Microsoft Business Solutions

Navision Security Hardening Guide

Avaldatud: oktoober 2004

Microsoft

Sisukord

Sissejuhatus

Microsoft® Windows® pakub laiahaardelist standarditel põhinevat võrguturvalisust. Kõige laiemas mõttes hõlmab turvalisus planeerimist ja kompromissidega arvestamist. Näiteks võib arvuti asuda lukustatud seifis, kus sellele pääseb juurde ainult üks süsteemiülem. See arvuti võib küll olla turvaline, ent sest on laiemas plaanis vähe kasu, kuna see pole ühendatud ühegi teise arvutiga. Peate aru pidama, kuidas muuta võrk võimalikult turvaliseks, ohverdamata selleks kasutatavust.

Enamik ettevõtteid oskab ette näha väliseid rünnakuid ja ehitab tulemüüre, kuid paljud asutused ei pööra tähelepanu sellele, kuidas turvarünnetega toime tulla siis, kui pahatahtlik kasutaja on juba tulemüürist mööda pääsenud. Turvameetmed töötavad kliendi keskkonnas hästi, kui kasutajad ei pea turvalise töötamise nimel täitma liiga palju protseduure ja juhiseid. Turvapoliitika järgimine peaks kasutajate jaoks olema võimalikult lihtne, muidu leiavad kasutajad töötamiseks vähemturvalisi võimalusi.

Kuna Navisioni installatsioonide suurus on ettevõtte vajadustest sõltuvalt vägagi erinev, tuleb iga kliendi vajadusi hoolikalt kaaluda, võrreldes turvalisuse nõutavat tõhususastet eeldatavate kuludega. Kliendi usalduse pälvinud nõuandjana saate kasutada oma kogemusi ja teadmisi ning soovitada poliitikat, mis vastab kliendi turvavajadustele, muutumata samas koormaks, mis võiks klienti sundida poliitika elluviimisest loobuma.

Navisioni turvalisuse head tavad

Järgmised üldreeglid võivad teid aidata Navisioni keskkonna turvalisuse tõstmisel:

- Kui soovite teenusena käitada Navision Database Serverit või kasutada serveri käivitamisel käsurea parameetrit *installasservice*, peaksite tagama, et teenus töötab NT Authority\Network Service'i kontona. NT Authority\Network Service'i konto on olemas ainult opsüsteemides Windows™ XP ja Windows Server™ 2003. Kui kasutate Windows 2000 Serverit, peaksite selle teenuse jaoks looma võimalikult väheste õigustega konto, muidu eraldatakse teenusele kohaliku süsteemi (Local System) konto. Sellel kontol ei tohiks olla rohkem õigusi kui tavalisel kasutajakontol või peaks see olema domeenikonto, mis pole ülemakonto ei domeenis ega üheski kohalikus arvutis.

  NT Authority\Network Service'i kontole või serveri kasutajakontole tuleb kindlasti anda andmebaasifailide lugemis- ja kirjutusõigus, et kasutajad saaksid andmebaasiga ühenduse luua**.**

  NT Authority\Network Service'i kontole andmebaasifaili lugemis- ja kirjutusõiguse andmine Windows XP-s:

  1. Liikuge Windows Exploreris kausta, mis sisaldab soovitud andmebaasifaili.
  2. Valige andmebaasifail. Paremklõpsake selle faili nime ja klõpsake käsku Atribuudid.
  3. Klõpsake aknas ***Atribuudid*** vahekaarti ***Turvalisus*** ja siis välja **Rühma- või kasutajanimed** all nuppu Lisa.
  4. Sisestage aknas ***Valige kasutajad, arvutid või rühmad*** väärtus *Võrguteenus* (Network Service) ja klõpsake nuppu OK.
  5. Võrguteenus (NETWORK SERVICE) lisatakse akna ***Atribuudid*** väljale **Rühma- või kasutajanimed**.
  6. Valige NETWORK SERVICE ja andke sellele väljal **Õigused** õigused *Lugemine* ja *Kirjutamine*.
- Navision Application Serveri teenus töötab vaikimisi NT Authority\Network Service'i kontona ning seega on sel kohalik juurdepääs Navision Database Serverile. Võrgus peate aga tagama, et Navision Application Serveri teenus töötaks sellise Windowsi domeenikontona, mille Navision Database Server ära tunneb (kui soovite, et sel oleks juurdepääs andmebaasiserverile). Sellel kontol ei tohiks olla ülemaõigusi ei domeenis ega üheski kohalikus arvutis.
- Kui kasutate rakendust SQL Server Option for Navision, töötab Microsoft SQL Server™ teenusena. Rakenduse SQL Server Option for Navision tööks on nõutav, et SQL Server saaks teha otsinguid aktiivkataloogis Active Directory, et tuua autentimiseks Windowsi kasutajarühmade loendeid. Seetõttu peate tagama, et SQL Serveri teenus töötab NT Authority\Network Service'i kontona.

  Tagamaks, et teenus töötab NT Authority\Network Service'i kontona:

  1. Otsige SQL Serveri arvutis üles teenus MSSQLSERVER. Paremklõpsake teenuse nime ja klõpsake siis käsku Atribuudid (Properties).
  2. Klõpsake akna ***Atribuudid*** (Properties) vahekaarti ***Sisselogimine*** (Log On).
  3. Klõpsake vahekaardi ***Sisselogimine*** (Log On) jaotises Logi sisse (Log on) kasutajana raadionuppu See konto (This Account), sisestage väärtus *NT Authority\NetworkService* ja klõpsake nuppu OK.

  SQL Serveri turvalisuse kohta lisateabe saamiseks külastage veebilehti:

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

  ja

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

- Kui kasutate mõnda Navisioni E-äri toodet (nt. Ärivärav ehk Commerce Gateway), peaksite tagama, et Commerce Gateway Request Server on õigesti installitud ning teenuste jaoks on määratud vaikekontosäte. Vaikekontosätte nimi on *CGRSUser* ja see annab Commerce Gateway Serverile juurdepääsu vähimale võimalikule hulgale muudele teenustele, mida server tööks vajab (sh. teenus *MSSQLSERVER* ning BizTalki teenus *BizTalk Group: BizTalkServerApplication*) ega hõlma erinevalt *Local Systemi* kontost muid globaalkontosätteid.
- Kasutage alati tugevaid paroole. Lisateavet tugevate paroolide kohta leiate lõigust „Tugevad paroolid“.
- Kasutage Windowsi logimisi. Navision võimaldab teil luua kahte liiki logimisi – andmebaasi logimisi ja Windowsi logimisi. Soovitame kasutada Windowsi logimisi, kuna sel juhul kasutatakse Windowsi autentimist ning saate rakendada korralikku paroolipoliitikat.
- Paroole ei tohiks korduvkasutada. Paroolide korduvkasutus terves süsteemis või domeenide lõikes on levinud teguviis. Näiteks võib kahe domeeni eest vastutav süsteemiülem luua mõlemas domeenis sama parooli kasutava domeeniülema konto ja määrata sama parooli koguni terve domeeni kõigis arvutites kohaliku ülemakonto parooliks. Kui aga ühe konto või arvuti andmete salastatust kompromiteeritakse, võib sellisel juhul ohtu sattuda kogu domeen.
- Pärast Navisioni installimist ja andmebaaside loomist või värskendamist peaksite looma Windowsi logimise ning andma sellele Navisionis rolli SUPER. See SUPER-kasutaja (ehk eeliskasutaja) haldab andmebaasihaldust, turvalisust jne. Määrake sellele logimisele tugev parool. Parooli tuleks kindlasti hoida konfidentsiaalsena. Selle kaitse peaks olema võrreldav SQL Serveri SA-parooli kaitsega. SUPER- ehk eeliskasutaja roll haldab kogu juurdepääsu andmebaasile, seetõttu peab selle kaitsetase olema võimalikult kõrge. SUPER-kasutaja parooli tohiksid teada ainult teie süsteemiülemad.
- Kõigil teistel kasutajatel, kellel on juurdepääs Navisioni andmebaasile, peaks olema võimalikult vähe õigusi. See tähendab, et neile tuleb Navisionis määrata rollid, mis annavad neile juurdepääsu ainult neile funktsioonidele, mida neil on ettevõttes oma töö tegemiseks vaja.
- Tagage, et ainult need kasutajad, kelle roll ettevõttes seda nõuab, saaksid FOB-faile importida, objektide kujundust muuta, andmebaasist varukoopiaid luua ja andmebaasi varukoopia põhjal taastada.
- Tehke oma Navisioni andmebaasist koopia ning pidage meeles, et varukoopiad tuleb korrapäraselt testida – ainult nii saate olla kindel, et andmebaasi saab varukoopia põhjal taastada.
- Hoidke varukoopiaid kindlas kohas, et vähendada näiteks selliste võimalike ohutegurite nagu tulekahju, suits, tolm, kõrge temperatuur, välk või loodusõnnetused (nt. maavärin) mõju.
- Ehkki Navision võib töötada mitmes Windowsi versioonis, soovitame teil kasutada kõige uuemat operatsioonisüsteemi, millel on kõige ajakohasemad turvalisusefunktsioonid. Praegu on nendeks operatsioonisüsteemideks Windows XP hoolduspaketiga SP2 ning Windows Server 2003.
- Värskeimate turvavärskenduste rakendamiseks kasutage opsüsteemide Windows 2000, Windows XP ja Windows Server 2003 funktsiooni Windows Update. Windowsi automaatvärskendusfunktsiooniga saate tagada, et ajaga käivad kaasas ka kõik teie klientarvutid, laadides alla ning installides värskeimad turvapaigad, hoolduspaketid ja värskendused.

- Soovitame Navisioni klientide ja Navision Database Serveri omavaheliseks suhtluseks kasutada turvalist TCPS-protokolli. TCPS on TCP/IP turvaline versioon, mis kasutab sisselülitatud krüptimisega SSPI-d (Security Support Provider Interface) ja Kerberose autentimist. TCPS on Navision Database Serveri vaikeprotokoll.
- Kliendil peaks õnnetuste puhuks olema taastekava, mis tagab pärast õnnetust teenuste kiire jätkamise. Taastekava peaks hõlmama näiteks järgmisi küsimusi:
  - uute/ajutiste seadmete hankimine;
  - andmebaaside varukoopiate põhjal uues süsteemis taastamine;
  - taastekava töökõlblikkuse testimine.

Füüsiline turvalisus

Füüsiline turvalisus on äärmiselt oluline, kuna seda ei saa tarkvaraturbega asendada. Kui näiteks kõvaketas varastatakse, siis varastatakse varem või hiljem ka kettal olevad andmed. Arutage kliendiga poliitika väljatöötamisel järgmisi füüsilise turvalisusega seotud küsimusi:

- Suurte installatsioonide puhul ettevõtetes, kus on oma IT-osakond, tagage, et serveriruumid ja tarkvara talletuskohad oleksid lukus.
- Selle kategooria seadmete seas on:
  - server, kus töötab Microsoft SQL Server 2000;
  - failiserver, kus asuvad Navisioni täitmisfailid.
- Hoidke vastava volituseta kasutajaid arvutitest eemal.
- Andmete tundlikkusest sõltumata veenduge, et paigaldatud oleks sissemurdmisele reageeriv häiresüsteem.
- Veenduge, et kriitilise tähtsusega andmete varukoopiaid talletataks mujal ja kindlasti tulekindlates konteinerites.

Töötajad

Haldusõigusi on kindlasti mõistlik kõigi toodete ja funktsioonide puhul piirata. Vaikimisi peaksid kliendid andma oma töötajatele süsteemifunktsioonidele ainult lugemispääsu, kui töötajal pole oma töö tegemiseks rohkem õigusi tarvis. Vähimate õiguste põhimõtet järgides soovitab Microsoft anda kasutajatele ainult minimaalsed andmetele ja funktsioonidele juurdepääsuks vajalikud õigused.
Võrgu turvalisust ohustavad ka rahulolematud ja endised töötajad. Klientidega turvalisuse teemal nõu pidades soovitage töötajate osas järgmist poliitikat:

- Uurige enne töötaja palkamist tema tausta.
- Oodake rahulolematutelt või endistelt töötajatelt „kättemaksu“.
- Töötaja lahkumisel veenduge, et kõik seostuvad Windowsi kontod ja paroolid keelataks. Aruandlusotstarbeks ärge kustutage kasutajaid. Ärge võtke vanu kontosid uuesti kasutusele.
- Koolitage kasutajad tähelepanelikuks ja laske neil kahtlasest tegevusest teatada.
- Ärge andke õigusi automaatselt. Kui kasutaja ei vaja juurdepääsu konkreetsele arvutile, arvutiruumile või failikogumile, siis veenduge, et ta seda juurdepääsu ei saaks.
- Koolitage keskastmejuhte töötajate probleeme märkama ja neile reageerima.

- Veenduge, et töötajad mõistaksid oma osa võrguturvalisuse säilitamises.
- Andke igale töötajale ettevõtte turvapoliitikast oma eksemplar.
- Ärge lubage kasutajatel installida tarkvara, mida tööandja pole heaks kiitnud.

Süsteemiülem

Soovitame teie klientide süsteemiülematel kindlasti silma peal hoida värskeimatel Microsofti turvaparandustel. Ründajad on võrku sissetungimiseks väikeste vigade leidmisel ja ühendamisel äärmiselt osavad. Süsteemiülemad peaksid esmalt tagama iga üksiku arvuti turvalisuse ning seejärel lisama turvavärskendused ja kasutama viirusetõrjetarkvara. Selles juhendis on ära toodud ohtralt linke ja ressursse, mis aitavad teil leida väärtuslikku teavet ning õppida tundma parimaid tavasid.

Võrgu turvaliseks muutmisel tuleb leida kompromiss ka ohutuse ja võrgu keerukuse vahel. Mida keerulisema ülesehitusega on võrk, seda raskem on võrku turvata või paigata, kui sissetungija on juba võrku pääsenud. Süsteemiülem peaks võrgu topograafia põhjalikult dokumenteerima, pidades silmas ülesehituse jätmist võimalikult lihtsaks.

Turvalisuse tagamisel on peamiselt tegemist riskide haldamisega. Kuna tehnoloogia pole imeravim, nõuab turvalisus tehnoloogia ühendamist poliitikaga. Teisisõnu ei saa kunagi olemas olla toodet, mille saaksite lihtsalt lahti pakkida ja võrku installida nii, et kohe oleks tagatud täiuslik turvalisus. Turvalisus on tehnoloogia ja poliitika ühine tulemus: võrgu turvalisuse taseme määratleb see, kuidas tehnoloogiat kasutatakse. Microsoft pakub turvateadlikku tehnoloogiat ja funktsioone, kuid iga ettevõtte jaoks oskab õige poliitika määratleda üksnes ettevõtte süsteemiülem ning teeb seda teie abiga. Kindlasti võtke turvalisuse aspekte juurutus- ja kasutuselevõtuprotsessis juba varakult arvesse. Uurige välja, mida teie klient soovib kaitsta ja mida ta on valmis selle nimel tegema.

Kavandamise lõppjärgus töötage välja plaanid õnnetusjuhtumite puhuks. Ühendage põhjalik planeerimine töökindla tehnoloogiaga – ja teie klient saab rõõmu tunda suurepärasest turvalisusest.

Lisateavet turvalisuse kohta leiate ingliskeelsest artiklist „Turvahalduse kümme muutmatut reeglit“, mis asub aadressil:
http://www.microsoft.com/technet/archive/community/columns/security/essays/10salaws.mspx

Turvahaldust käsitlevaid artikleid leiate ka veebisaidilt:
http://www.microsoft.com/technet/community/columns/secmgmt/smarch.mspx

Serveri operatsioonisüsteemi turvamine

Ehkki paljudel väiksematel klientidel ei pruugi serverioperatsioonisüsteemi olla, peate turvalisuse parimaid tavasid kindlasti mõistma, selgitamaks neid keerukama ülesehitusega võrgukeskkonnaga suurklientidele. Samuti peaksite teadma, et paljusid käesolevas dokumendis kirjeldatud poliitikavõtteid ja tavasid saab hõlpsasti rakendada ka nende klientide puhul, kellel on kasutusel ainult klientoperatsioonisüsteemid.

Käesolevas lõigus käsitletud mõisted kehtivad nii Microsoft Windows 2000 Serveri kui ka Microsoft Windows Server 2003 toodete kohta, ehkki see teave pärineb peamiselt Windows Server 2003 elektroonilisest spikrist. Windows Server 2003 pakub tugevat turvafunktsioonide komplekti. Windows Server 2003 elektrooniline spikker sisaldab täielikku teavet kõigi turvafunktsioonide ja protseduuride kohta.

Lisateavet Windows 2000 Serveri kohta saate Windows 2000 Serveri turvalisusekeskusest (Security Center) aadressil:
http://www.microsoft.com/technet/security/prodtech/win2000/default.mspx

Samuti võite lugeda Windows 2000 turvalisuse lisameetmete juhendit („Windows 2000 Security Hardening Guide“) aadressil:
http://www.microsoft.com/technet/security/prodtech/win2000/win2khg/default.mspx

Lisateavet Windows Server 2003 kohta leiate turvalisusejuhendist „*Windows Server 2003 Security Guide“* aadressil:
http://www.microsoft.com/technet/security/prodtech/win2003/w2003hg/sgch00.mspx

Windowsi serverite turvalisusemudeli põhifunktsioonid on autentimine, pääsujuhtimine ja ühekordne sisselogimine:

- Autentimine on protsess, mille käigus süsteem kontrollib kasutaja isikut tema sisselogimismandaadi kaudu. Kasutaja nime ja parooli võrreldakse autoriseeritud kasutajate loendiga. Kui süsteem tuvastab vastavuse, annab autoriseerimine kasutajale juurdepääsu süsteemile vastavalt tema õigusteloendis määratud ulatusele.
- Juurdepääsu kontroll ehk pääsujuhtimine piirab kasutaja juurdepääsu teabele või arvutiressurssidele, võttes aluseks kasutaja isiku ja liikmestaatuse eelmääratletud rühmades. Süsteemiülemad määravad pääsujuhtimise abil üldjuhul seda, milline juurdepääs on kasutajatel võrguressurssidele (nt. serverid, kaustad ja failid). Enamasti antakse kasutajatele ja kasutajarühmadele kindlatele objektidele juurdepääsu õigus.
- Ühekordne sisselogimine lubab kasutajal Windowsi domeeni ühe parooli abil üks kord sisse logida nii, et seejärel tunneb iga selles Windowsi domeenis asuv arvuti ta sama kasutajana ära. Ühekordne sisselogimine aitab süsteemiülematel juurutada paroolautentimist kogu Windowsi võrgus, tehes kasutajatele juurdepääsu lihtsamaks.

Järgmised lõigud sisaldavad kolme eelmainitud põhifunktsiooni üksikasjalikumaid kirjeldusi.

Autentimine

Autentimine on süsteemiturvalisuse põhitahke. Seda kasutatakse domeeni sisselogiva või võrguressurssidele juurdepääsu taotleva kasutaja isiku kontrollimiseks. Enamiku autentimissüsteemide puhul on nõrgimaks lüliks kasutaja parool.

Paroolid on esimene kaitseliin domeeni ja kohalike arvutite kaitsmiseks volitamata juurdepääsu eest. Soovitage kliendile järgmisi paroolipõhimõtteid:

- Kasutage alati tugevaid paroole.
- Kui parool on vaja paberile kirjutada, hoidke paberit turvalises kohas. Kui paberit pole enam vaja, siis hävitage see.
- Ärge avaldage oma parooli mitte kellelegi.

- Kasutage kõigi kasutajakontode jaoks erinevaid paroole.
- Muutke parooli aeg-ajalt.
- Hoolitsege ka selle eest, et paroolid poleks arvutis salvestatud kergesti leitavasse kohta.

Tugevad paroolid

Sageli kiputakse alahindama või kahe silma vahele jätma paroolide osa ettevõtte arvutivõrgu turvalisuse tagamises. Nagu juba eespool mainitud, moodustavad paroolid esimese kaitseliini teie võrku sissetungijate vastu. Seepärast peaksite veenduma, et kliendid nõuaksid oma töötajatelt tugevate paroolide kasutamist.

Samas arenevad aina edasi paroolide murdmiseks mõeldud tööriistad ning ka paroolide avamiseks kasutatavad arvutid on üha võimsamad. Kui paroolimurdmise tööriistale anda piisavalt aega, võib see lahti murda iga parooli. Siiski on tugevaid paroole nõrkadega võrreldes märksa keerulisem lahti murda.

Juhiseid selliste tugevate paroolide loomiseks, mida kasutaja suudaks meelde jätta, leiate võrgusaitidelt:

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

ja

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

Paroolipoliitika määratlemine

Kui aitate oma kliendil paroolipoliitikat määratleda, siis kontrollige kindlasti, et see poliitika nõuaks kõigi kasutajakontode puhul tugevaid paroole. Enamiku süsteemide puhul piisab Windows Server 2003 juhendis „Security Guide“ pakutud soovituste järgimisest:

- Määratlege poliitikasäte **Enforce password history** (Jõusta parooliajalugu), et süsteem peaks meeles mitut varasemat parooli. Selle poliitikasätte puhul ei saa kasutajad parooli aegumisel uuesti valida sama parooli.

  Soovitatav säte: 24

- Määratlege poliitikasäte **Maximum password age** (Parooli maksimaalne vanus), et paroolid aeguksid nii sageli, kui see on kliendi keskkonnas vajalik.

  Soovitatav säte: 42 (vaikesäte) kuni 90.

- Määratlege poliitikasäte **Minimum password age** (Parooli minimaalne vanus), et paroole ei saaks muuta enne teatud arvu päevade möödumist parooli seadmisest. See poliitikasäte töötab koos poliitikasättega **Enforce password history** (Jõusta parooliajalugu). Kui parooli minimaalne vanus on määratletud, ei saa kasutajad oma algse parooli kasutamiseks parooli korduvalt muuta ja sel moel vältida poliitikasätet **Enforce password history**. Kasutajad peavad parooli muutmiseks määratud arvu päevi ootama.

  Soovitatav säte: 2.

- Määratlege paroolisäte **Minimum password length** (Parooli miinimumpikkus), et parool koosneks vähemalt määratud arvul märkidest. Pikad paroolid (seitse märki või rohkem) on enamasti lühikestest paroolidest tugevamad. Selle poliitikasätte kehtimisel ei saa kasutajad valida tühja parooli, vaid peavad looma parooli, mille pikkus on vähemalt määratud arv märke.
  Soovitatav säte: 8.
- Lubage poliitikasäte **Password must meet complexity requirements** (Parool peab vastama keerukusnõuetele). Selle poliitikasätte puhul kontrollitakse kõiki uusi paroole, veendumaks, et need vastavad tugeva parooli põhinõuetele. Säte tagab, et parool sisaldaks vähemalt kolme märki neljast kategooriast (suurtähed, väiketähed, numbrid, mittetärgilised märgid), kuid mitte ühtegi osa kasutajanimest ega kasutaja ees- või perekonnanimest.

  Märkus
  Neile nõuetele vastavad paroolid pole tingimata väga tugevad. Kõigile nimetatud nõuetele vastab näiteks parool „Parool1“.

  Soovitatav säte: Yes (Jah).
- Nõuete täieliku loendi leiate Windowsi serverite elektroonilise spikri (Help) peatükist „Password Must Meet Complexity Requirements“ (Parool peab vastama keerukusnõuetele).
- Store passwords using reversible encryption (Talletage paroolid pöördkrüptimise abil) – pöördkrüptimist kasutatakse süsteemides, kus rakendus vajab juurdepääsu tekstilistele paroolidele. Enamiku juurutuste puhul pole seda vaja.

  Soovitatav säte: No (Ei).

Lisateavet leiate Windows Server 2003 juhendist „Security Guide“:

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

Konto väljalukustamise poliitika määratlemine

Konto väljalukustamise poliitika määratlemisel olge ettevaatlik. Konto väljalukustamise poliitikat ei tohiks kunagi kasutada väikeettevõttes, kuna sel juhul võidakse välja lukustada volitatud kasutajad, mis võib teie kliendile väga kulukaks minna.

Kui klient otsustab konto väljalukustamise poliitikat kasutada, seadke **Account lockout threshold policy** (Konto väljalukustamise läve poliitika) sätte väärtus piisavalt kõrgeks, et volitatud kasutajaid ei lukustataks kasutajakontost välja üksnes seetõttu, et nad tipivad parooli mitu korda valesti.

Lisateavet konto väljalukustamise poliitika kohta leiate Windowsi serverite elektroonilisest spikri (Help) peatükist „Account Lockout Policy Overview“ (Konto väljalukustamise poliitika ülevaade).

Konto väljalukustamise poliitika rakendamise või muutmise kohta leiate lisateavet Windowsi serverite elektroonilise spikri peatükist „To Apply or Modify Account Lockout Policy“ (Konto väljalukustamise poliitika rakendamine või muutmine).

Pääsujuhtimine

Windowsi võrgu ja ressursside (sh. Navision) turvaliseks muutmisel tuleks kindlasti arvesse võtta seda, millised õigused on kasutajatel, kasutajarühmadel ja teistel arvutitel võrgus. Ühe või mitme arvuti turvamiseks saate anda kasutajatele või rühmadele kindlaid kasutusõigusi. Objekti (nt. faili või kausta) turvamiseks võite sellele määrata õigused, mis lubavad kasutajatel või rühmadel selle objektiga teha üksnes kindlaid toiminguid. Pääsujuhtimise põhilised mõisted on:

- õigused;
- objektide omandistaatus;
- õiguste pärimine;
- kasutusõigused;
- objekti auditeerimine.

Õigused

Õigustega saab määratleda, milline juurdepääs on kasutajal või rühmal objektile või objekti atribuudile (nt. failid, kaustad ja registriobjektid). Õigusi rakendatakse mis tahes turvatud objektidele (nt. failid või registriobjektid). Õigusi saab anda igale kasutajale, rühmale või arvutile. Hea tava on anda õigusi rühmadele.

Objektide omandistaatus

Objekti loomisel määratakse objektile omanik. Windows 2000 Serveris on vaikimisi omanik objekti looja. Windows Server 2003 puhul pole see enam nii, kui objektide looja on mõni rühma Administrators (Ülemad) liige.

Kui mõni ülemarühma liige loob opsüsteemis Windows Server 2003 objekti, siis saab selle objekti omanikuks rühm Administrators, mitte objekti loonud isiku konto eraldi. Seda saab muuta kohalike turvasätete (Local Security Settings) lisandmooduli Microsoft Management Console (MMC) kaudu, kasutades sätet **System objects: Default owner for objects created by members of the Administrators group** (Süsteemiobjektid: ülemarühma liikmete loodud objektide vaikeomanik). Sõltumata sellest, mis õigused on objektile antud, saab objekti omanik alati objekti õigusi muuta.

Lisateavet leiate Windowsi serverite elektroonilise spikri (Help) peatükist „Ownership“ (Omandistaatus).

Õiguste pärimine

Pärimise abil saab süsteemiülem õigusi hõlpsasti määrata ja hallata. Selle funktsiooni kasutamisel pärivad ühte ümbrisesse kuuluvad objektid automaatselt kõik selle ümbrise päritavad õigused. Kui näiteks loote kaustas faile, pärivad need failid kõik selle kausta õigused. Pärida saab ainult päritavaks märgitud õigusi.

Kasutusõigused

Kasutusõigused annavad teie arvutikeskkonna kasutajatele ja rühmadele kindlaid sisselogimis- ja muud õigused.

Lisateavet kasutusõiguste kohta leiate Windowsi serverite elektroonilise spikri (Help) peatükist „User Rights“ (Kasutusõigused).

Objekti auditeerimine

Saate auditeerida kasutajate juurdepääsu objektidele. Neid turvalisusega seotud sündmusi saab sündmustevaaturi (Event Viewer) kaudu vaadata turvalisuselogist.

Lisateavet leiate Windows Serveri elektroonilise spikri (Help) peatükist „Auditing“ (Auditeerimine).

Pääsujuhtimise parimad tavad

- Määrake õigusi rühmadele, mitte kasutajatele. Kuna kasutajakontosid otse hallata pole kuigi tõhus, peaks kasutajapõhine õiguste määramine olema erand, mitte reegel.
- Teatud erijuhtumite puhul kasutage õiguste keelamist (Deny permissions). Näiteks saate õiguste keelamise abil välistada sellise rühma alamrühma, millel on õigused lubatud (Allow permissions).
- Ärge kunagi keelake objektile juurdepääsu rühma Everyone (Kõik) jaoks. Kui keelate kõigi kasutajate juurdepääsu objektile, hõlmab see ka süsteemiülemaid. Parem lahendus oleks rühm Everyone eemaldada, andes objektile juurdepääsu õiguse mõnele muule kasutajale, rühmale või arvutile. Pidage meeles, et kui õigusi pole määratletud, siis pole juurdepääsu antud.
- Määrake objekti õigused puus võimalikult kõrgel tasemel ja rakendage seejärel pärilikkus, et levitada turvasätteid kogu puu ulatuses. Pääsujuhtimise sätteid saab siis kiiresti ja tõhusalt rakendada kõigile emaobjekti tütardele või alampuule. Nii saate kõige väiksema vaevaga avaldada kõige rohkem mõju. Määratavad õigusesätted peaksid olema piisavad enamiku kasutajate, rühmade ja arvutite jaoks.
- Otse antud õigused võivad vahel päritud õigused alistada. Päritud õiguste keelamine ei takista juurdepääsu objektile, kui objekti puhul on olemas otsene õiguse lubamise (Allow permission) kanne. Otsesed õigused alistavad mis tahes päritud õigused (ka päritud õiguste keelamised).
- Active Directory® objektide õigustega töötades veenduge, et olete aru saanud Active Directory objektide puhul kehtivatest parimatest tavadest.

Lisateavet leiate Windows Server 2003 elektroonilise spikri (Help) peatükist „Best Practices for Assigning Permissions on Active Directory Objects“ (Active Directory objektide õiguste määramise parimad tavad).

Väline tulemüür

Tulemüür on riistvaraline või tarkvaraline vahend, mis takistab andmepakettidel määratud võrku siseneda või võrgust lahkuda. Liiklusvoo juhtimiseks avatakse või suletakse tulemüüri pordid andmepakettidele. Tulemüür jälgib iga andmepaketi puhul mitut teabekildu: protokolli, mille

kaudu paketti edastatakse, paketi sihtkohta või saatjat, paketi sisu tüüpi ja selle pordi numbrit, kuhu pakett saadetakse. Kui tulemüür on konfigureeritud aktsepteerima määratud protokolli edastamist sihtpordi kaudu, lubatakse pakett läbi. Microsoft Windows Small Business Server 2003 Premium Edition tarnitakse tulemüürilahendusega Microsoft Internet Security and Acceleration (ISA) Server 2000. Tulemüüri sisaldab ka Small Business Server Standard Edition.

ISA Server 2004

Internet Security and Acceleration (ISA) Server 2000 suunab turvaliselt taotluste ja vastuste liikumist Interneti ning sisevõrgus asuvate klientarvutite vahel.

ISA Server toimib kohalikku võrku ühendatud klientide jaoks turvalise lüüsina Internetti. ISA Serveri arvuti on teistele sideteel asuvatele osapooltele läbipaistev. Interneti-kasutaja ei tohiks aru saada, et võrgus on tulemüüriserver, välja arvatud juhul, kui kasutaja proovib pääseda juurde sellisele teenusele või minna saidile, millele ISA Serveri arvuti on juurdepääsu keelanud. Interneti-server, millele kasutaja proovib juurde pääseda, tõlgendab ISA Serveri arvuti taotlusi klientrakendusest pärinevate taotlustena.

Kui valite IP (Internet Protocol) fragmendifiltreerimise, lubate veebi puhverserveri ja tulemüüriteenustel paketifragmente filtreerida. Paketifragmentide filtreerimisel jäetakse kõik killustatud ehk fragmenditud IP-paketid kõrvale. Üks levinud „rünnakuviis“ hõlmab fragmenditud pakettide saatmist ja seejärel uuesti kokkupanemist moel, mis võib süsteemi kahjustada.

ISA Server sisaldab rünnakute avastamiseks mehhanismi, mis tuvastab võrgu ründamise katse kellaaja ja teostab rünnaku puhul konfigureeritud toimingute (või häirete) jada.

Kui ISA Serveri arvutisse on installitud teenus IIS (Internet Information Services), peate selle konfigureerima nii, et see ei kasutaks samu porte, mida ISA Server kasutab väljaminevate veebitaotluste (vaikimisi 8080) ja sissetulevate veebitaotluste (vaikimisi 80) jaoks. Näiteks võite seada IIS-i jälgima porti 81 ning konfigureerida siis ISA Serveri arvuti suunama sissetulevad veebitaotlused selle kohaliku arvuti porti 81, kus IIS töötab.

Kui ISA Serveri ja IIS-i kasutatavate portide vahel tekib konflikte, peatab installiprogramm IIS-i avaldamisteenuse. Seejärel saate panna IIS-i jälgima mõnda muud porti ning IIS-i avaldamisteenuse taaskäivitada.

ISA Serveri poliitikad

Võite määratleda ISA Serveri poliitika, mis juhib juurdepääsu nii sissetuleval kui ka väljamineval suunal. Saidi- ja kohareeglite abil saab määrata, millistele saitidele ja sisule on juurdepääs olemas. Protokollireeglid näitavad, kas konkreetsel protokollil on juurdepääs nii sissetuleva kui ka väljamineva liikluse jaoks.

Saate luua saidi- ja sisureegleid, protokollireegleid, veebiavaldamisreegleid ja IP-pakettide filtreid. Need poliitikad määratlevad, kuidas ISA Serveri kliendid suhtlevad Internetiga ja milline suhtlemine on lubatud.

Viirusetõrje

Arvutiviirus on täitmisfail, mis on loodud iseennast kopeerima, andmefaile ja programme kustutama või rikkuma ning tuvastamist vältima. Viirusi kirjutatakse sageli ringi ja kohandatakse, et neid ei saaks tuvastada. Sageli saadetakse viirusi meilimanusena. Viirusetõrjeprogramme tuleb pidevalt värskendada, et need oskaksid ära tunda nii uusi kui ka muudetud viirusi. Viirused on arvutite vastastes rünnakutes levinuim oht.

Viirusetõrjeprogrammid on loodud viirusprogrammide tuvastamiseks ja tõrjumiseks. Kuna uusi viirusprogramme luuakse pidevalt juurde, pakuvad paljud viirusetõrjeprogrammide tootjad klientidele tarkvara perioodilisi värskendusi. Microsoft soovitab viirusetõrjetarkvara kliendi võrgukeskkonnas kindlasti kasutusele võtta.

Viirusetõrjetarkvara installitakse enamasti kolme kohta: kasutaja tööjaama, serverisse ja võrku, kuhu saabub (ja kust vahel ka välja saadetakse) organisatsiooni e-post.

Viirusetüübid

Arvutisüsteeme nakatavaid viirusi on kolme põhitüüpi: buutsektori viirused, faile nakatavad viirused ja Trooja hobused.

Buutsektori viirused

Kui arvuti käivitub, skannib see enne operatsioonisüsteemi või muude käivitusfailide laadimist esmalt kõvaketta buutsektorit. Buutsektori viirus asendab kõvaketta buutsektoris oleva teabe oma koodiga. Kui arvuti on nakatunud buutsektori viirusega, loetakse viiruse kood mällu enne kõike muud. Kui viirus on mällu loetud, võib see end paljundada muudele nakatunud arvutis kasutatavatele ketastele.

Faile nakatavad viirused

Levinuim viirusetüüp on faile nakatav viirus, mis kinnitub täitmisfaili külge, lisades oma koodi täitmisfailile. Viiruse kood lisatakse enamasti nii, et seda on võimatu tuvastada. Nakatatud faili käivitamisel võib viirus end ka teiste täitmisfailide külge kinnitada. Seda tüüpi viirusega nakatunud failide nimelaiend on tavaliselt .com, .exe või.sys.

Mõni faile nakatav viirus on loodud kindlate programmide jaoks. Programmitüübid, mida enamasti võetakse sihikule, on ülekattefailid (.ovl) ja DLL-failid. Ehkki neid faile ei käitata, kutsuvad täitmisfailid neid. Viirus edastatakse kutse loomisel.

Andmete kahjustamine leiab aset viiruse vallandamisel. Viirus võidakse vallandada nakatunud faili käivitamisel või mõne kindla keskkonnasätte (nt. kindel süsteemikuupäev) vastamisel teatud tingimusele.

Trooja hobused

Trooja hobune pole tegelikult viirus. Põhierinevus viiruse ja Trooja hobuse vahel on selles, et Trooja hobune ei paljunda ennast, vaid üksnes hävitab kõvakettal olevat teavet. Trooja hobune võib end maskeerida igati tavaliseks programmiks, näiteks mänguks või utiliidiks. Käitamisel võib see aga andmeid hävitada või rikkuda.

Viirusetõrje parimad tavad

Makroviiruse levikut saab tõkestada. Jagage oma klientidega järgmisi näpunäiteid nakatumise vältimiseks:

- Installige viirusetõrjelahendus, mis skannib Internetist saabuvaid sõnumeid juba enne seda, kui sõnumid läbivad marsruuteri. See tagab e-kirjade kontrolli teadaolevate viiruste osas.
- Tehke kindlaks sissetulevate dokumentide päritolu. Dokumente tohiks avada ainult juhul, kui nende saatja on kliendi hinnangul usaldusväärne isik.
- Rääkige dokumendi loonud inimesega. Kui kasutajatel on dokumendi turvalisuse osas vähimaidki kõhklusi, peaksid nad pöörduma dokumendi loonud isiku poole.
- Kasutage Microsoft Office'i makroviiruste vastast kaitset. Office'is teavitavad rakendused kasutajat, kui dokument sisaldab makrosid. See funktsioon võimaldab kasutajal makrod dokumendi avamisel lubada või keelata.
- Kasutage makroviiruste tuvastamiseks ja eemaldamiseks viirusetõrjetarkvara. Viirusetõrjetarkvara oskab makroviirusi dokumentides ära tunda ja sageli ka eemaldada. Microsoft soovitab kasutada sellist viirusetõrjetarkvara, mis on saanud rahvusvahelise arvutiturvalisuse assotsiatsiooni ICSA (International Computer Security Association) sertifikaadi.

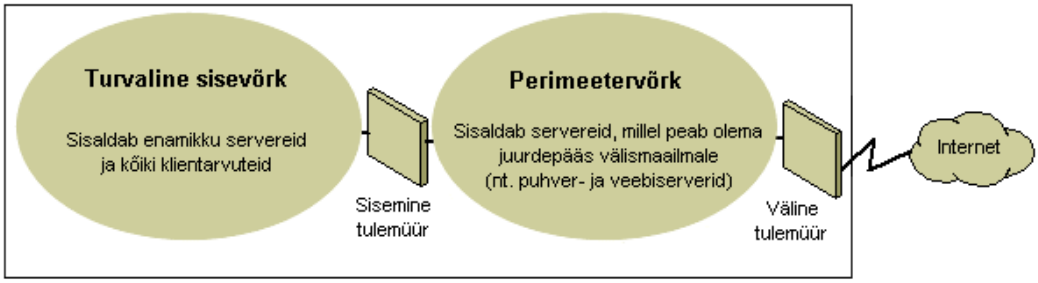
Viiruste ja arvutiturbe kohta lisateabe saamiseks külastage järgmisi Microsofti turvalisuse veebisaite:

- Microsofti turvalisus: http://www.microsoft.com/security/default.asp
- Turvalisusega seotud dokumendid Microsoft TechNetis: http://www.microsoft.com/technet/security/Default.mspx

Võrguturvalisuse strateegiad

Kuna IP-Internetivõrgu keskkonna tehniline lahendus ja juurutamine nõuavad kompromissi leidmist privaat- ning avalike võrkude vajaduste, on tulemüürist saanud võrgutervikluse turvamisel võtmetegureid. Tulemüür pole üksikkomponent. USA arvutiturvalisuse assotsiatsioon (NCSA – National Computer Security Association) määratleb tulemüüri „süsteemina või süsteemide kombinatsioonina, mis jõustab kahe või enama võrgu vahelise piiri". Ehkki kasutusel on mitmesuguseid mõisteid, nimetatakse seda piiri sageli perimeetervõrguks. Perimeetervõrk kaitseb teie sisevõrku või ettevõtte kohtvõrku (LAN) sissetungijate eest, kontrollides juurdepääsu Internetist või muudest suurtest võrkudest.

Järgmine diagramm kujutab tulemüüridega ümbritsetud perimeetervõrku, mis on privaatvõrgu kaitsmiseks paigutatud privaatvõrgu ja Interneti vahele:



Elementaarne perimeetervõrk

Organisatsioonid kasutavad tulemüüre turvalisuse tagamisel erinevalt. IP-pakettide filtreerimine pakub nõrka turvalisust, selle haldamine on kohmakas ja sissetungijad saavad sellest hõlpsasti jagu. Rakenduselüüsid on paketifiltritest turvalisemad ja neid on hõlpsam hallata, kuna need keskenduvad üksnes mõnele konkreetsele rakendusele (nt. kindel e-posti süsteem). Kontuurilüüsid on tõhusaimad juhul, kui võrgurakenduse kasutaja on turvalisuse seisukohalt olulisem kui rakenduse edastatavad andmed. Puhverserver on mitmekülgne turvatööriist, mis hõlmab rakenduselüüsi, turvalist juurdepääsu anonüümsete kasutajate jaoks ning muid teenuseid. Järgnevalt antakse neist võimalustest täpsem ülevaade:

- **IP-pakettide filtreerimine**
  IP-pakettide filtreerimine oli tulemüüritehnoloogia kõige varem kasutusele võetud funktsioon. Pakettide päiseid kontrollitakse, otsides neist lähte- ja sihtaadressi, TCP- ja UDP-portide numbreid ning muud teavet. Pakettide filtreerimine on piiratud võimalustega tehnoloogia, mis toimib kõige paremini selge turvalisuse keskkonnas, kus näiteks usaldatakse kõike perimeetervõrgu raamidesse jäävat ning ei usaldata mitte midagi, mis jääb perimeetervõrgust väljapoole. Viimastel aastatel on erinevad tootjad pakettide filtreerimise meetodit täiustanud, lisades paketifiltreerimistuumale intelligentseid, ise otsuseid vastuvõtvaid funktsioone, luues sel moel uue paketifiltreerimise vormi nimega *olekukohane protokollikontroll* („stateful protocol inspection“). Saate paketifiltreerimist konfigureerida näiteks nii, et vastu võetaks kindlat tüüpi pakette, ülejäänud aga keelataks, või keelataks kindlad tüüpi paketid ja lubataks kõik ülejäänud.
- **Rakenduselüüsid**
  Rakenduselüüse kasutatakse juhul, kui suurimat turvalisusemuret valmistab rakenduse tegelik sisu. See, et rakenduselüüsid on rakendusekohased, on ühtaegu nii nende tugev kui ka nõrk külg, kuna neid pole kerge tehnoloogia muudatustega kohandada.
- **Kontuurilüüsid**
  Kontuurilüüsid on tulemüüri ehitatud tunnelid, mis ühendavad ühel pool tulemüüri asuvaid kindlaid protsesse või süsteeme teisel pool asuvate kindlate protsesside või süsteemidega. Kontuurilüüse on kõige parem kasutada juhul, kui rakendust kasutav isik on potentsiaalselt suurem turvarisk kui rakenduse edastatav teave. Kontuurilüüs erineb paketifiltrist selle poolest, et oskab luua ühendust ka väljaspool riba asuva rakenduseskeemiga, mis võib lisada täiendavat teavet.
- **Puhverserverid**
  Puhverserverid on mitmekülgsed turvalisusetööriistad, mis hõlmavad kohtvõrgu ja Interneti vahelist liiklust haldavaid tulemüüri ning rakenduselüüsi funktsioone. Samuti pakuvad puhverserverid võimalust dokumente vahemällu talletada ning juurdepääsu kontrollida. Puhverserver võib jõudlust parandada sageli taotletavate andmete (nt. populaarse veebilehe) vahemällu talletamise ja otse kasutajatele pakkumisega.

Samuti oskab puhverserver filtreerida ja tagasi lükata taotlusi, mida omanik ei pea sobivaks (nt. volitamata kasutaja taotlus kellelegi teisele kuuluvatele failidele juurdepääsuks).

Veenduge, et klient kasutaks ära neid tulemüüri turvalisusefunktsioone, millest talle on abi. Paigutage perimeetervõrk võrgutopoloogias kohta, kus kogu väljaspoolt ettevõtte võrku saabuv liiklus peab läbima välise tulemüüri hallatava perimeetri. Tulemüüri juurdepääsuõigusi saab vastavalt kliendi vajadustele täpselt kohandada. Samuti saab tulemüüre konfigureerida nii, et need teataksid kõigist loata juurdepääsukatsetest.

Et nende portide arv, mida peate sisemises tulemüüris lahti hoidma, oleks võimalikult väike, võite kasutada mõnda rakenduskihi tulemüüri (nt. ISA Server 2000).

Lisateavet TCP/IP kohta vt. artiklist „Designing a TCP/IP Network“ („TCP-IP-võrgu loomine“) aadressil:
http://www.microsoft.com/resources/documentation/WindowsServ/2003/all/deployguide/en-us/dnsbb_tcp_overview.asp

Traadita võrgud

Vaikimisi on traadita võrgud konfigureeritud nii, et traadita signaale saab pealt kuulata. Traadita side riistvara vaikesätete, traadita võrkude pakutava juurdepääsetavuse ning praeguste krüptimismeetodite tõttu võivad need olla pahatahtlikele sissetungijatele haavatavad. Olemas on pealtkuulamise eest kaitsvaid konfiguratsioonivõimalusi ja tööriistu, kuid need ei kaitse arvuteid Interneti-ühenduse kaudu sissetungivate häkkerite ega viiruste eest. Seetõttu on äärmiselt oluline, et arvutite Interneti kaudu sissetungijate eest kaitsmiseks kaasataks võrku tulemüür.

Lisateavet traadita võrgu kaitsmise kohta leiate ingliskeelsest artiklist „How to Make Your 802.11b Wireless Home Network More Secure“ (802.11b traadita koduvõrgu turvalisemaks muutmine) aadressil:
http://support.microsoft.com/default.aspx?scid=kb;en-us;309369

Võrguturvalisuse stsenaariumid

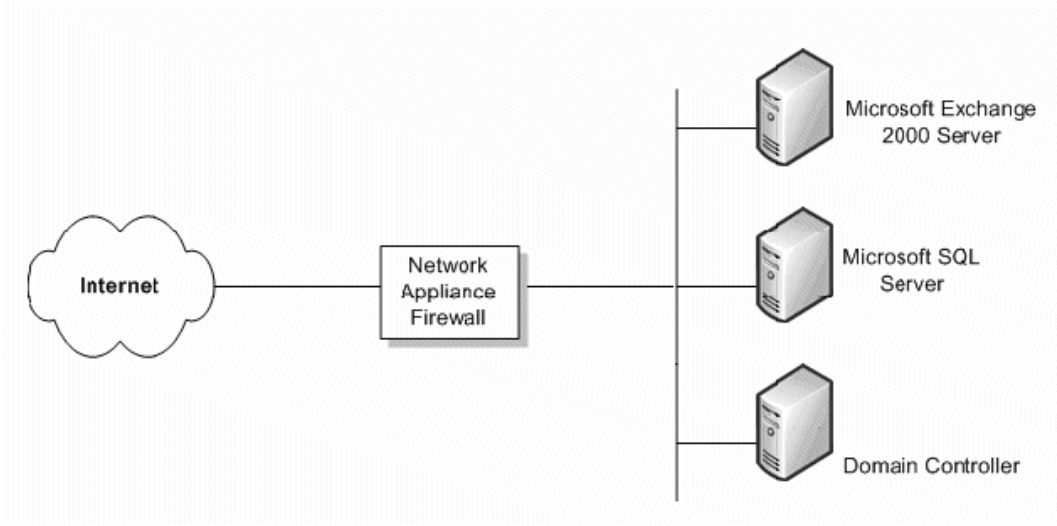
Kliendi organisatsioonis nõutava võrguturvalisuse tase sõltub mitmest tegurist. Enamasti tuleb leida kompromisslahendus eelarve ning ettevõtte andmete kaitstuna hoidmise vahel. Väikeettevõttel võib olla kasutusel vägagi keeruka ülesehitusega turve, mis pakub kõrgeimat võimalikku võrguturvalisuse taset, kuid väikeettevõttel ei pruugi sellise turvalisusetaseme jaoks raha olla. Selles lõigus anname ülevaate neljast stsenaariumist ning jagame soovitusi erineval tasemel turvalisuse pakkumiseks.

Tulemüür puudub

Kui teie kliendil on Interneti-ühendus, kuid tulemüür puudub, tuleb kasutusele võtta mõni võrguturvalisuse meede. Olemas on lihtsaid võrgutulemüürirakendusi, mis pakuvad enamiku algajate häkkerite eemalhoidmiseks piisaval tasemel turvalisust.

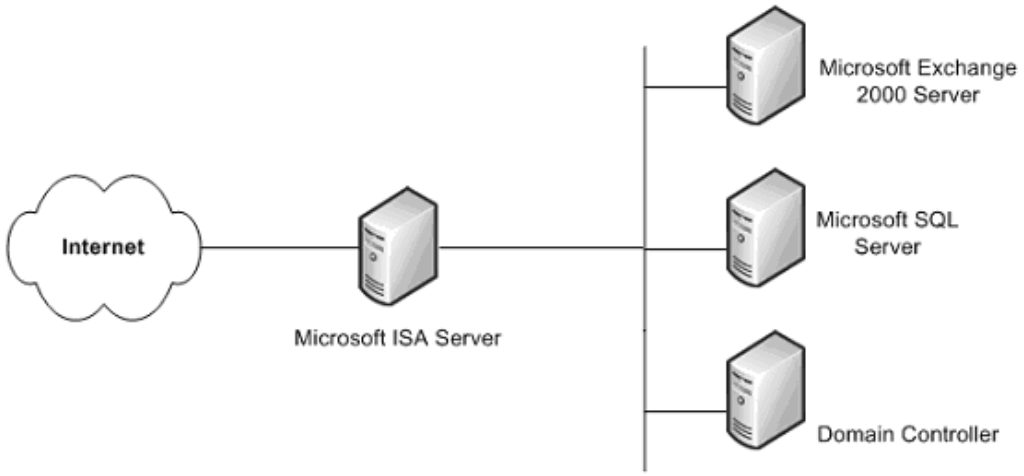
Üks lihtne tulemüür

Minimaalne soovitatav turvalisusetase nõuab ühte tulemüüri Interneti ja teie kliendi andmete vahel. See tulemüür ei pruugi pakkuda täiustatud turvalisust ning seda ei tohiks pidada eriti turvaliseks. Kuid ka see on parem kui mitte midagi.



Lihtne tulemüür

Loodetavasti võimaldab kliendi eelarve võtta eelarve andmete kaitsmiseks kasutusele mõne turvalisema lahenduse. Üks selline lahendus on ISA Server. Selle lisaserveriga kaasnevad küll kõrgemad kulud, kuid see pakub tavatarbijaile mõeldud tulemüürist märgatavalt paremat turvalisust, kuna tavatulemüürid pakuvad enamasti ainult võrguaadresside transleerimist (NAT – Network Address Translation) ja pakettide filtreerimist.



ISA Serveri tulemüür

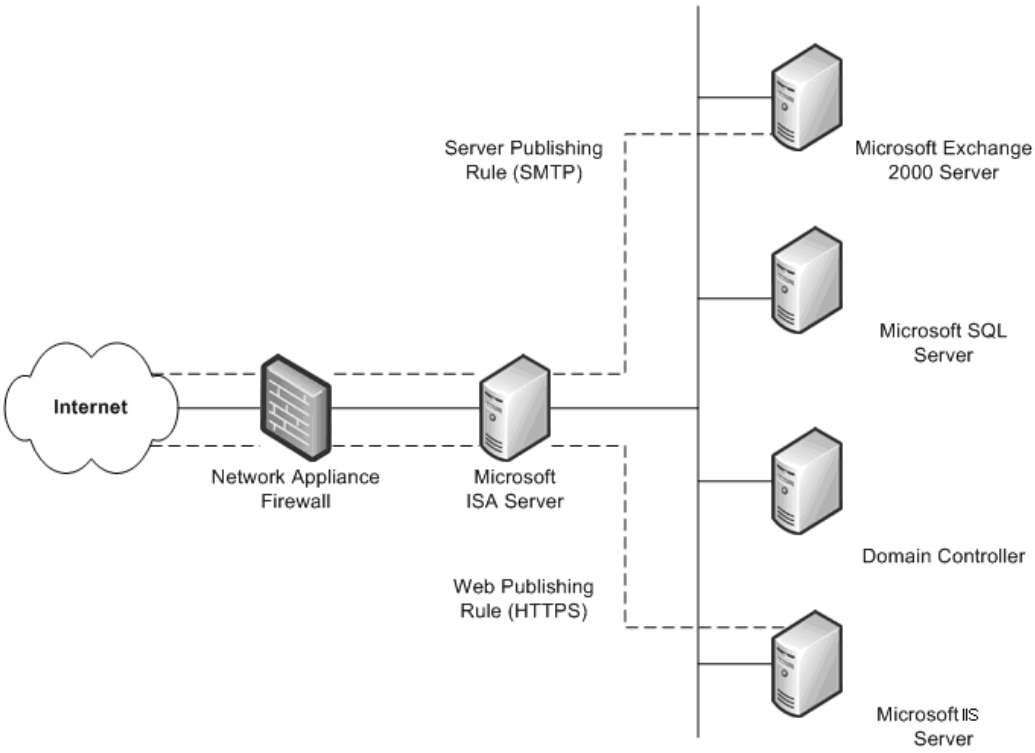
See ühe tulemüüriga lahendus on tunduvalt turvalisem algtaseme tulemüüri kasutamisest ning pakub Windowsi-kohaseid turvateenuseid.

Üks olemasolev tulemüür

Kui kliendil on sisevõrku Internetist eraldav tulemüür juba olemas, võiksite soovitada täiendavat tulemüüri, mis pakub mitmesuguseid võimalusi sisemiste Interneti-ressursside konfigureerimiseks.

Üks selline meetod on veebiavaldamine. See tähendab, et ettevõtte Interneti-kasutajatele juurdepääsu pakkuva veebiserveri ees võetakse kasutusele ISA Server. Sissetulevate veebitaotluste töötlemisel võib ISA Server jätta endast välismaailmale veebiserveri mulje, täites kliendi veebisisutaotlusi oma vahemälust. ISA Server edastab taotlused veebiserverile ainult siis, kui taotlusi ei saa tema vahemälust täita.

Teine võimalus on serveriavaldamine. ISA Server lubab sisemisi servereid Internetile avaldada ilma sisevõrgu turvalisust ohtu seadmata. Saate konfigureerida veebiavaldamise ja serveriavaldamise reegleid, mis määratlevad, millised taotlused tuleks saata kohaliku võrgu serverisse. See pakub sisemiste serverite jaoks täiendavat turvalisusekihti.

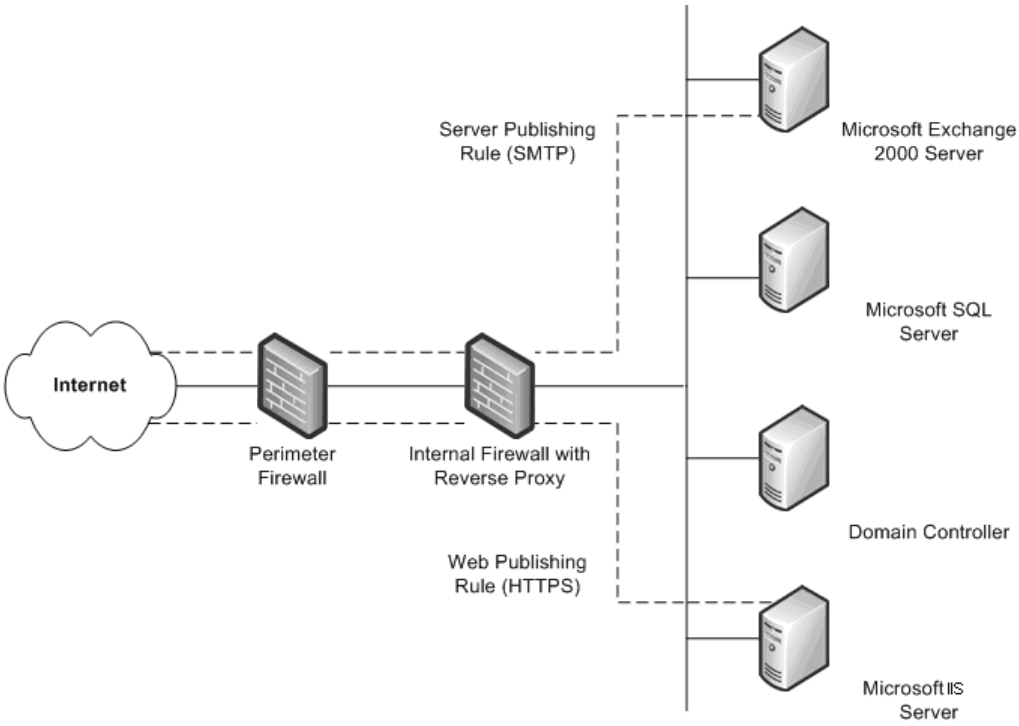


Olemasolev tulemüür, millele on lisatud ISA Server

Kaks olemasolevat tulemüüri

Neljanda stsenaariumi puhul on ettevõttes juba olemas kaks tulemüüri ning paika seatud perimeetervõrk (DMZ). Üks või mitu olemasolevat serverit pakub pöördpuhverteenuseid, et Interneti-kliendid ei pöörduks otse sisevõrgu serverite poole. Selle asemel püüab üks tulemüüridest (eelistatult sisemine

tulemüür) sisemistele serveritele suunatud võrgutaotlused kinni, analüüsib pakette ja edastab need siis Interneti-hosti asemel.



Kaks olemasolevat tulemüüri

See stsenaarium sarnaneb eelmise stsenaariumiga pärast teise tulemüüri lisamist. Ainus erinevus on selles, et pöördpuhverteenuseid osutav sisemine tulemüür pole ISA Server. Selle stsenaariumi puhul peaksite iga tulemüüri halduritega tihedat koostööd tegema, määratlemaks turvapoliitikale vastavad serveriavaldamisreeglid.

Turvapaikade haldamine

Operatsioonisüsteemid ja rakendused on sageli äärmiselt keerukad. Nad võivad koosneda paljude programmeerijate kirjutatud miljonitest koodiridadest. Äärmiselt oluline on tagada, et tarkvara töötaks usaldusväärselt ega ohustaks IT-keskkonna turvalisust või stabiilsust. Probleemide minimeerimiseks testitakse tooteid enne avaldamist põhjalikult. Ründajad tegelevad aga järjekindlalt tarkvarast nõrkade kohtade otsimisega ning kõigi tulevaste rünnakute ettenägemine pole võimalik.

Paljudes organisatsioonides on paigahaldus osa üldisest muudatuste ja konfiguratsioonihalduse strateegiast. Ettevõtte iseloomust ja suurusest sõltumata on ülimalt oluline luua korralik paigahaldusstrateegia, ka siis, kui ettevõttes pole veel tõhusat muudatuste ja konfiguratsioonihaldust moodustatud. Enamik arvutisüsteemide suhtes edukalt toime pandud rünnakutest tehakse nende süsteemide vastu, kus pole turvapaiku installitud.

Turvapaiku peab tõsiselt võtma suurem osa organisatsioone. Kui tarkvaras on leitud nõrk koht, jagavad ründajad selle kohta teavet kiiresti ka teistele häkkeritele. Kui nõrk koht on leitud Microsofti tarkvaras, püüab Microsoft

turvapaiga välja anda võimalikult kiiresti. Paiga installimiseni võib turvalisus, millest klient sõltub ja mida eeldab, olla loodetust tunduvalt nõrgem.

Navisioni keskkonnas peate tagama, et teie klientidel oleks värskeimad turvapaigad installitud kogu süsteemis. Veenduge, et klient kasutaks ühte Microsofti pakutavatest võimalustest. Need on järgmised:

- **Microsofti turvateatiste teenus**
  Turvateatiste teenus (Security Notification Service) on meililoend, mis teavitab kasutajaid uutest värskendustest. Need teatised on väärtuslik osa proaktiivsest turvalisusestrateegiast. Teatised on saadaval ka TechNeti tooteturvalisuse teatiste veebisaidil: http://www.microsoft.com/technet/security/bulletin/notify.mspx
- **Microsofti automaatvärskendused**
  Windows võib turvavärskendusi automaatselt arvutitesse installida.
- **Microsofti turvabülletääni otsingutööriist**
  Turvabülletäänide (Security Bulletin) otsingutööriist on saadaval turvabülletäänide veebisaidil: http://www.microsoft.com/technet/security/current.aspx. Klient saab otsustada, milliseid värskendusi ta vajab, võttes aluseks praegu kasutatava operatsioonisüsteemi, rakendused ja juba installitud hoolduspaketid.
- **Microsofti turvaanalüüsi vahend (MBSA – Microsoft Baseline Security Analyzer)**
  See graafiline tööriist on saadaval Microsofti turvaanalüüsi vahendi veebisaidil: http://www.microsoft.com/technet/security/tools/mbsahome.mspx. See tööriist võrdleb arvuti praegust olekut Microsofti hallatava värskendusteloendiga. Samuti teeb MBSA elementaarseid turvakontrolle, kontrollides muu hulgas paroolide tugevuse ja aegumise sätteid ning külalisekontode poliitikat. MBSA otsib ka haavatavusi järgmistes süsteemides: Microsoft Internet Information Services (IIS), SQL Server™ 2000, Exchange 5.5, Exchange 2000 ja Exchange Server 2003.
- **Microsofti tarkvaravärskendusteenused (SUS – Software Update Services)**
  See varem Windows Update'i ettevõtete väljaandena (Windows Update Corporate Edition) tuntud tööriist võimaldab ettevõtetel kõiki Windows Update'i avalikul veebisaidil saadaolevaid kriitilisi värskendusi ja turvapakette (SRP) kohalikes arvutites majutada. See tööriist moodustab üheskoos automaatvärskenduste (AU) klientide uue väljalaskega võimsa automaatse allalaadimis- ja installistrateegia aluse. Uus AU-kliendi komplekt hõlmab operatsioonisüsteemide Windows 2000 ja Windows Server 2003 klienti ning oskab allalaaditud värskendusi automaatselt installida. Lisateavet Microsoft SUS-i kohta leiate veebisaidilt:
  http://www.microsoft.com/windows2000/windowsupdate/sus/default.asp
- **Microsoft Systems Management Serveri (SMS) tarkvaravärskendusteenuste funktsioonipakett**
  SMS-i tarkvaravärskendusteenuste funktsioonipakett sisaldab tööriistu, mis on mõeldud tarkvaravärskenduste kogu ettevõttes kasutusele võtmise protsessi hõlbustamiseks. Nende tööriistade seas on turvavärskenduste inventuuririist (Security Update Inventory Tool), Microsoft Office'i värskenduste inventuuririist, tarkvaravärskenduste levitamise viisard (Distribute Software Updates Wizard) ning SMS-veebiaruandlusriist (SMS Web Reporting Tool) koos veebiaruannete lisandmooduliga tarkvaravärskenduste jaoks. Kõigi nende tööriistade kohta leiate lisateavet aadressilt:
  http://www.microsoft.com/smserver/downloads/20/featurepacks/suspack/

Rääkige oma kliendiga neist tööriistadest ja soovitage need kasutusele võtta. Turvaprobleemidele tuleb tähelepanu pöörata nii ruttu kui võimalik, võttes samas arvesse keskkonna stabiilsuse säilitamist.

SQL Server 2000 turvasätted

Kuna Navision töötab ka SQL Server 2000 peal, peate kindlasti kasutusele võtma meetmed kliendi SQL Server 2000 installi turvalisuse parandamiseks. SQL Serveri turvalisust aitavad parandada järgmised toimingud:

- Veenduge, et installitud oleks operatsioonisüsteemi värskeim versioon ning kõik SQL Server 2000 hoolduspaketid ja värskendused. Uuemad üksikasjad leiate Microsofti turvalisuse veebisaidilt http://www.microsoft.com/security/default.asp
- Failisüsteemi taseme turvalisuse tagamiseks veenduge, et kõik SQL Server 2000 andme- ja süsteemifailid oleksid installitud NTFS-partitsioonidele. Failidele peaks NTFS-õiguste kaudu olema juurdepääs ainult haldus- või süsteemitaseme kasutajatele. See kaitseb faile kasutajate eest, kes proovivad neile juurde pääseda ajal, kui MSSQLSERVER-i teenus ei tööta.
- Kasutage SQL Server 2000 teenuse (MSSQLSERVER) jaoks väheste õigustega domeenikontot, näiteks NT Authority\Network Service'i kontot või LocalSystemi kontot (soovitatav). Sel kontol peaks domeenis olema minimaalselt õigusi ja see peaks aitama võimalikku serveri suhtes toime pandud rünnakut pidurdada (mitte peatada). Teisisõnu peaks sellel kontol olema domeenis ainult kohalikud kasutajataseme õigused. Kui SQL Server 2000 kasutab teenuste käitamiseks domeeniülema kontot, seab serveri turvalisuse ohtusattumine ohtu kogu domeeni turvalisuse. Selle sätte muutmiseks kasutage SQL Serveri ettevõttehaldurit (Enterprise Manager). Failide pääsujuhtimisloendeid (ACL – Access Control List), registrit ja kasutajate õigusi muudetakse automaatselt.
- Suurem osa SQL Server 2000 väljaandeid installitakse kahe vaikeandmebaasiga: **Northwind** ja **pubs**. Need on näidisandmebaasid, mida kasutatakse testimiseks, koolituseks ja üldnäidetena. Tootmissüsteemis ei tohiks neid kasutusele võtta. Kui potentsiaalne sissetungija teab, et need andmebaasid on kasutusel, võib ta proovida süsteemi rünnata, tuginedes nende andmebaaside vaikesätetele ja vaikekonfiguratsioonile. Kui **Northwind** ja **pubs** on tootmissüsteemi SQL Server 2000 arvutis olemas, tuleks need eemaldada.
- SQL Server 2000 süsteemi auditeerimine on vaikimisi keelatud, seega tingimusi ei auditeerita. Seetõttu on sissetungi keeruline tuvastada ning ründajatel on hõlpsam oma jälgi peita. Peaksite lubama vähemalt nurjunud logimiskatsete auditeerimise.

SQL Server 2000 värskeima turvateabe saamiseks külastage saiti http://www.microsoft.com/sql/techinfo/administration/2000/security/default.asp

Microsoft Business Solutions

Microsoft Business Solutions on Microsofti allüksus, mis pakub laias valikus kõikehõlmavaid integreeritud ärirakendusi ja teenuseid, mis aitavad väikestel, keskmise suurusega ja suurtel ettevõtetel klientide, töötajate, partnerite ning tarnijatega paremini suhelda. Microsoft Business Solutionsi rakendused optimeerivad strateegilisi äriprotsesse paljudes valdkondades, mille seas on finantsjuhtimine, analüüsimine, personalijuhtimine, projektijuhtimine, kliendisuhete haldus, teenindus- ja hooldushaldus, tarneketi juhtimine, e-äri ning tootmise ja jaemüügi juhtimine. Rakendused on loodud nii, et need aitaksid klientidel oma äritegevuses edu saavutada. Lisateavet Microsoft Business Solutionsi kohta leiate veebisaidil: http://www.microsoft.com/BusinessSolutions/