru í kaflanum Traust aðgangsorð.
- Nota skal innskráningu í Windows. Í Navision er hægt að stofna tvenns konar innskráningar – Innskráningar í gagnagrunn og Innskráningar í Windows. Við mælum með því að innskráningar í Windows séu notaðar því þær nota Windows-sannvottun og gera kleift að koma á viðeigandi stefnu um aðgangsorð.
- Ekki skal endurnýta aðgangsorð. Oft eru sömu aðgangsorðin notuð í mismunandi kerfum og lénum. Til dæmis gæti kerfisstjóri sem sér um tvö lén stofnað lénsstjórareikninga í hvoru léni með sama aðgangsorði og jafnvel valið aðgangsorð kerfisstjóra á staðbundnum vélum sem er eins í öllu léninu. Í þessi tilviki gæti allt lénið verið í hættu ef óheimill aðgangur fæst að einum reikningi eða tölvu.
- Þegar Navision hefur verið sett upp og gagnagrunnarnir stofnaðir eða uppfærðir skal stofna innskráningu í Windows og úthluta henni SUPER-hlutverkið í Navision. Þessi SUPER-notandi sér um gagnagrunnsstjórnun, öryggi og þess háttar. Gefa skal þessari innskráningu traust aðgangsorð. Þessu aðgangsorði skal halda leyndu. Það ætti að njóta sömu verndar og SA-aðgangsorðið í SQL Server. Öllum gagnagrunnsaðgangi er stjórnað af SUPER-hlutverkinu og það krefst hámarksverndar. Eingöngu kerfisstjórar ættu að vita aðgangsorð SUPER-notandans.
- Allir aðrir notendur með aðgang að Navision-gagnagrunninum ættu að hafa lágmarksheimildir. Það felur í sér að úthluta þeim hlutverkum í Navision sem veita þeim aðeins aðgang að þeim aðgerðum og virkni sem eru nauðsynleg fyrir vinnu þeirra hjá fyrirtækinu.
- Tryggja skal að aðeins þeir notendur sem þess þurfa vegna hlutverka sinna innan fyrirtækisins geti flutt inn FOB-skrár, endurhannað hluti auk þess að stofna og endurheimta öryggisafrit af gagnagrunnum.
- Taka skal regluleg öryggisafrit af Navision-gagnagrunninum og muna að prófa öryggisafritin til að tryggja að hægt sé að endurheimta þau.
- Geyma skal öryggisafritin á öruggum stað til að takmarka áhrif af hættum eins og eldi, reyk, ryki, miklum hita, eldingum og náttúruhamförum (til dæmis, jarðskjálfta).
- Þó að hægt sé að keyra Navision með nokkrum útgáfum af Windows, mælum við með því að notuð séu nýjustu stýrikerfin með nýjustu öryggiseiginleikum. Eins og er eru það Windows XP, Service Pack 2 og Windows Server 2003.
- Nota skal Windows Update þjónustuna sem fylgir Windows 2000, Windows XP og Windows Server 2003 til að beita nýjustu öryggisuppfærslunum. Nota skal sjálfvirkar uppfærslur í Windows til að halda öllum biðlaratölvum nýuppfærðum með nýjustu öryggislagfæringum, þjónustupökkum og uppfærslum.
- Við mælum með því að öruggu samskiptareglurnar TCPS séu notaðar fyrir samskipti á milli Navision-biðlaranna og Navision Database Server. TCPS er örugg útgáfa af TCP/IP og notar SSPI (Security Support Provider Interface) virkri dulritun og Kerberos-sannvottun. TCPS er sjálfgefin samskiptaregla fyrir Navision Database Server.

- Viðskiptavinurinn ætti að hafa viðbragðsáætlun sem tryggir að starfsemin geti hafist fljótt aftur eftir hörmungar. Viðbragðsáætlunin ætti að innihalda atriði eins og:
    - Öflun nýs/bráðabirgðabúnaðar.
    - Endurheimt öryggisafrita í ný kerfi.
    - Prófun á því hvort viðbragðsáætlunin gangi.

Efnislegt öryggi

Efnislegt öryggi er bráðnauðsynlegt þar sem engin leið er að bæta það upp með hugbúnaðaröryggi. Til dæmis, ef hörðum diski er stolið verður gögnunum á þeim diski að endingu einnig stolið. Ræða skal eftirfarandi efnisleg öryggisatriði þegar reglur eru þróaðar í samvinnu við viðskiptavin:

- Fyrir stórar uppsetningar hjá sérstökum upplýsingatæknideildum skal tryggja að netþjónaherbergi og staðir þar sem hugbúnaður er geymdur séu læstir.
- Tölvur í þessum flokki eru:
    - Netþjónninn með Microsoft SQL Server 2000
    - Skráaþjónninn þar sem keyrsluskrár Navision eru geymdar.
- Halda skal óviðkomandi notendum frá tölvunum.
- Tryggja skal að þjófavarnir séu settar upp, óháð því hversu viðkvæm gögnin eru.
- Tryggja skal að öryggisafrit af mikilvægum gögnum séu geymd utan vinnustaðarins og að öryggisafritin séu geymd í eldtraustum ílátum.

Starfsmenn

Það er góð hugmynd að takmarka stjórnunarheimildir að öllum vörum og aðgerðum. Sjálfgefið ætti að vera að viðskiptavinir veiti starfsmönnum sínum aðeins lesaðgang að kerfisaðgerðum nema þeir þurfi aukinn aðgang til að sinna starfi sínu. Microsoft leggur til að stefnu um lágmarksheimildir sé fylgt: veita skal notendum lágmarksheimildir sem nauðsynlegar eru til að fá aðgang að gögnum og virkni.
Óánægðir og fyrrum starfsmenn eru ógn við netöryggi. Þegar öryggismál eru rædd við viðskiptavini skal leggja til eftirfarandi stefnu varðandi starfsmenn:

- Rannsaka skal bakgrunn starfsmanns fyrir ráðningu.
- Búast skal við "hefnd" frá óánægðum starfsmönnum og fyrrum starfsmönnum.
- Ganga skal úr skugga um að allir tengdir Windows-reikningar og aðgangsorð séu gerð óvirk þegar starfsmaður hættir. Vegna skýrslugerðar skal ekki eyða notendum. Ekki skal endurnýta reikningana.
- Kenna skal notendum árvekni og að tilkynna grunsamlegar aðgerðir.
- Ekki skal veita heimildir sjálfkrafa. Ef notendur þurfa ekki aðgang að tilteknum tölvum, tölvuverum eða skráasöfnum skal tryggja að þeir hafi ekki aðgang.
- Kenna skal stjórnendum að koma auga á og bregðast við hugsanlegum starfsmannavandamálum.
- Ganga skal úr skugga um að starfsmenn skilji hlutverk sitt við að viðhalda netöryggi.
- Láta skal alla starfsmenn hafa afrit af reglum fyrirtækisins.
- Ekki skal heimila notendum að setja upp hugbúnað sem fyrirtækið gefur ekki leyfir fyrir.

Kerfisstjórinn

Við mælum með því að kerfisstjórar viðskiptavinanna haldi í við nýjustu öryggislagfæringar Microsoft. Árásaraðilar eru mjög snjallir við að sameina litla galla til að gera stórar árásir á netkerfi mögulegar. Kerfisstjórar ættu fyrst að ganga úr skugga um að einstakar tölvur séu eins öruggar og hægt er og bæta síðan við öryggisuppfærslum og nota vírusvarnarhugbúnað. Margir tenglar og úrræði eru sett fram í þessum leiðbeiningum til að auðvelda lesendum að finna dýrmætar upplýsingar og bestu venjur.

Flækjustig kallar á aðra málamiðlun í öryggi netsins. Því flóknara sem netið er, því erfiðara er að tryggja það eða laga þegar árásaraðili hefur fengið aðgang að því. Kerfisstjórinn ætti að skrá svæðislýsingu netsins ítarlega með það að markmiði að halda því eins einföldu og hægt er.

Öryggi snýst aðallega um áhættustýringu. Þar sem tæknin er ekki allra meina bót krefst öryggi samblands af tækni og reglum. Með öðrum orðum, það verður aldrei til vara sem hægt er að taka úr pakkanum og setja upp á netinu sem kemur strax á fullkomnu öryggi. Öryggi leiðir bæði af tækni og reglum — þ.e., það hvernig tæknin er notuð ákvarðar að lokum öryggisstig netsins. Microsoft sendir frá sér tækni og aðgerðir sem taka mið af öryggi en aðeins kerfisstjórinn, með þinni hjálp, getur ákveðið réttar reglur fyrir hvert fyrirtæki. Gera skal öryggisáætlanir snemma í innleiðingarferlinu. Kynnið ykkur hvað viðskiptavinurinn vill vernda og hvað hann er tilbúinn að gera til þess.

Loks skal þróa viðbragðsáætlanir vegna neyðartilfella áður en þau koma upp. Sameinið ítarlega skipulagningu og trausta tækni svo viðskiptavinurinn njóti mikils öryggis.

Nánari upplýsingar um öryggi almennt, sjá "The Ten Immutable Laws of Security Administration," á:
http://www.microsoft.com/technet/archive/community/columns/security/essays/10salaws.mspx.

og greinar um öryggisstjórnun á:
http://www.microsoft.com/technet/community/columns/secmgmt/smarch.mspx

Stýrikerfi netþjónsins tryggt

Þó að margir minni viðskiptavinir hafi ekki netþjónsstýrikerfi er mikilvægt að skilja og geta miðlað bestu öryggisvenjum til stærri viðskiptavina með flóknari netumhverfi. Einnig skal hafa í huga að auðvelt er að nota margar af þeim reglum og venjum sem lýst er í þessu skjali hjá þeim viðskiptavinum sem hafa aðeins biðlarastýrikerfi.

Hugtökin í þessum kafla eiga bæði við um Microsoft Windows 2000 Server og Microsoft Windows Server 2003 þó að þessar upplýsingar hafi aðallega verið fengnar úr hjálpinni með Windows Server 2003. Windows Server 2003 hefur öflugt safn öryggisaðgerða. Hjálpin með Windows Server 2003 inniheldur upplýsingar um allar öryggisaðgerðir og -ferla.

Meiri upplýsingar um Windows 2000 Server fást með því að skoða öryggismiðstöð Windows 2000 á slóðinni
http://www.microsoft.com/technet/security/prodtech/win2000/default.mspx.

og lesa “Windows 2000 Security Hardening Guide” á:
http://www.microsoft.com/technet/security/prodtech/win2000/win2khg/default.mspx

Meiri upplýsingar um Windows Server 2003 fást með því að skoða *Windows Server 2003 Security Guide* á slóðinni
http://www.microsoft.com/technet/security/prodtech/win2003/w2003hg/sgch00.mspx

Helstu aðgerðir í öryggiskerfi Windows netþjóna eru sannvottun, aðgangsstýring og ein innskráning:

- Sannvottun er ferlið í kerfinu þar sem kenni notanda er sannvottað með innskráningarupplýsingum þeirra. Notandanafn og aðgangsorð eru borin saman við samþykktan lista. Ef kerfið finnur samsvörun veitir sannvottun notandanum þann aðgang sem tilgreindur er fyrir notandann á heimildalistanum.
- Aðgangsstýring takmarkar aðgang notanda að upplýsingum eða tölvubúnaði á grundvelli notandakennis og Kerfisstjórar nota vanalega aðgangsstýringu til að stjórna aðgangi sem notendur hafa að tilföngum á neti eins og netþjónum, skráasöfnum og skrám. Þetta er vanalega framkvæmt með því að veita notendum og hópum heimildir til að nota tiltekna hluti.
- Ein innskráning gerir notanda kleift að skrá sig einu sinni inn á Windows-lénið, með einu aðgangsorði, og vera sannvottaður í hvaða tölvu sem er í Windows-léninu. Ein innskráning gerir kerfisstjórum kleift að innleiða sannvottun aðgangsorða í öllu Windows-netinu og veita notendum auðveldan aðgang um leið.

Í köflunum hér á eftir eru nánari lýsingar á þessum þrem lykilaðgerðum.

Sannvottun

Sannvottun er grundvallaratriði í öryggi kerfisins og er notuð til að staðfesta auðkenni notenda sem reyna að skrá sig inn á lén eða fá aðgang að tilföngum á neti. Veiki hlekkurinn í flestum sannvottunarkerfum er aðgangsorð notandans.

Aðgangsorð eru fyrsta varnarlínan gegn óheimilum aðgangi að léninu og staðbundnum tölvum. Mælið með eftirfarandi bestu venjum:

- Alltaf skal nota traust aðgangsorð.
- Ef nauðsynlegt er að skrifa aðgangsorð á blað skal geyma blaðið á öruggum stað og eyða því þegar þess er ekki lengur þörf.
- Aldrei skal deila aðgangsorðum með neinum.
- Nota skal mismunandi aðgangsorð fyrir alla notendareikninga.
- Breyta skal aðgangsorðum með reglulegu millibili.
- Hafa skal gætur á því hvar aðgangsorð eru vistuð í tölvum.

Traust aðgangsorð

Hlutverk aðgangsorða í því að treysta netkerfi fyrirtækja er oft vanmetið og vill gleymast. Eins og áður var nefnt eru aðgangsorð fyrsta varnarlínan gegn óheimilum aðgangi að netinu. Því skal tryggja að viðskiptavinirnir beini því til starfsmanna að nota traust lykilorð.

Verkfæri til að grufla upp aðgangsorð verða hins vegar stöðugt betri og tölvurnar sem notaðar eru til að grufla upp aðgangsorð eru öflugri en nokkru sinni fyrr. Á nógu löngum tíma nær sjálfvirka verkfærið að grufla upp hvaða aðgangsorð sem er. Engu að síður er mun erfiðara að grufla upp traust lykilorð en ótraust.

Leiðbeiningar um hvernig hægt er að búa til traust lykilorð sem notandinn getur munað eru á

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

og

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

Aðgangsorðareglur skilgreindar

Þegar viðskiptavininum er hjálpað að skilgreina reglur um aðgangsorð skal tryggja að búin sé til regla sem krefst þess að allir notendareikningar hafi traust aðgangsorð. Í flestum kerfum er nægilegt að fylgja ráðlegginum í Windows Server 2003 Security Guide:

- Skilgreina skal reglustillinguna **Enforce password history** þannig að nokkur eldri aðgangsorð séu geymd. Með þessari reglustillingu geta notendur ekki notað sama aðgangsorðið þegar aðgangsorðið rennur út.

  Ráðlögð stilling: 24

- Skilgreina skal reglustillinguna **Maximum password age** þannig að aðgangsorð renni út eins oft og nauðsynlegt er í umhverfi viðskiptavinarins.

  Ráðlögð stilling: á milli 42 (sjálfgildið) og 90.

- Skilgreina skal reglustillinguna **Minimum password age** þannig að ekki sé hægt að breyta aðgangsorðum fyrr en þau eru orðin ákveðið margra daga gömul. Þessi reglustilling vinnur með reglustillingunni **Enforce password history**. Ef lágmarksaldur aðgangsorða er skilgreindur geta notendur ekki ítrekað breytt aðgangsorðum sínum til að komast hjá reglustillingunni **Enforce password history** og nota síðan upphaflegu aðgangsorðin sín. Notendur verða bíða í tiltekinn dagafjölda til að breyta aðgangsorðum sínum.

  Ráðlögð stilling: 2.

- Skilgreina skal reglustillinguna **Minimum password length** þannig að aðgangsorð verði að innihalda minnst tiltekinn fjölda staftákna. Löng aðgangsorð, sjö stafir eða fleiri, eru yfirleitt traustari en stutt. Með þessari reglustillingu geta notendur ekki notað auð aðgangsorð og þeir verða að búa til aðgangsorð sem hafa lágmarksfjölda staftákna.

  Ráðlögð stilling: 8.

- Virkja skal reglustillinguna **Password must meet complexity requirements**. Þessi reglustilling kannar öll ný aðgangsorð til að tryggja að þau uppfylli grunnkröfur um traust aðgangsorð. Þessi stilling tryggir að aðgangsorð hafi minnst þrjú tákn úr flokkunum fjórum (hástafir, lágstafir, tölustafir, tákn sem ekki eru bókstafir eða tölustafir), og að það innihaldi ekki hluta af notandanafninu og fornafni eða eftirnafni notandans.

  Til athugunar
  Aðgangsorð sem uppfylla þessar kröfur eru ekki endilega mjög traust. Til dæmis uppfyllir aðgangsorðið “Aðgangsorð1” þessar kröfur.

  Ráðlögð stilling: Yes

- Ítarlegur listi yfir þessar kröfur eru í kaflanum "Password Must Meet Complexity Requirements" í hjálpinni með Windows Server.
- Store passwords using reversible encryption (tvíátta dulritun) – Tvíátta dulritun er notuð í kerfum þar sem forrit þarf aðgang að aðgangsorðum í hreinum texta. Hún er ekki nauðsynleg í flestum innleiðingum.

  Ráðlögð stilling: No.

Nánari upplýsingar eru í Windows Server 2003 Security Guide:

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

Regla um læsingu reikninga skilgreind

Farið varlega þegar reglur um læsingu reikninga eru skilgreindar. Aldrei skyldi setja reglu um læsingu reiknings í litlu fyrirtæki þar sem hún er líka mjög líkleg til að læsa úti notendur með heimild og það getur verið mjög kostnaðarsamt fyrir viðskiptavininn.

Ef viðskiptavinurinn ákveður að nota reglu um læsingu reiknings skal stilla **Account lockout threshold policy** á nógu háa tölu til þess að notendur með heimild séu ekki læstir út úr notendareikningunum sínum vegna þess að þeir skrifi aðgangsorðið sitt nokkrum sinnum vitlaust.

Nánari upplýsingar um reglur um læsingu reikninga eru í kaflanum "Account Lockout Policy Overview" í hjálpinni með Windows Server.

Upplýsingar um hvernig eigi að beita eða breyta reglum um læsingu reikninga eru í kaflanum "To Apply or Modify Account Lockout Policy" í hjálpinni með Windows Server.

Aðgangsstýring

Hægt er að tryggja Windows-net og tilföng þess (þar á meðal Navision) með því að íhuga hvaða réttindi notendur, hópar notenda og aðrar tölvur hafa á netinu. Hægt er að tryggja tölvu eða margar tölvur með því að veita notendum eða hópum tilteknar notendaheimildir. Hægt er að tryggja hlut, eins og skrá eða möppu, með því að úthluta heimildum sem leyfa notendum eða hópum að framkvæma tilteknar aðgerðir á hlutnum. Lykilhugtök í aðgangsstýringu eru meðal annars:

- Heimildir
- Eign hluta

- Erfðir heimilda
- Notendaheimildir
- Endurskoðun hluta

Heimildir

Heimildir skilgreina þá tegund aðgangs sem veitt er notanda eða hópi að hlut eða hlutareiginleika eins og skrám, möppum og stýriskrárhlutum. Heimildum er beitt á alla tryggða hluti eins og skrár eða stýriskrárhluti. Hægt er að veita öllum notendum, hópum eða tölvum heimildir. Það er góð venja að úthluta heimildum til hópa.

Eign hluta

Eiganda er úthlutað á hlut þegar hluturinn er búinn til. Sjálfgefið er í Windows 2000 Server að eigandinn sé sá sem býr til hlutinn. Þessu hefur verið breytt í Windows Server 2003 fyrir hluti sem búnir eru til af meðlimum í hópnum Administrators.

Þegar meðlimur í hópnum Administrators býr til hlut í Windows Server 2003, verður hópurinn Administrators eigandinn en ekki einstaklingurinn sem bjó til hlutinn. Hægt er að breyta þessari hegðun í Local Security Settings Microsoft Management Console (MMC) með stillingunni **System objects: Default owner for objects created by members of the Administrators group**. Sama hvaða heimildir eru stilltar fyrir hlut, eigandi hlutarins getur alltaf breytt heimildum hlutarins.

Meiri upplýsingar eru undir "Ownership" í hjálpinni með Windows Server.

Erfðir heimilda

Erfðir gera kerfisstjórum kleift að úthluta og sjá um heimildir með auðveldum hætti. Þessi aðgerð veldur því að hlutir í geymi erfa sjálfkrafa allar erfanlegar heimildir geymisins. Til dæmis, þegar skrár eru búnar til í möppu erfa þær heimildir möppurnar. Aðeins þær heimildir sem merkt er að skuli erfast, erfast.

Notendaheimildir

Notendaheimildir veita notendum og hópum tilteknar heimildir og innskráningarréttindi í tölvuumhverfinu.

Upplýsingar um notendaréttindi eru undir "User Rights" í hjálpinni með Windows Server.

Endurskoðun hluta

Hægt er að endurskoða aðgang notenda að hlutum. Síðan er hægt að skoða þessi öryggistengdu tilvik í öryggiskladdanum með Event Viewer.

Meiri upplýsingar eru undir "Auditing" í hjálpinni með Windows Server.

Bestu venjur í aðgangsstýringu

- Úthluta skal heimildum á hópa en ekki notendur. Þar sem það er óskilvirkt að viðhalda notendareikningum beint ætti úthlutun heimilda til stakra notenda að heyra til undantekninga.
- Nota skal Deny permissions í tilteknum sértilfellum. Til dæmis er hægt að nota Deny permissions til að undanskilja undirmengi í hóp sem er með heimildir.
- Aldrei skal neita hópnum Everyone aðgangi að hlut. Ef öllum er meinaður aðgangur að hlut nær það einnig til kerfisstjóra. Betri lausn væri að fjarlægja hópinn Everyone, svo lengi sem öðrum notendum, hópum eða tölvum er veitt heimild að hlutnum. Munið að ef engar heimildir eru skilgreindar er enginn aðgangur heimilaður.
- Úthluta skal heimildum á hlut eins ofarlega í trénu og hægt er og beita síðan erfðum til að miðla öryggisstillingunum um tréð. Hægt er að beita aðgangsstýringarstillingum á fljótlegan og skilvirkan hátt á alla undirhluti eða undirtré yfirhlutar. Með því að gera þetta fást hámarksáhrif með minnstri fyrirhöfn. Heimildarstillingarnar sem kokmið er á ættu að vera réttar fyrir meirihluta notenda, hópa og tölva.
- Beinar heimildir geta stundum komið í stað erfðra heimilda. Erfðar Deny permissions stillingar koma ekki í veg fyrir aðgang að hlut ef hluturinn er með beina Allow permission færslu. Beinar heimildir hafa forgang yfir erfðar heimildir, jafnvel erfðar synjanir á heimild.
- Vegna heimilda fyrir hluti í Active Directory® skal tryggja að þið hafið skilning á bestu venjum vegna hluta í Active Directory.

Nánari upplýsingar eru í kaflanum "Best Practices for Assigning Permissions on Active Directory Objects" í hjálpinni með Windows Server 2003.

Ytra öryggi - Eldveggur

Eldveggur er vélbúnaður eða hugbúnaður sem kemur í veg fyrir að gagnapakkar berist inn í eða fari út fyrir tilgreint net. Til að stjórna umferðinni eru tengi í eldveggnum annað hvort opnuð eða lokuð fyrir upplýsingapökkum. Eldveggurinn lítur á mismunandi upplýsingar í hverjum gagnapakka: samskiptaregluna sem pakkinn er sendur með, viðtökustað eða sendanda pakkans, tegund innihalds pakkans og númer tengisins sem hann er sendur til. Ef eldveggurinn er stilltur til að samþykkja tilgreinda samskiptareglu í gegnum tengið er pakkanum hleypt í gegn. Microsoft Windows Small Business Server 2003 Premium Edition er seldur með Microsoft Internet Security and Acceleration (ISA) Server 2000 sem eldveggslausn. Eldveggur fylgir líka Small Business Server Standard Edition.

ISA Server 2004

Internet Security and Acceleration (ISA) Server 2000 beinir beiðnum og svörum á milli tölva á Internetinu og biðlaratölva á innra netinu með öruggum hætti.

ISA Server vinnur sem örugg gátt til Internetsins fyrir biðlara á staðbundna netinu. ISA Server tölvan er gagnsæ gagnvart öðrum aðilum á samskiptaslóðinni. Internet-notandinn ætti ekki að taka eftir því að eldveggsþjónn sé til staðar nema notandinn reyni að fá aðgang að þjónustu eða fara á vefsetur þar sem ISA Server tölvan synjar aðgangi. Internet-þjónninn sem tengst er við túlkar beiðnirnar frá ISA Server tölvunni eins og beiðnirnar berist frá biðlaraforritinu.

Þegar síun Internet Protocol (IP) hluta er valið eru vefstaðgengils- og eldveggsþjónustur virkjaðar til að sía tvístraða pakka. Með því að sía pakkahluti er öllum tvístruðum IP-pökkum fleygt. Velþekkt “árás” felst í því að senda tvístraða pakka og setja þá síðan saman aftur þannig að það geti valdið kerfinu skaða.

ISA Server er með árásargreiningarbúnað sem greinir tímann þegar reynt er að ráðast á net og framkvæmir safn samskipaðra aðgerða (eða viðvarana) ef til árásar kemur.

Ef Internet Information Services (IIS) er uppsett á ISA Server tölvunni verður að samskipa það þannig að það noti ekki tengin sem ISA Server notar fyrir vefbeiðnir frá þjóninum (sjálfgildið er 8080) og vefbeiðnir sem berast þjóninum (sjálfgildið er 80). Til dæmis er hægt að stilla IIS á að fylgjast með tengi 81 og samskipa síðan ISA Server tölvunni til að beina vefbeiðnum sem berast á tengi 81 í staðbundnu tölvunni sem keyrir IIS.

Ef árekstur er á milli tengja sem ISA Server og IIS nota stöðvar uppsetningarforritið birtingarþjónustu IIS. Síðan er hægt að breyta IIS til að fylgjast með öðru tengi og endurræsa birtingarþjónustu IIS.

Reglur fyrir ISA Server

Hægt er að skilgreina reglu í ISA Server sem stjórnar aðgangi utan og innan að. Reglur um setur og efni tilgreina hvaða setrum og efni hægt er að fá aðgang að. Reglur um samskiptareglur tilgreina hvort tiltekin samskiptaregla sé tiltæk fyrir samskipti á innleið og útleið.

Hægt er að stofna reglur um setur og efni, reglur um samskiptareglur, reglur um vefbirtingu og IP-pakkasíur. Þessar reglur ákvarða hvernig ISA Server biðlarar eiga samskipti við Internetið og hvaða samskipti eru heimil.

Vírusvarnir

Tölvuvírus er keyrsluskrá sem er hönnuð til að afrita sig, eyða eða skemma gagnaskrám og forritum og komast hjá greiningu. Reyndar eru vírusar oft endurskrifaðir og lagfærðir þannig að þeir finnist ekki. Vírusar eru oft sendir sem viðhengi í tölvupósti. Stöðugt þarf að uppfæra vírusvarnarforrit til að leita að nýjum og breyttum vírusum. Vírusar eru algengasta aðferðin við tölvuskemmdarverk.

Vírusvarnarhugbúnaður er sérstaklega hannaður til að finna og koma í veg fyrir vírusa. Þar sem nýir vírusar koma stöðugt fram bjóða margir framleiðendur vírusvarnarforrita viðskiptavinum sínum reglubundnar uppfærslur á hugbúnaðinum. Microsoft mælir sterklega með því að vírusvarnarhugbúnaður sé settur upp í umhverfi viðskiptavinarins.

Vírushugbúnaður er venjulega settur upp á þessum þrem stöðum: vinnustöðvum notenda, netþjónum og netinu þar sem tölvupóstur kemur inn í (og í sumum tilvikum fer frá) fyrirtækinu.

Tegundir vírusa

Það eru þrjár megin gerðir vírusa sem smita tölvukerfi: ræsigeiravírusar, skráasýkingarvírusar og Trójuhestaforrit.

Ræsigeiravírusar

Þegar tölva er ræst fer hún yfir ræsigeirann á harða diskinum áður en stýrikerfið eða aðrar ræsiskrár eru hlaðnar inn. Ræsigeiravírus er hannaður til að skipta á upplýsingum á ræsigeirum harða disksins og eigin kóta. Þegar tölva er smituð með ræsigeiravírus er víruskótinn lesinn inn í minni á undan nokkru öðru. Þegar vírusinn er kominn í minnið getur hann afritað sig á aðra diska sem eru notaðir í sýktu tölvunni.

Skráasmitsvírus

Algengasta tegund vírusa, skráasmitsvírusar, festir sig við keyrsluskrá með því að bæta eigin kóta við keyrsluskrána. Víruskótanum er vanalega bætt við þannig að hann finnist ekki. Þegar sýkta skráin er keyrð getur vírusinn fest sig við aðrar keyrsluskrár. Skrár sem smitast af þessari tegund vírusa hafa yfirleitt nafnaukana .com, .exe eða .sys.

Sumir skráasmitsvírusar eru hannaðir í ákveðnum tilgangi. Forritstegundir sem oft er ráðist á eru .ovl-skrár (“overlay”) og .dll-skrár (“dynamic-link library”). Þó að þessar skrár séu ekki keyrðar kalla keyrsluskrár í þær. Vírusinn flyst á milli þegar kallað er.

Skemmdir á gögnum verða þegar vírusinn er ræstur. Hægt er að ræsa vírus þegar sýkt skrá er keyrð eða þegar tiltekin umhverfisskilyrði eru uppfyllt (eins og tiltekin kerfisdagsetning).

Trójuhestsforrit

Trójuhestsforrit er í raun ekki vírus. Lykilmunurinn á milli vírusa og Trójuhesta er sá að Trójuhestar afrita sig ekki; þeir eyðileggja bara upplýsingar á harða diskinum. Trójuhestur dulbýr sig sem lögmætt forrit eins og leik eða nytjaforrit. Þegar hann er keyrður getur hann þó eyðilagt eða ruglað gögnum.

Bestu venjur um vírusvarnir

Hægt er að koma í veg fyrir útbreiðslu fjölvavírusa. Hér eru nokkur ráð til að forðast smit sem deila ætti með viðskiptavinum:

- Setja skal upp vírusvarnarlausn sem leitar að vírusum í skilaboðum sem berast frá Internetinu áður en skilaboðin fara í gegnum beininn. Þetta tryggir að leitað er að þekktum vírusum í tölvupósti.
- Þekkið uppruna skjala sem tekið er á móti. Ekki ætti að opna skjöl nema þau séu frá einhverjum sem viðskiptavinurinn treystir.

- Tala skal við þann sem bjó til skjalið. Ef notendur eru í einhverjum vafa um hvort skjalið sé öruggt ættu þeir að hafa samband við þann sem bjó til skjalið.
- Nota skal fjölvavírusavörn Microsoft Office. Í Office láta forritin notandann vita ef fjölvar eru í skjali. Þessi aðgerð gerir notandanum kleift að gera fjölvana virka eða óvirka þegar skjalið er opnað.
- Nota skal vírusleitarhugbúnað til að finna og fjarlægja fjölvavírusa. Vírusleitarhugbúnaður getur greint og oft fjarlægt fjölvavírusa úr skjölum. Microsoft mælir með notkun vírusvarnarhugbúnaður sem er vottaður af International Computer Security Association (ICSA).

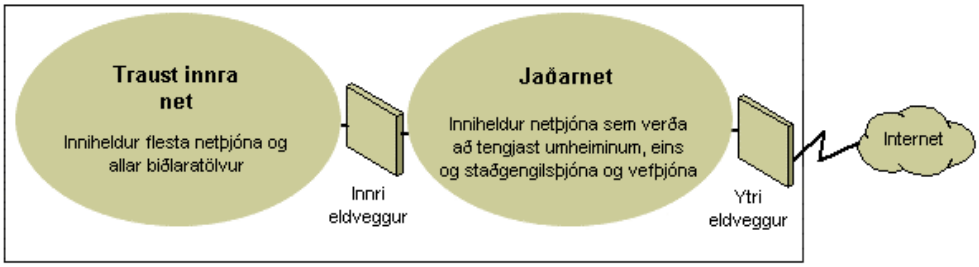
Nánari upplýsingar um vírusa og tölvuöryggi almennt eru á eftirtöldum vefsetrum Microsoft um öryggi:

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

Áætlanir um netöryggi

Þar sem hönnun og innleiðing IP-netumhverfis krefst jafnvægis á milli hagsmuna einkanets og almenns nets hefur eldveggurinn orðið lykilþáttur í því að verja heilleika neta. Eldveggur er ekki stakur hlutur. National Computer Security Association (NCSA) skilgreinir eldvegg sem "kerfi eða samsetningu kerfa sem setur mörk á milli tveggja eða fleiri neta." Þó að mismunandi hugtök séu notuð eru þessi mörk víða þekkt sem jaðarnet. Jaðarnetið verndar innra netið eða staðarnetið (LAN) fyrir árásum með því að stjórna aðgangi frá Internetinu eða öðrum stórum netum.

Þessi mynd sýnir jaðarnet sem umlukið er eldveggjum og sett á milli einkanets og Internetsins til að tryggja einkanetið:



Grunnjaðarnet

Fyrirtæki hafa mismunandi hátt á því að nota eldveggi í öryggisskyni. IP-pakkasíun veitir lítið öryggi, er erfið umsjónar og er auðvelt að komast hjá. Forritagáttir eru öruggari en pakkasíur og auðveldara er að stjórna þeim því þau eiga aðeins við tiltekin fá forrit eins og ákveðið tölvupóstkerfi. Rásagáttir eru skilvirkastar þegar notandi netforrits er meira áhyggjuefni en gögnin sem send eru frá forritinu. Staðgengilsþjónn er yfirgripsmikið öryggisverkfæri sem inniheldur forritsgátt, öruggan aðgang fyrir ónafngreinda notendur og aðra þjónustu. Hér eru upplýsingar um þessa valkosti:

- **IP-pakkasíun**
  IP-pakkasíun var fyrsta innleiðing eldveggstækni. Pakkahausar eru skoðaðir til að sjá uppruna- og viðtökuvistföng, gáttanúmer fyrir Transmission Control Protocol (TCP) og User Datagram Protocol (UDP) og aðrar upplýsingar. Pakkasíun er takmörkuð tækni sem nýtist best í skýru öryggisumhverfi þar sem, til dæmis, öllu utan jaðarnetsins er ekki treyst og öllu innan þess er treyst. Á undanförnum árum hafa ýmsir framleiðendur endurbætt pakkasíunaraðferðina með því að bæta greindum ákvarðanatökuaðgerðum við pakkasíunarkjarnann og þannig búið til nýja gerð af pakkasíun sem kallast *"stateful protocol inspection"*. Hægt er að samskipa pakkasíun til að samþykkja ákveðnar tegundir af pökkum en hafna öllum öðrum eða til að hafna ákveðnum tegundum af pökkum og samþykkja allar aðrar.
- **Forritsgáttir**
  Forritsgáttir eru notaðar þegar sjálft efni forrits er aðal áhyggjuefnið. Það að þær séu bundnar við forrit er bæði styrkur þeirra og veikleiki því þær aðlagast ekki auðveldlega að breytingum á tækni.
- **Rásagáttir**
  Rásagáttir eru göng sem gerð eru í gegnum eldvegg til að tengja ákveðna ferla eða kerfi öðrum megin við ákveðna ferla eða kerfi hinum megin. Best er að nota rásagáttir við aðstæður þar sem hugsanlega er meiri hætta af notanda forritsins en upplýsingunum sem forritið vinnur með. Rásagáttin er frábrugðin pakkasíu að því leiti að hún getur tengst utan-bands forritsskema sem getur bætt við aukaupplýsingum.
- **Staðgengilsþjónar**
  Staðgengilsþjónar eru yfirgripsmikil öryggisverkfæri sem innihalda eldvegg og forritsgáttaraðgerðir sem stjórna Internet-umferð til og frá staðarneti. Staðgengilsþjónar veita einnig flýtiminnisvistun skjala og aðgangsstýringu. Staðgengilsþjónn getur bætt frammistöðu með því að vista og miðla beint gögnum sem oft er beðið um eins og vinsæla vefsíðu. Staðgengilsþjónn getur einnig síað og fleygt beiðnum sem eigandinn telur ekki eiga við, svo sem beiðnir um óheimilan aðgang að einkaskrám.

Gangið úr skugga um að viðskiptavinurinn nýti sér þær öryggisaðgerðir eldveggja sem geta hjálpað honum. Setjið jaðarnet í netskipulagið á stað þar sem öll umferð utan frá fyrirtækisnetinu þarf að fara í gegnum jaðarinn sem ytri eldveggurinn viðheldur. Hægt er að fínstilla stjórn á eldveggnum til að uppfylla þarfir viðskiptavinarins og samskipa eldveggi til að tilkynna allar tilraunir til óheimils aðgangs.

Til að halda fjölda tengja sem þarf að opna í innri eldveggnum í lágmarki er hægt að nota hugbúnaðareldvegg eins og ISA Server 2000.

Nánari upplýsingar um TCP/IP eru undir "Designing a TCP/IP Network" á http://www.microsoft.com/resources/documentation/WindowsServ/2003/all/deployguide/en-us/dnsbb_tcp_overview.asp.

Þráðlaus net

Sjálfgefið er að þráðlaus net séu þannig samskipuð að hægt sé að hlera þráðlaus merki. Þau geta verið viðkvæm fyrir því að óviðkomandi aðilar fái aðgang vegna sjálfgefinna stillinga í sumum þráðlausum vélbúnaði, aðgengisins sem þráðlaus net bjóða og dulritunaraðferða sem eru til staðar. Til eru samskipunarkostir og verkfæri sem geta varið kerfi fyrir hlerun en hafið hugfast að þau gera ekkert til að verja tölvurnar fyrir tölvuþrjótum og vírusum sem komast inn í gegnum Internet-tenginguna. Þess vegna er mjög mikilvægt að nota eldvegg til að vernda tölvurnar fyrir óæskilegum árásaraðilum á Internetinu.

Nánari upplýsingar um hvernig vernda skuli þráðlaus net eru undir "How to Make Your 802.11b Wireless Home Network More Secure" á http://support.microsoft.com/default.aspx?scid=kb;en-us;309369.

Dæmi um netöryggi

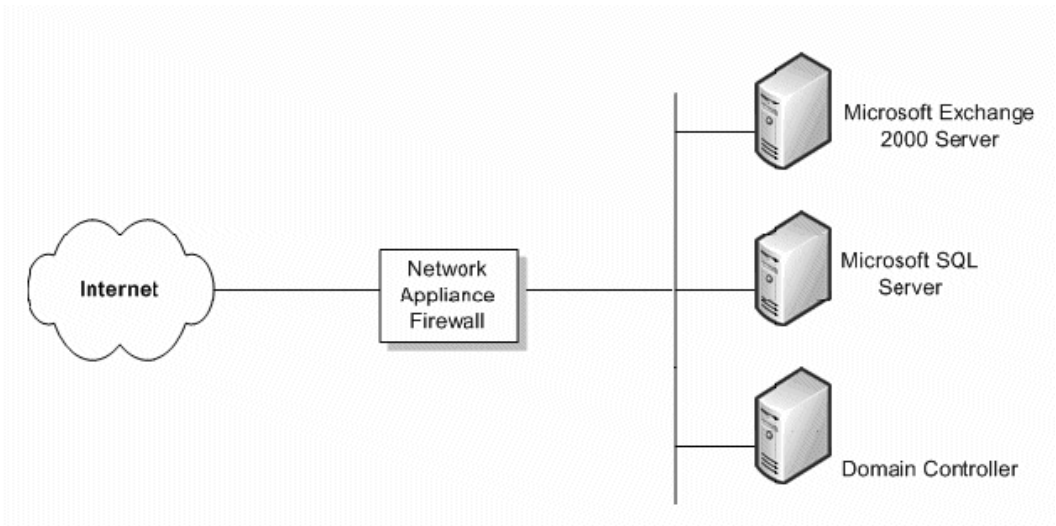
Stig netöryggis sem fyrirtæki viðskiptavinarins þarfnast fer eftir nokkrum þáttum. Yfirleitt er gerð málamiðlun á milli kostnaðar og þarfarinnar fyrir að tryggja öryggi gagna fyrirtækisins. Það er mögulegt að lítil fyrirtæki hafi mjög flókið öryggisskipulag sem veitir mesta mögulega netöryggi en lítil fyrirtæki hafa hugsanlega ekki efni á svo miklu öryggi. Í þessum kafla lítum við á fjögur dæmi og gefum ráð í hverju þeirra fyrir sig sem veita mismikið öryggi.

Enginn eldveggur

Ef viðskiptavinurinn er með tengingu við Internetið en engan eldvegg þarf að koma á einhvers konar netöryggi. Til eru einföld eldveggsforrit sem veita nægilegt öryggi til að stöðva flesta tölvuþrjóta.

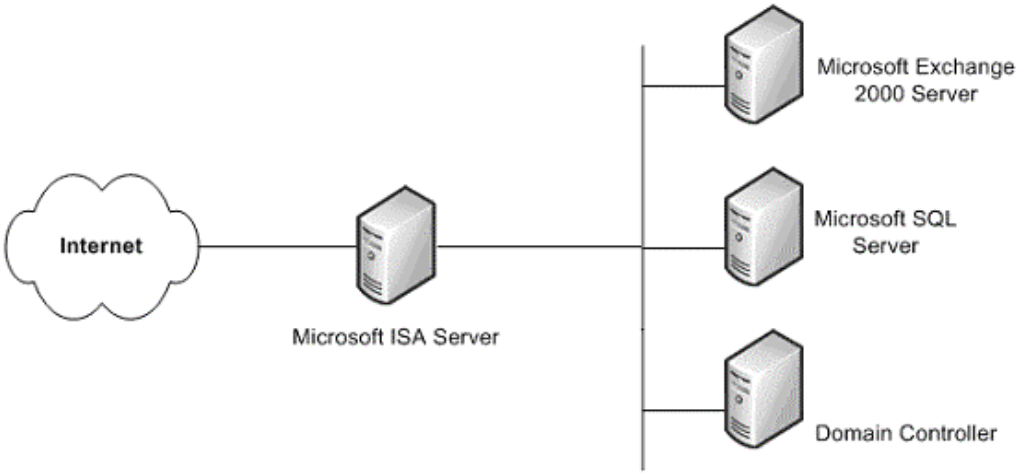
Einn einfaldur eldveggur

Lágmarks ráðlagt öryggisstig er einn eldveggur á milli Internetsins og gagna viðskiptavinarins. Þessi eldveggur veitir hugsanlega ekki þróað öryggi og ætti ekki að teljast mjög öruggur. En hann er betri en ekkert.



Einfaldur eldveggur

Vonandi býður fjárhagur viðskiptavinarins upp á öruggari lausn sem verndar gögn fyrirtækisins. Ein slík lausn er ISA Server. Viðbótarkostnaðurinn af þessum viðbótar netþjóni veitir mun meira öryggi en venjulegur eldveggur þar sem þeir veita vanalega aðeins hliðrun netfanga (NAT) og pakkasíun.



ISA Server eldveggur

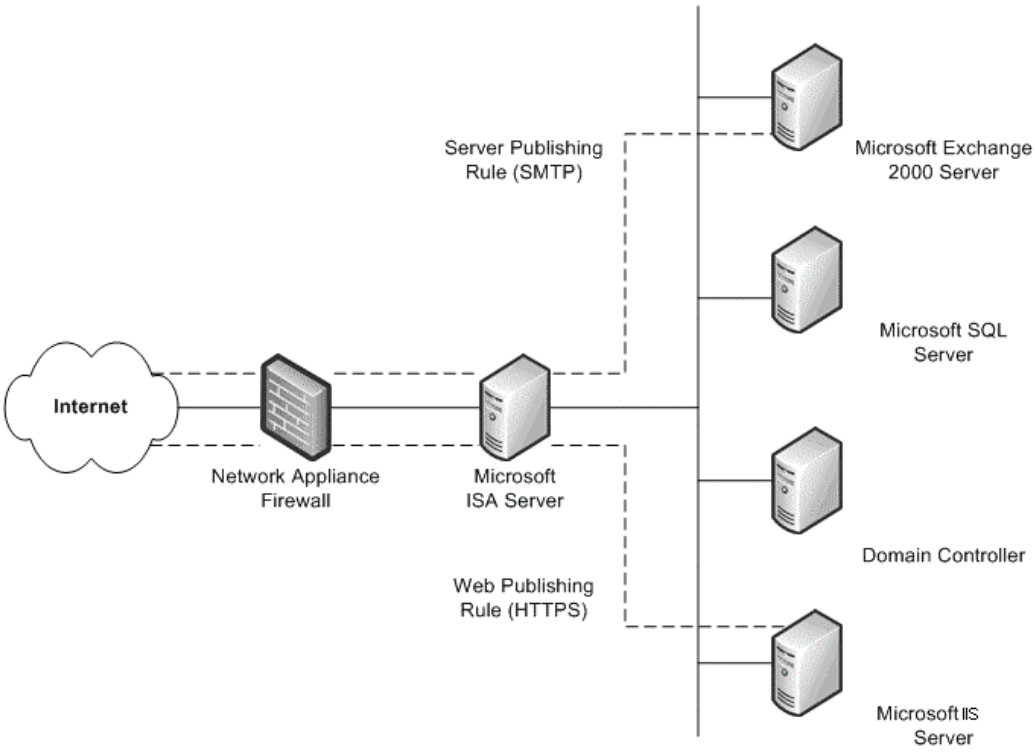
Þessi eins eldveggslausn er öruggari en einföld eldveggsforrit og veitir öryggisþjónustu sem á sérstaklega við Windows.

Einn eldveggur fyrir

Ef viðskiptavinurinn er þegar með eldvegg sem skilur innra netið frá Internetinu mætti íhuga að setja upp annan eldvegg sem veitir margar leiðir til að samskipta innri tilföng fyrir Internetið.

Ein slík aðferð er vefbirting. Það er þegar ISA Server er settur upp fyrir framan vefþjón fyrirtækisins sem veitir Internet-notendum aðgang. Fyrir vefbeiðnir á innleið getur ISA Server hermt eftir vefþjóni gagnvart umheiminum og afgreitt beiðnir biðlara um vefefni úr skyndiminninu. ISA Server framsendir eingöngu beiðnir til vefþjónsins þegar ekki er hægt að afgreiða beiðnirnar úr skyndiminninu.

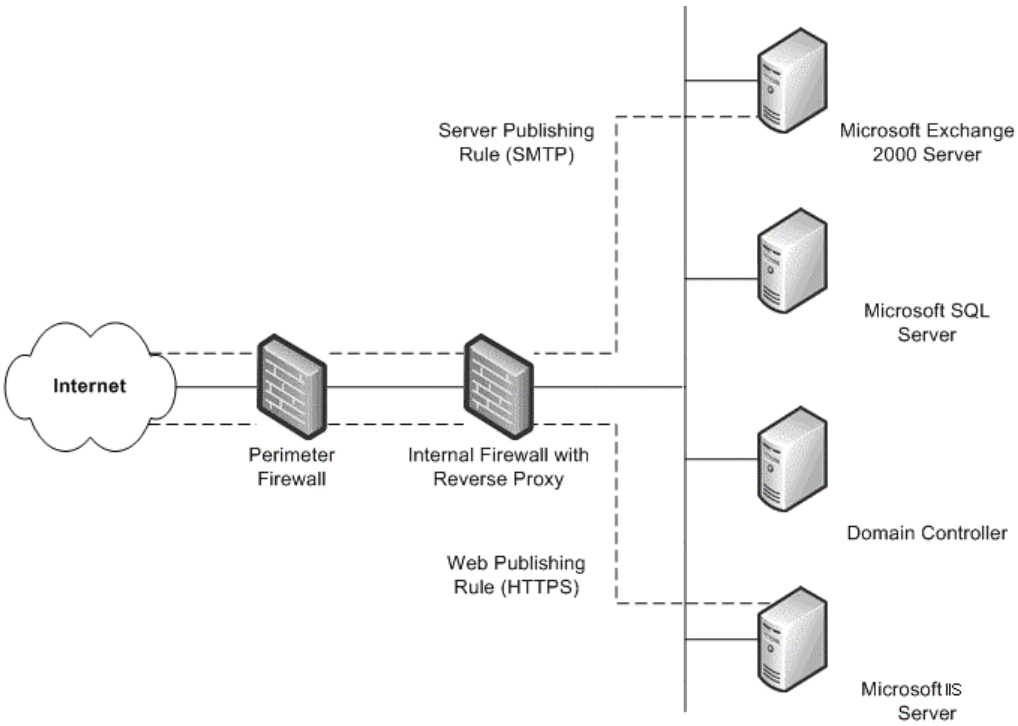
Önnur aðferð er þjónsbirting. ISA Server heimilar birtingu á innri þjónum á Internetinu án þess að stofna öryggi innra netsins í hættu. Hægt er að samskipa reglur um vefbirtingu og þjónsbirtingu sem ákvarða hvaða beiðnir skuli sendar netþjóni á staðarnetinu og veita aukið öryggi fyrir innri netþjónana.



Eldveggur sem fyrir er ásamt viðbættum ISA Server

Tveir eldveggir til staðar

Fjórða dæmið er þegar fyrirtækið er með tvo eldveggi til staðar með uppsettu jaðarneti (DMZ). Einn eða fleiri þessara netþjóna er með öfuga staðgengilsþjónustu þannig að biðlarar á Internetinu fá ekki beinan aðgang að netþjónum á innra netinu. Þess í stað grípur annar eldveggurinn, best er að það sé innri eldveggurinn, inn í netbeiðnir til innri netþjóna, kannar pakkana og framsendir þá síðan fyrir hönd Internet-hýsitölvunnar.



Tveir eldveggir til staðar

Þetta dæmi líkist dæminu á undan eftir að seinni eldveggnum hefur verið bætt við. Eini munurinn er sá að innri eldveggurinn sem styður öfugan staðgengil er ekki ISA Server. Í þessu dæmi ætti að vinna náið með stjórnendum hvors eldveggs um sig til að skilgreina þjónsbirtingarreglur sem fylgja öryggisreglunum.

Stjórnun öryggislagfæringa

Stýrikerfi og forrit eru oft gríðarlega flókin. Þau geta verið sett saman úr milljónum lína af kóta sem skrifaðar eru af mörgum forriturum. Það er nauðsynlegt að hugbúnaðurinn vinni áreiðanlega og stofni ekki öryggi eða stöðugleika upplýsingatækniumhverfisins í hættu. Til að draga úr vandamálum eru forrit prófuð ítarlega áður en þau eru gefin út. Hins vegar vinna árásaraðilar stöðugt að því að finna veikleika í hugbúnaði þannig að það er ekki hægt að sjá fyrir allar árásir.

Í mörgum fyrirtækjum er stjórnun lagfæringa hluti af heildarstefnu um stjórnun á breytingum og samskipun. Burt séð frá eðli og stærð fyrirtækisins er hins vegar mikilvægt að hafa góða stefnu um stjórnun lagfæringa, jafn vel þó fyrirtækið hafi enn ekki komið á skilvirkri stjórnun á breytingum og samskipunum. Meginþorri vel heppnaðra árása á tölvukerfi verða í þeim kerfum þar sem öryggislagfæringar hafa ekki verið settar upp.

Öryggislagfæringar eru ákveðin áskorun í flestum fyrirtækjum. Þegar veikleiki hefur fundist í hugbúnaði eru árásaraðilar vanalega fljótir að dreifa upplýsingum um það um samfélag tölvuþrjóta. Þegar veikleiki finnst í hugbúnaði þess leitast Microsoft við að gefa út öryggislagfæringu eins fljótt og hægt er. Þar til lagfæringin hefur verið sett upp getur öryggið sem viðskiptavinurinn treystir á og væntir verið skert til muna.

Í Navision-umhverfinu þarf að tryggja að viðskiptavinirnir hafi nýjustu öryggislagfæringarnar upp settar í öllu kerfinu. Tryggja skal að viðskiptavinurinn noti eina af þeim tæknum sem Microsoft hefur gert tiltækar. Þeirra á meðal eru:

- **Öryggistilkynningaþjónusta Microsoft**
  Öryggistilkynningaþjónustan er tölvupóstlisti sem dreifir tilkynningum þegar uppfærslur eru gefnar út. Þessar tilkynningar eru mikilvægur liður í virkri öryggisstefnu. Þær eru einnig tiltækar á vefsetrinu TechNet Product Security Notification: http://www.microsoft.com/technet/security/bulletin/notify.mspx.
- **Sjálfvirkar uppfærslur Microsoft**
  Windows getur sjálfkrafa sett upp öryggisuppfærslur.
- **Leitarverkfæri fyrir öryggistilkynningar Microsoft**
  Leitarverkfæri fyrir öryggistilkynningar er tiltækt á vefsetrinu Security Bulletin Service: http://www.microsoft.com/technet/security/current.aspx. Viðskiptavinir geta ákveðið hvaða uppfærslur þeir þurfa á grundvelli stýrikerfisins, forritana og þjónustupakkana sem þeir eru að nota.
- **Microsoft Baseline Security Analyzer (MBSA)**
  Þetta myndræna verkfæri er fáanlegt á vefsetri Microsoft Baseline Security Analyzer: http://www.microsoft.com/technet/security/tools/mbsahome.mspx. Þetta verkfæri ber gildandi stöðu tölvunnar við lista yfir uppfærslur frá Microsoft. MBSA framkvæmir einnig grunnöryggiskannanir á styrkleika aðgangsorða og stillingum gildistíma, reglum um gestareikninga og fjölda annara sviða. MBSA leitar einnig að veikleikum í Microsoft Internet Information Services (IIS), SQL Server™ 2000, Exchange 5.5, Exchange 2000 og Exchange Server 2003.
- **Microsoft Software Update Services (SUS)**
  Áður þekkt sem Windows Update Corporate Edition. Þetta verkfæri gerir fyrirtækjum kleift að geyma allar mikilvægar uppfærslur og öryggispökkum (security rollup packages - SRP) sem fáanlegar eru á vefsetrinu Windows Update á staðbundnum tölvum. Þetta verkfæri vinnur með nýrri útgáfu af sjálfvirkum uppfærslubiðlurum til að leggja grunn að öflugri stefnu sjálfvirkt niðurhal og uppsetningu. Nýja biðlarasafnið inniheldur biðlara fyrir Windows 2000 og Windows Server 2003 og hefur möguleika á því að setja sjálfkrafa upp sóttar uppfærslur. Nánari upplýsingar um Microsoft SUS eru á slóðinni http://www.microsoft.com/windows2000/windowsupdate/sus/default.asp.
- **Microsoft Systems Management Server (SMS) Software Update Services Feature Pack**
  SMS Software Update Services Feature Pack inniheldur fjölda verkfæra sem ætlað er að auðvelda dreifingu hugbúnaðaruppfærslna um fyrirtækið. Verkfærin innihalda Security Update Inventory Tool, Microsoft Office Inventory Tool for Updates, Distribute Software Updates Wizard og SMS Web Reporting Tool með Web Reports Add-in for Software Updates. Nánari upplýsingar um hvert verkfæri eru á http://www.microsoft.com/smserver/downloads/20/featurepacks/suspack/.

Talið við viðskiptavinina um öll þessi verkfæri og hvetjið til notkunar þeirra. Það er mjög mikilvægt að tekið sé á öryggismálum eins fljótt og hægt er jafnframt því að viðhalda stöðugleika umhverfisins.

Öryggisstillingar SQL Server 2000

Þar sem Navision keyrir líka á SQL Server 2000 er mikilvægt að gripið sé til ráðstafana til að auka öryggi uppsetningar viðskiptavinarins á SQL Server 2000. Eftirtaldar aðgerðir auka öryggi SQL Server:

- Ganga skal úr skugga um að nýjustu þjónustupakkar fyrir stýrikerfið og SQL Server 2000 séu upp settir. Nýjustu upplýsingar er að finna á vefsetri Microsoft um öryggismál http://www.microsoft.com/security/default.asp.
- Hvað varðar öryggi skráakerfi skal tryggja að allar gagna- og kerfisskrár SQL Server 2000 séu settar upp á NTFS-diskhlutum. Nota ætti NTFS-heimildir til að gera skrárnar aðeins tiltækar fyrir kerfisstjóra eða notendur á kerfisstigi. Þetta tryggir að notendur fá ekki aðgang að þessum skrám þegar þjónustan MSSQLSERVER er ekki í keyrslu.
- Nota skal lénsreikning með litlar heimildir eins og NT Authority\Network Service eða LocalSystem (ráðlagt) reikninginn fyrir SQL Server 2000 þjónustu (MSSQLSERVER). Þessi reikningur ætti að hafa lágmarksréttindi í léninu og ætti að auðvelda að halda árás á netþjóninn í skefjum (en ekki stöðva) ef til hennar kemur. Með öðrum orðum ætti þessi reikningur aðeins að hafa heimildir staðbundins notanda í léninu. EF SQL Server 2000 notar reikning lénskerfisstjóra til að keyra þjónustuna leiðir öryggisrof í þjóninum til öryggisrofs í öllu léninu. Til að breyta þessari stillingu skal nota SQL Server Enterprise Manager. Aðgangsstjórnunarlistum (ACL) á skrám, stýriskránni og notendaréttindum verður breytt sjálfkrafa.
- Flestar útgáfur af SQL Server 2000 eru settar upp með tveim sjálfgefnum gagnagrunnum, **Northwind** og **pubs**. Báðir gagnagrunnarnir eru sýnigagnagrunnar sem eru notaðir við prófanir, þjálfun og almenn dæmi. Ekki ætti að keyra þá í starfandi kerfi. Vitneskjan um að þessir gagnagrunnar séu til staðar getur hvatt árasaraðila til að reyna misnotkun á grunni sjálfgefinna stillinga og sjálfgefinnar samskipunar. Ef **Northwind** og **pubs** eru til staðar í starfandi SQL Server 2000 tölvu skal fjarlægja þá.
- Sjálfgefið er að endurskoðun á SQL Server 2000 kerfinu sé óvirk og því eru engin skilyrði yfirfarin. Þetta gerir greiningu innrása erfiðari og auðveldar árásaraðilum að fela slóð sína. Að lágmarki ætti að virkja endurskoðun á misheppnuðum innskráningum.

Nýjustu öryggisupplýsingar um SQL Server 2000 eru á http://www.microsoft.com/sql/techinfo/administration/2000/security/default.asp.

Um Microsoft Business Solutions

Microsoft Business Solutions, dótturfyrirtæki Microsoft, býður mikið úrval samþættra viðskiptalausna og þjónustu sem hönnuð er til að auðvelda litlum, miðlungs stórum og stórum fyrirtækjum að ná betri tengslum við viðskiptavini, starfsmenn, samstarfsaðila og birgja. Forrit Microsoft Business Solutions bæta rekstrarferla í fjármálastjórnun, greiningu, starfsmannahaldi, verkefnastjórnun, tengslastjórnun, þjónustustjórnun, aðfangakeðjustjórnun, rafrænum viðskiptum, framleiðslu- og smásölustjórnun. Forritin eru hönnuð til að veita innsýn svo viðskiptavinir eigi auðveldara með að ná árangri í viðskiptum. Meiri upplýsingar um Microsoft Business Solutions eru á http://www.microsoft.com/BusinessSolutions/