Microsoft Business Solutions

Navisionin suojausopas

Julkaistu lokakuussa 2004

Microsoft

Sisällysluettelo

Esittely

Microsoft® Windows® -käyttöjärjestelmä mahdollistaa kehittyneen, standardeihin perustuvan verkkosuojauksen. Laajimmillaan suojaukseen liittyy suunnittelu sekä hyvien ja huonojen puolien huomioon ottaminen. Tietokoneen voi esimerkiksi lukita holviin niin, että vain yksi järjestelmänvalvoja voi käyttää sitä. Tällöin tietokone on suojattu, mutta siitä ei ole juurikaan hyötyä, sillä sitä ei ole yhdistetty muihin tietokoneisiin. On selvitettävä, kuinka verkosta voi saada mahdollisimman suojatun käytettävyyttä unohtamatta.

Useimmat organisaatiot varautuvat ulkoisiin hyökkäyksiin ja käyttävät palomuureja. Monikaan yritys ei kuitenkaan ota huomioon sitä, millä tavalla suojausmurtoa voi lievittää, jos pahantahtoinen käyttäjä on päässyt palomuurin sisälle. Asiakasympäristön suojausmenetelmät toimivat hyvin, jos käyttäjien ei tarvitse suorittaa liian useita toimintoja ja vaiheita voidakseen tehdä töitään suojatusti. Suojauskäytäntöjen noudattamisen tulee olla käyttäjille mahdollisimman helppoa, jotta nämä eivät kehittelisi heikommin suojattuja menetelmiä asioiden hoitamiseksi.

Navision-asennusten koko voi vaihdella suuresti, joten on syytä harkita kunkin asiakkaan tarpeita ja punnita suojauksen tehokkuutta siihen mahdollisesti liittyvien kustannusten kannalta. Asiakkaiden luotettuna neuvonantajana velvollisuutesi on arvioida tilanteet mahdollisimman hyvin ja suositella käytäntöä, joka vastaa asiakkaan suojaustarpeisiin mutta ei kuitenkaan muodosta sellaista taakkaa, joka saisi asiakkaan lopettamaan käytännön noudattamisen.

Navision-suojauksen parhaat käytännöt

Seuraavien yleissääntöjen avulla voit tehostaa Navision-ympäristön suojausta:

- Jos haluat suorittaa Navision Database Serverin palveluna tai käyttää palvelimen käynnistykseen komentorivin parametria *installasservice*, varmista, että palvelu toimii NT Authority\Network Service -tilinä. NT Authority\Network Service -tili on vain Windows™ XP:ssä ja Windows Server™ 2003:ssa. Jos käytät Windows 2000 Serveriä, luo tili, jossa on palvelun vähimmäiskäyttöoikeudet. Muussa tapauksessa palvelulle määritetään paikallinen järjestelmätili. Luodulla tilillä tulee olla enintään samat oikeudet kuin tavallisella käyttäjätilillä, tai tilin tulee olla toimialuetili, joka ei ole järjestelmänvalvoja toimialueella tai missään paikallisessa tietokoneessa.

  Muista määrittää sille NT Authority\Network Service -tilille tai käyttäjätilille, jonka alaisuudessa palvelin toimii, tietokantatiedostojen luku- ja kirjoitusoikeudet, jotta käyttäjät voivat muodostaa yhteyden tietokantaan.

  Voit antaa NT Authority\Network Service -tilille tietokantatiedoston luku- ja kirjoitusoikeudet Windows XP:ssä seuraavasti:

  1. Siirry Resurssienhallinnassa kansioon, joka sisältää haluamasi tietokantatiedoston.
  2. Valitse tietokantatiedosto, napsauta sitä hiiren kakkospainikkeella ja valitse Ominaisuudet.
  3. Valitse ***Ominaisuudet***-ikkunassa ***Suojaus***-välilehti ja valitse **Ryhmä- tai käyttäjänimet -**kentässä Lisää.
  4. Kirjoita käyttäjien, tietokoneiden tai ryhmien valinnan valintaikkunan tekstikenttään *Verkkopalvelu* ja valitse OK.
  5. Järjestelmä lisää VERKKOPALVELU-kohteen ***Ominaisuudet***-ikkunan **Ryhmät tai käyttäjänimet -**kenttään.
  6. Valitse VERKKOPALVELU ja määritä sille **Käyttöoikeudet**-kentässä luku- ja kirjoitusoikeudet.
- Navision Application Server -palvelu toimii oletusarvon mukaan NT Authority\Network Service -tilinä, joten se voi käsitellä Navision Database Serveriä paikallisesti. Verkossa on kuitenkin varmistettava, että Navision Application Server -palvelu toimii Navision Database Serverin tunnistamana Windows-toimialatilinä, jos haluat palvelun voivan käyttää tietokantapalvelinta. Tilin ei tule olla toimialueen tai minkään paikallisen tietokoneen järjestelmänvalvoja.
- Jos käytät Navisionin SQL-palvelinvaihtoehtoa, Microsoft SQL Server™ toimii palveluna. Navisionin SQL-palvelinvaihtoehdon käyttäminen vaatii, että SQL Server voi hakea Active Directorysta Windows-käyttäjäryhmien luetteloita käyttöoikeuksien tarkistusta varten. On siis varmistettava, että SQL Server -palvelu toimii NT Authority\Network Service -tilinä.

  Voit varmistaa seuraavasti, että palvelu toimii NT Authority\Network Service -tilinä:

  1. Etsi SQL Server -tietokoneessa MSSQLSERVER-palvelu, napsauta sitä hiiren kakkospainikkeella ja valitse Ominaisuudet.
  2. Valitse ***Ominaisuudet***-ikkunassa ***Kirjautuminen***-välilehti.
  3. Valitse ***Kirjautuminen***-välilehden Kirjaudu nimellä -kohdassa Tili-vaihtoehto, valitse *NT Authority\NetworkService* ja valitse OK.

  Lisätietoja SQL Serverin suojauksesta on seuraavissa osoitteissa:

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

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

- Jos käytät Navisionin sähköisen kaupankäynnin tuotteita, kuten Commerce Gateway -sovellusta, varmista, että Commerce Gateway Request Server on asennettu oikein ja että käytössä on palveluiden oletustiliasetus. Oletustiliasetus on *CGRSUser*, ja se antaa Commerce Gateway Serverille käyttöoikeuden tämän tarvitsemien muiden palveluiden vähimmäisjoukkoon, johon kuuluvat muun muassa *MSSQLSERVER*- ja *BizTalk Service BizTalk Group: BizTalkServerApplication* -palvelu. Oletustiliasetus ei sisällä yleisiä tiliasetuksia toisin kuin paikallinen järjestelmätili.
- Käytä aina vahvoja salasanoja. Lisätietoa vahvoista salasanoista on kohdassa Vahvat salasanat.
- Käytä kirjautumisia Windowsiin. Navisionissa voi luoda kahdenlaisia kirjautumisia: kirjautumisia tietokantaan ja kirjautumisia Windowsiin. Suosittelemme kirjautumista Windowsiin, koska tällöin järjestelmä käyttää Windowsin käyttöoikeuksien tarkistusta ja mahdollistaa kunnollisen salasanakäytännön.
- Salasanoja ei pidä käyttää uudelleen. Usein samoja salasanoja käytetään eri järjestelmissä ja toimialueissa. Kahden toimialueen järjestelmänvalvoja saattaa esimerkiksi luoda toimialueen valvojan tilin molempiin toimialueisiin ja määrittää tileille saman salasanan. Hän saattaa jopa määrittää toimialueen tietokoneisiin paikallisen järjestelmänvalvojan salasanat, jotka ovat samoja koko toimialueella. Tällaisessa tilanteessa koko toimialueen suojaus murtuu, jos yhden tilin tai tietokoneen suojaus murtuu.
- Kun Navision on asennettu ja tietokannat on luotu tai päivitetty, luo kirjautuminen Windowsiin ja määritä sille Navisionissa tehokäyttäjän rooli. Tämä tehokäyttäjä hoitaa esimerkiksi tietokantojen hallinnan ja suojauksen. Määritä tälle kirjautumiselle vahva salasana. Salasana tulee pitää salassa. Sen tulee antaa sama suojaus kuin SA-salasanan SQL Serverissä. Tehokäyttäjän rooli hallitsee kaikkea tietokannan käsittelyä, joten se vaatii parhaan mahdollisen suojauksen. Tehokäyttäjän salasanan tulee olla vain järjestelmänvalvojien tiedossa.
- Kaikkien muiden Navision-tietokantaa käsittelevien käyttäjien tulee saada vähimmät mahdolliset oikeudet. Heille tulee siis määrittää Navisionissa roolit, joiden avulla he voivat käsitellä vain työssään tarvitsemiansa ominaisuuksia ja toimintoja.
- Varmista, että vain sellaiset henkilöt, joiden rooli yrityksessä vaatii sitä, voivat tuoda FOB-tiedostoja, suunnitella objekteja uudelleen ja palauttaa tietokantojen varmuuskopioita.
- Tee Navision-tietokannasta säännöllisesti varmuuskopioita ja muista testata varmuuskopiot, jotta niiden palauttaminen varmasti onnistuu tarvittaessa.
- Säilytä varmuuskopioita turvallisessa paikassa, jotta ne eivät joudu alttiiksi tulelle, savulle, pölylle, korkeille lämpötiloille, salamoille ja ympäristökatastrofeille (esimerkiksi maanjäristykselle).
- Navision toimii useissa Windows-versioissa, mutta suosittelemme uusimpien käyttöjärjestelmien käyttämistä niin, että uusimmat suojausominaisuudet on asennettu. Tällä hetkellä suositeltuja versioita ovat Windows XP, Service Pack 2 ja Windows Server 2003.
- Ota uusimmat suojauspäivitykset käyttöön käyttämällä Windows Update -palvelua, joka toimitetaan Windows 2000:n, Windows XP:n ja Windows Server 2003:n mukana. Pidä kaikki asiakastietokoneet ajan tasalla ja varmista Windowsin Automaattiset päivitykset -ominaisuuden avulla, että niissä on uusimmat suojauskorjaukset, Service Pack -paketit ja päivitykset.
- Suosittelemme Navision-asiakkaiden ja Navision Database Serverin välisessä tiedonvälityksessä käytettäväksi suojattua TCPS-yhteyskäytäntöä. TCPS on TCP/IP-yhteyskäytännön suojattu versio, joka käyttää salausta hyödyntävää SSPI (Security Support Provider Interface) -käyttöliittymää ja Kerberos-todennusta. TCPS on Navision Database Serverin oletusyhteyskäytäntö.

- Asiakkaalla tulee olla vakavia virhetilanteita varten selviytymissuunnitelma, jonka avulla palvelut voidaan nopeasti palauttaa virhetilanteen jälkeen. Selviytymissuunnitelman tulee sisältää seuraavat kohteet:
    - uusien tai väliaikaisten laitteiden hankkiminen
    - varmuuskopioiden palauttaminen uusiin järjestelmiin
    - selviytymissuunnitelman toiminnan varmistaminen testaamalla.

Fyysinen suojaus

Fyysinen suojaus on ehdottoman tärkeää, koska sitä ei mitenkään voi korvata ohjelmistosuojauksella. Jos esimerkiksi kiintolevyasema varastetaan, myös aseman sisältämät tiedot tulevat varastetuiksi. Ota seuraavat suojaukseen liittyvät asiat puheeksi asiakkaan kanssa, kun kehitätte suojausjärjestelmää:

- Jos suurissa asennuskohteissa on erillisiä tietotekniikan osastoja, tulee varmistua siitä, että palvelinhuoneet ja ohjelmistojen säilytyshuoneet ovat lukittuja.
- Tähän luokkaan kuuluvat seuraavat laitteet:
    - Microsoft SQL Server 2000 -palvelin
    - tiedostopalvelin, jossa suoritettavat Navision-tiedostot sijaitsevat.
- Asiattomia käyttäjiä ei tule päästää tietokoneiden ääreen.
- Varashälyttimet tulee asentaa tietojen luottamuksellisuuden tasosta riippumatta.
- Kriittisten tietojen varmuuskopiot tulee säilyttää muualla, ja varmuuskopiot tulee sijoittaa tulenkestäviin säilöihin.

Työntekijät

Kaikkien tuotteiden ja ominaisuuksien hallintaoikeuksia kannattaa rajoittaa. Asiakkaiden tulee oletusarvoisesti antaa työntekijöilleen vain lukuoikeus järjestelmätoimintoihin, elleivät työntekijät tarvitse laajempia oikeuksia töidensä suorittamista varten. Microsoft suosittelee vähimmäisoikeuksien periaatetta: käyttäjille tulee antaa vain ne vähimmäisoikeudet, joita he tarvitsevat tietojen ja toimintojen käsittelemiseksi.
Tyytymättömät ja entiset työntekijät ovat uhka verkon turvallisuudelle. Kun keskustelet suojauksesta asiakkaiden kanssa, suosittele seuraavaa työntekijöihin liittyvää käytäntöä:

- Tutki henkilön tausta ennen palkkaamista.
- Varaudu tyytymättömien työntekijöiden ja entisten työntekijöiden “kostoon”.
- Varmista, että työntekijän jättäessä työpaikan kaikki häneen liittyvät Windows-tilit ja salasanat poistetaan käytöstä. Älä poista käyttäjiä, jotta raportointi onnistuisi. Älä myöskään käytä tilejä uudelleen.
- Kouluta käyttäjät olemaan valppaita ja ilmoittamaan epäilyttävästä toiminnasta.
- Älä myönnä oikeuksia automaattisesti. Jos käyttäjät eivät tarvitse tiettyjen tietokoneiden, tietokonehuoneiden tai tiedostojoukkojen käyttömahdollisuutta, varmista, että heillä ei ole niiden käyttöoikeuksia.
- Kouluta järjestelmänvalvojat havaitsemaan mahdolliset työntekijöihin liittyvät ongelmat ja reagoimaan niihin.
- Varmista, että työntekijät ymmärtävät roolinsa verkon suojauksen ylläpidossa.

- Lähetä yrityksen käytännöt jokaiselle työntekijälle.
- Älä salli käyttäjien asentaa ohjelmistoa, joka ei ole työnantajan valtuuttama.

Järjestelmänvalvoja

Suosittelemme, että asiakkaan järjestelmänvalvojat ottavat käyttöön uusimmat Microsoftilta saatavilla olevat suojauskorjaukset. Hyökkääjät ovat erittäin taitavia yhdistämään pieniä virheitä, jotka lopulta mahdollistavat suuret hyökkäykset verkkoon. Järjestelmänvalvojien tulee ennen muuta varmistaa, että jokainen yksittäinen tietokone on mahdollisimman hyvin suojattu, minkä jälkeen järjestelmään tulee lisätä suojauspäivityksiä ja ottaa käyttöön virustentorjuntaohjelmisto. Tässä oppaassa on useita linkkejä ja resursseja, joiden avulla voit etsiä arvokkaita tietoja ja parhaita käytäntöjä.

Monimutkaisuus saattaa heikentää verkon suojausta. Mitä monimutkaisempi verkko on, sitä vaikeampaa se on suojata tai korjata, jos asiaton tunkeutuja on kerran päässyt sisään. Järjestelmänvalvojan tulee kirjata verkon rakenne kauttaaltaan ja pyrkiä pitämään rakenne mahdollisimman yksinkertaisena.

Suojaus liittyy ensisijaisesti riskienhallintaan. Tekniikka ei ole kaikkivoipaa, joten suojaukseen tarvitaan tekniikan ja käytäntöjen yhdistelmää. Saatavilla ei siis koskaan ole tuotetta, jonka voisi asentaa pakkauksestaan suoraan verkkoon ja joka takaisi välittömästi täydellisen suojauksen. Suojaus on tekniikan ja käytäntöjen yhdistelmä, eli tekniikan käyttäminen määrää sen, kuinka suojattu verkko on. Microsoftin tekniikoissa ja ominaisuuksissa suojaus on otettu huomioon, mutta vain järjestelmänvalvoja voi avullasi määrittää sopivat käytännöt kutakin organisaatiota varten. Ota suojaus huomioon jo asennuksen ja käyttöönoton varhaisissa vaiheissa. Selvitä, mitä kohteita asiakkaasi haluaa suojella ja mitä he ovat valmiita tekemään suojelun varmistamiseksi.

Kehitä lopuksi hätätilanteiden varalle toimintasuunnitelmia, ennen kuin hätätilanne todella ilmenee. Yhdistä perinpohjainen suunnittelu laadukkaaseen tekniikkaan, niin asiakkaan verkko on suojattu hyvin.

Lisätietoja suojauksesta on englanninkielisessä artikkelissa The Ten Immutable Laws of Security Administration osoitteessa http://www.microsoft.com/technet/archive/community/columns/security/essays/10salaws.mspx

sekä suojauksenhallintaan liittyvissä englanninkielisissä artikkeleissa osoitteessa http://www.microsoft.com/technet/community/columns/secmgmt/smarch.mspx

Palvelinkäyttöjärjestelmän suojaaminen

Pienillä asiakkailla ei ehkä ole palvelinkäyttöjärjestelmää. On kuitenkin tärkeää ymmärtää suojauksen parhaat käytännöt, jotta voit kertoa niistä suuremmille asiakkaille, joiden verkkoympäristö on pienasiakkaiden ympäristöä monimutkaisempi. Ota huomioon myös, että useita tässä asiakirjassa esitettyjä käytäntöjä voidaan helposti soveltaa sellaisiin asiakkaisiin, joilla on vain palvelinkäyttöjärjestelmät.

Tämän osion käsitteet liittyvät sekä Microsoft Windows 2000 Server- että Microsoft Windows Server 2003 -tuotteisiin, vaikka tiedot on otettu lähinnä Windows Server 2003:n käytönaikaisista ohjeista. Windows Server 2003:ssa on paljon suojausominaisuuksia. Windows Server 2003:n käytönaikaisissa ohjeissa on täydelliset tiedot kaikista suojausominaisuuksista ja -käytännöistä.

Lisätietoja Windows 2000 Serveristä on Windows 2000 Server Security Center -sivustolla osoitteessa
http://www.microsoft.com/technet/security/prodtech/win2000/default.mspx.

Voit myös tutustua englanninkieliseen Windows 2000 Security Hardening Guide -oppaaseen osoitteessa
http://www.microsoft.com/technet/security/prodtech/win2000/win2khg/default.mspx

Lisätietoja Windows Server 2003 -palvelimesta on *Windows Server 2003 Security Guide* -oppaassa osoitteessa
http://www.microsoft.com/technet/security/prodtech/win2003/w2003hg/sgch00.mspx

Windows-palvelimien suojausmallin keskeisiä ominaisuuksia ovat käyttöoikeuksien todennus, käytönhallinta ja yksittäinen kirjautuminen:

- Käyttöoikeuksien todennuksessa järjestelmä tarkistaa käyttäjän henkilöllisyyden kirjautumistietojen perusteella. Käyttäjän nimeä ja salasanaa verrataan valtuutettuun luetteloon. Jos järjestelmä havaitsee vastaavuuden, käyttöoikeuksien todennus antaa käyttäjälle ne oikeudet, jotka hänelle on määritetty käyttöoikeusluettelossa.
- Käytönhallinta rajoittaa käyttäjien pääsyä tietoihin tai tietokoneresursseihin käyttäjien henkilöllisyyden ja ennalta määrättyihin ryhmiin kuulumisen perusteella. Järjestelmänvalvojat käyttävät usein käytönhallintaa määrittääkseen käyttäjien mahdollisuudet käyttää verkkoresursseja, kuten palvelimia, hakemistoja ja tiedostoja. Yleensä käyttäjille ja ryhmille myönnetään oikeudet käsitellä tiettyjä objekteja.
- Yksittäinen kirjautuminen sallii käyttäjän kirjautua Windows-toimialueelle kerran, yhtä salasanaa käyttäen, niin että käyttöoikeuksien todennus voidaan suorittaa missä tahansa Windows-toimialueen tietokoneessa. Yksittäisen kirjautumisen avulla järjestelmänvalvojat voivat hallita salasanojen todennusta koko Windows-verkossa, ja toisaalta käyttäjät voivat tehdä töitään helposti.

Seuraavissa osioissa kuvataan tarkemmin nämä kolme avainominaisuutta.

Käyttöoikeuksien todennus

Käyttöoikeuksien todennus on ehdottoman tärkeä osa järjestelmän suojausta, ja sen avulla voidaan varmistaa kenen tahansa sellaisen käyttäjän henkilöllisyys, joka yrittää kirjautua toimialueelle tai käyttää verkkoresursseja. Useimpien todennusjärjestelmien heikko lenkki on käyttäjän salasana.

Salasanat ovat toimialueiden ja paikallisten tietokoneiden ensimmäinen puolustuslinja asiatonta käyttöä vastaan. Suosittele asiakkaillesi seuraavia salasanakäytäntöjä:

- Käytä aina vahvoja salasanoja.
- Jos salasanat on kirjoitettava paperille, säilytä paperia suojatussa paikassa ja tuhoa paperi, kun sitä ei enää tarvita.

- Älä koskaan jaa salasanoja kenenkään kanssa.
- Käytä eri salasanaa jokaisessa käyttäjätilissä.
- Vaihda salasanoja säännöllisesti.
- Huolehdi, että salasanat on tallennettu tietokoneissa turvallisiin kohteisiin.

Vahvat salasanat

Salasanojen roolia organisaation verkon suojauksessa aliarvioidaan ja vähätellään usein. Kuten aiemmin todettiin, salasanat suojaavat verkkoa asiattomalta käytöltä. On siis syytä varmistaa, että asiakkaat neuvovat työntekijöitään käyttämään vahvoja salasanoja.

Salasanojen murtamistyökalut kuitenkin paranevat jatkuvasti, ja salasanojen murtamiseen käytetyt tietokoneet ovat tehokkaampia kuin koskaan. Automaattinen salasanan murtamisohjelma voi murtaa minkä tahansa salasanan, jos sille vain annetaan tarpeeksi aikaa. Vahvojen salasanojen murtaminen on kuitenkin paljon vaikeampaa kuin heikkojen salasanojen.

Lisätietoja vahvojen salasanojen luomisesta on osoitteissa

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

ja

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

Salasanakäytännön määrittäminen

Kun autat asiakasta määrittämään salasanakäytäntöään, pidä huoli siitä, että käytäntö vaatii kaikille käyttäjätileille vahvan salasanan. Useimmissa järjestelmissä riittää, että noudatetaan Windows Server 2003 Security Guide -suojausohjeita:

- Määritä **Valvo vanhoja salasanoja** -käytäntöasetus niin, että järjestelmä muistaa useita aiempia salasanoja. Tätä asetusta käytettäessä käyttäjät eivät voi käyttää samaa salasanaa uudelleen, kun salasana vanhenee.

  Suositeltu asetus: 24

- Määritä **Salasanan enimmäisikä** -käytäntöasetus niin, että salasanat vanhenevat niin usein kuin asiakkaan käyttöympäristössä vaaditaan.

  Suositeltu asetus: 42 (oletusarvo) - 90.

- Määritä **Salasanan vähimmäisikä** -käytäntöasetus niin, että salasanoja ei voi muuttaa, ennen kuin ne ovat olleet käytössä tietyn määrän päiviä. Tämä asetus toimii yhdessä **Valvo vanhoja salasanoja -**asetuksen kanssa. Jos salasanan vähimmäisikä on määritetty, käyttäjät eivät voi jatkuvasti muuttaa salasanaansa saadakseen **Valvo vanhoja salasanoja** -asetuksen ohitettua ja alkuperäisen salasanansa käyttöön. Sen sijaan käyttäjien on odotettava tietty määrä päiviä, ennen kuin he voivat muuttaa salasanaansa.

  Suositeltu asetus: 2.

- Määritä **Salasanan vähimmäispituus** -käytäntöasetus niin, että salasanoissa on oltava vähintään tietty määrä merkkejä. Vähintään seitsemänmerkkiset pitkät salasanat ovat yleensä lyhyitä salasanoja vahvempia. Tätä asetusta käytettäessä käyttäjät eivät voi käyttää tyhjiä salasanoja, ja heidän on luotava salasanoja, joissa on vähintään tietty määrä merkkejä.

  Suositeltu asetus: 8.

- Ota **Salasanan täytyy vastata monimutkaisuusvaatimuksia** -käytäntöasetus käyttöön. Käytäntöasetus tarkistaa kaikki uudet salasanat ja varmistaa, että ne täyttävät vahvojen salasanojen vaatimukset. Asetus varmistaa, että salasanoissa on vähintään kolme merkkiä neljästä luokasta (isot kirjaimet, pienet kirjaimet, numerot, muut kuin aakkosnumeeriset merkit) ja että salasana ei sisällä käyttäjätunnuksen osia eikä käyttäjän etu- tai sukunimen osia.

  Huomautus
  Vaikka salasana täyttäisi nämä vaatimukset, se ei välttämättä ole vahva salasana. Esimerkiksi salasana “Salasana1” täyttää nämä vaatimukset.

  Suositeltu asetus: Kyllä

- Koko vaatimusluettelo on Windows Serverin käytönaikaisten ohjeiden kohdassa Salasanan täytyy vastata monimutkaisuusvaatimuksia.

- Tallenna salasanat käyttäen kaksisuuntaista salausta -asetukseen liittyvää kaksisuuntaista salausta käytetään järjestelmissä, joissa sovelluksen on voitava käsitellä tekstimuotoisia salasanoja. Sitä ei tarvita useimmissa kokoonpanoissa.

  Suositeltu asetus: Ei.

Lisätietoja on Windows Server 2003 Security Guide -oppaassa:

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

Tilin lukituskäytännön määrittäminen

Ole varovainen, kun määrität tilin lukituskäytäntöä. Tilin lukituskäytäntöä ei pidä ottaa käyttöön pienissä yrityksissä, sillä se saattaa helposti lukita myös valtuutettujen käyttäjien tilejä, mikä voi tulla asiakkaalle hyvin kalliiksi.

Jos asiakas päättää ottaa käyttöön tilin lukituskäytännön, määritä **Tilin lukituskynnys** -käytäntöasetus tarpeeksi suureksi, jotta valtuutettujen käyttäjien käyttäjätilit eivät lukittuisi vain sen vuoksi, että käyttäjät kirjoittavat salasanansa muutaman kerran väärin.

Lisätietoja tilin lukituskynnyskäytännöstä on Windows Serverin käytönaikaisessa ohjeessa tilin lukituskäytäntöä käsittelevässä yleiskatsauksessa.

Lisätietoja tilin lukituskäytännön käyttöönottamisesta ja muokkaamisesta on Windows Serverin käytönaikaisessa ohjeessa.

Käytönhallinta

Windows-verkko ja sen resurssit (mukaan lukien Navision) voidaan suojata ottamalla huomioon, mitä käyttöoikeuksia käyttäjillä, käyttäjäryhmillä ja muilla tietokoneilla on verkossa. Voit suojata tietokoneen tai useita tietokoneita myöntämällä käyttäjille tai ryhmille erillisiä käyttöoikeuksia. Voit suojata

tiedoston tai kansion kaltaisen kohteen määrittämällä käyttöoikeuksia, jotka sallivat käyttäjien tai ryhmien suorittaa kohteessa tiettyjä toimintoja. Käytönhallinnan peruskäsitteitä ovat muun muassa seuraavat:

- käyttöoikeudet
- objektien omistus
- käyttöoikeuksien periminen
- järjestelmäoikeudet
- objektien valvonta.

Käyttöoikeudet

Käyttöoikeudet määrittävät, mitä oikeuksia käyttäjälle tai ryhmälle on määritetty objektiin tai objektin ominaisuuteen, esimerkiksi tiedostoihin, kansioihin ja rekisterikohteisiin. Käyttöoikeuksia sovelletaan kaikkiin suojattuihin kohteisiin, kuten tiedostoihin ja rekisterikohteisiin. Käyttöoikeuksia voidaan myöntää käyttäjille, ryhmille tai tietokoneille, mutta suojauksen kannalta niitä kannattaa määrittää ryhmille.

Objektien omistus

Objektille määritetään omistaja objektin luonnin yhteydessä. Windows 2000 Serverissä objektin luoja on oletusarvon mukaan omistaja. Windows Server 2003:ssa tätä käytäntöä on muutettu Järjestelmänvalvojat-ryhmän jäsenten osalta.

Jos Järjestelmänvalvojat-ryhmän jäsen luo objektin Windows Server 2003:ssa, omistajaksi tulee objektin luoneen henkilön sijasta koko Järjestelmänvalvojat-ryhmä. Tätä toimintaa voidaan muuttaa Paikalliset suojausasetukset -MMC-laajennuksen avulla käyttämällä asetusta **Järjestelmäobjektit: Järjestelmänvalvojat-ryhmän jäsenten luomien objektien oletusomistaja**. Olipa objektille määritetty mitä käyttöoikeuksia tahansa, objektin omistaja voi aina muuttaa objektin käyttöoikeuksia.

Lisätietoja on Windows Serverin käytönaikaisen ohjeen omistajuutta käsittelevässä ohjeaiheessa.

Käyttöoikeuksien periminen

Perimisen avulla järjestelmänvalvojat voivat helposti määrittää ja hallita käyttöoikeuksia. Jos asetus on käytössä, säilössä olevat objektit perivät automaattisesti kaikki säilön periytyvät käyttöoikeudet. Jos esimerkiksi luot tiedostoja kansioon, tiedostot perivät kansion käyttöoikeudet. Vain periytyviksi merkityt käyttöoikeudet periytyvät.

Järjestelmäoikeudet

Järjestelmäoikeudet määrittävät erityisiä etuoikeuksia ja kirjautumisoikeuksia tietokoneympäristön käyttäjille ja ryhmille.

Lisätietoja on Windows Serverin käytönaikaisten ohjeiden järjestelmäoikeuksia koskevassa kohdassa.

Objektien valvonta

Voit valvoa sitä, kuinka käyttäjät käyttävät objekteja. Näitä suojaukseen liittyviä tapahtumia voi tarkastella Tapahtumanvalvonnan suojauslokissa.

Lisätietoja on Windows Serverin käytönaikaisen ohjeen valvontaa käsittelevässä ohjeaiheessa.

Käytönhallinnan parhaat käytännöt

- Määritä käyttöoikeudet käyttäjien sijasta ryhmille. Käyttäjätilien hallinta yksittäin on tehotonta, joten käyttöoikeuksia tulee määrittää yksittäisille käyttäjille vain poikkeustilanteissa.
- Käytä oikeuksien estämistä joissakin erikoistilanteissa. Oikeuksien estämisen avulla voit esimerkiksi poistaa oikeudet sellaiseen ryhmään kuuluvalta käyttäjäjoukolta, jolle on myönnetty oikeudet.
- Älä koskaan estä objektin käyttöä Kaikki-ryhmältä. Jos estät kaikilta objektin käyttöoikeudet, oikeudet poistuvat myös järjestelmänvalvojilta. Parempi ratkaisu on Kaikki-ryhmän poistaminen, jos annat muille käyttäjille, ryhmille tai tietokoneille objektin käyttöoikeuden. Muista, että jos käyttöoikeuksia ei määritetä, objektin käsitteleminen ei ole sallittua.
- Määritä objektin käyttöoikeudet käyttäjäpuussa niin korkealla kuin mahdollista, ja määritä suojausasetukset sitten periytymään koko puun alueelle. Voit nopeasti määrittää käyttöoikeusasetuksia kaikille pääobjektin aliobjekteille. Tämä on tehokkain toimintatapa, jonka voi suorittaa vähimmällä vaivalla. Määritettyjen käyttöoikeusasetusten tulee soveltua käyttäjien, ryhmien ja tietokoneiden enemmistölle.
- Erilliset käyttöoikeudet voivat joskus ohittaa perityt käyttöoikeudet. Perityt käyttöoikeuksien estot eivät estä objektin käsittelemistä, jos objektille on erikseen määritetty Salli-käyttöoikeusmerkintä. Erilliset käyttöoikeudet ohittavat perityt käyttöoikeudet, myös perityt käyttöoikeuksien estot.
- Kun määrität Active Directory® -objektien käyttöoikeuksia, varmista, että ymmärrät Active Directory -objekteihin liittyvät parhaat käytännöt.

Lisätietoja on Windows Server 2003:n käytönaikaisen ohjeen kohdassa, joka käsittelee Active Directory -objektien käyttöoikeusmääritysten parhaita käytäntöjä.

Ulkoinen suojauspalomuuri

Palomuuri on laitteisto-osa tai ohjelmisto, joka estää datapaketteja joko saapumasta verkkoon tai poistumasta verkosta. Tietoliikenteen hallitsemiseksi palomuurin portit joko avautuvat tai sulkeutuvat datapaketteja varten. Palomuuri tarkistaa jokaisesta datapaketista useita tietoja: yhteyskäytännön, jota käyttämällä paketti välitetään, paketin kohteen tai lähettäjän, paketin sisältötyypin sekä porttinumeron, johon paketti lähetetään. Jos palomuuri on määritetty hyväksymään kyseessä oleva yhteyskäytäntö kohteena olevan portin läpi, paketti pääsee läpi. Microsoft Windows Small Business Server 2003 Premium Editionin mukana toimitetaan palomuuriratkaisuna Microsoft ISA (Internet Security and Acceleration) Server 2000. Myös Small Business Server Standard Editionissa on palomuuri.

ISA Server 2004

ISA (Internet Security and Acceleration) Server 2000 reitittää pyynnöt ja vastaukset Internetin ja asiakaskoneiden välillä turvallisesti sisäisessä verkossa.

ISA Server toimii paikallista verkkoa käyttävien asiakkaiden suojattuna väylänä Internetiin. ISA Server -tietokone on läpinäkyvä tiedonvälityspolun muille osapuolille. Internet-käyttäjä ei huomaa palomuuripalvelinta, ellei käyttäjä yritä käsitellä sellaista palvelua tai siirtyä sellaiselle sivustolle, jonka käsittelemistä ISA Server ei salli. Käytettävä Internet-palvelin tulkitsee ISA Server -tietokoneen lähettämät pyynnöt samalla tavalla kuin jos pyynnöt olisivat lähtöisin asiakassovelluksesta.

Kun valitset pirstaleiden IP (Internet Protocol) -suodatuksen, Web-välityspalvelin- ja palomuuripalvelut voivat suodattaa pakettipirstaleita. Pakettipirstaleita suodatettaessa kaikki pirstoutuneet IP-paketit hylätään. Erääseen tunnettuun hyökkäysmenetelmään liittyy pirstoutuneiden pakettien lähettäminen ja pakettien kokoaminen niin, että järjestelmälle saattaa koitua harmia.

ISA Server havaitsee tunkeutumiset ja ilmoittaa ajan, jolloin verkkoon on yritetty hyökätä. Lisäksi se suorittaa hyökkäystilanteissa joukon määritettyjä toimintoja (hälytyksiä).

Jos IIS (Internet Information Services) -palvelu on asennettu ISA Server -tietokoneeseen, palvelu on määritettävä niin, että se ei käytä samoja portteja, joita ISA Server -palvelin käyttää lähteviin Web-pyyntöihin (oletusarvon mukaan portti 8080) tai saapuviin Web-pyyntöihin (oletusarvon mukaan portti 80). Voit esimerkiksi muuttaa IIS-palvelun valvomaan porttia 81 ja määrittää ISA Server -tietokoneen ohjaamaan saapuvat Web-pyynnöt IIS-palvelua suorittavan paikallisen tietokoneen porttiin 81.

Jos ISA Server -palvelimen ja IIS-palvelun käyttämät portit aiheuttavat ristiriidan, asennusohjelma pysäyttää IIS-julkaisupalvelun. Tällöin voit vaihtaa IIS-palvelun valvomaan toista porttia ja käynnistää IIS-julkaisupalvelun uudelleen.

ISA Server -käytännöt

Voit määrittää ISA Server -käytännön, joka määrittää saapuvan ja lähtevän käytön. Sivusto- ja sisältösäännöt määrittävät, mitä sivustoja ja sisältöä käyttäjät voivat käsitellä. Yhteyskäytäntösäännöt määrittävät, voiko tiettyä yhteyskäytäntöä käyttää saapuvaan ja lähtevään tietoliikenteeseen.

Voit luoda sivusto- ja sisältösääntöjä, yhteyskäytäntösääntöjä, Web-julkaisusääntöjä ja IP-pakettisuodattimia. Nämä käytännöt määrittävät, millä tavalla ISA Server -asiakkaat ovat yhteydessä Internetiin ja minkälainen tietoliikenne on sallittua.

Virussuojaus

Tietokonevirus on suoritettava tiedosto, joka on suunniteltu monistamaan itseään, poistamaan tai vahingoittamaan datatiedostoja ja ohjelmia sekä välttämään havaituksi tulemista. Viruksia kirjoitetaan usein uudelleen ja muunnetaan niin, että niitä ei voida havaita. Viruksia lähetetään usein sähköpostin liitetiedostoina. Virustentorjuntaohjelmat on päivitettävä säännöllisesti, jotta ne havaitsisivat myös uudet ja muokatut virukset. Virukset ovat tietokonevandalismin kaikkein yleisin muoto.

Virustentorjuntaohjelmistot on suunniteltu havaitsemaan ja estämään virusohjelmat. Uusia virusohjelmia luodaan jatkuvasti, joten useat virustentorjuntatuotteiden valmistajat tarjoavat asiakkailleen säännöllisiä ohjelmistopäivityksiä. Microsoft suosittelee painokkaasti virustentorjuntaohjelmiston käyttöönottamista asiakkaan ympäristössä.

Virustentorjuntaohjelmisto asennetaan yleensä seuraaviin kolmeen kohteeseen: käyttäjien työasemiin, palvelimiin ja verkkoon, jonka kautta sähköposti saapuu organisaatioon (ja joissakin tapauksissa lähtee organisaatiosta).

Virustyypit

Tietokonejärjestelmiä saastuttavia viruksia on kolmea päätyyppiä: käynnistyssektorin virukset, tiedostoihin tarttuvat virukset ja Troijan hevoset.

Käynnistyssektorin virukset

Kun tietokone käynnistyy, se tarkistaa kiintolevyn käynnistyssektorin ennen käyttöjärjestelmän tai muiden käynnistystiedostojen lataamista. Käynnistyssektorin virus on suunniteltu niin, että se korvaa kiintolevyn käynnistyssektorit omalla koodillaan. Kun tietokoneessa on käynnistyssektorin virus, tietokone lukee viruksen koodin muistiinsa ennen mitään muuta. Kun virus on muistissa, se voi kopioida itsensä muihin viruksen tartuttaman tietokoneen käyttämiin levyasemiin ja levyihin.

Tiedostoihin tarttuvat virukset

Yleisin virustyyppi on tiedostoihin tarttuva virus, joka kiinnittää itsensä suoritettavaan ohjelmaan lisäämällä oman koodinsa suoritettavaan tiedostoon. Viruskoodi lisätään yleensä sellaisella tavalla, että sitä ei huomata. Kun viruksen tartuttama tiedosto suoritetaan, virus voi kiinnittää itsensä muihin suoritettaviin tiedostoihin. Tällaisen viruksen tartuttamissa tiedostoissa on tiedostopäätteenä yleensä .com, .exe tai .sys.

Jotkin tiedostoihin tarttuvat virukset on suunniteltu tiettyjä ohjelmia varten. Viruksia on usein kohdistettu peittokaavio (.ovl)- ja dynaamisesti linkitettävä kirjasto (.dll) -tiedostoihin. Tietokone ei suorita näitä tiedostoja, mutta suoritettavat tiedostot kutsuvat niitä. Virus välittyy eteenpäin, kun viruksen tartuttamaa tiedostoa kutsutaan.

Tiedot vahingoittuvat viruksen aktivoituessa. Virus saattaa aktivoitua, kun sen tartuttama tiedosto suoritetaan tai kun tietty ympäristöasetus toteutuu (esimerkiksi tiettynä järjestelmäpäivämääränä).

Troijan hevosia sisältävät ohjelmat

Troijan hevonen ei oikeastaan ole virus. Viruksen ja Troijan hevosen tärkein ero on siinä, että Troijan hevonen ei kopioi itseään, se vain tuhoaa kiintolevyllä olevia tietoja. Troijan hevonen on naamioitu viattomaksi ohjelmaksi, kuten peliksi tai apuohjelmaksi. Kun ohjelma suoritetaan, se saattaa kuitenkin tuhota tai sotkea tietoja.

Virussuojauksen parhaat käytännöt

Makroviruksen leviämisen voi estää. Seuraavassa on vihjeitä, joiden avulla tartunnan voi välttää ja jotka tulee kertoa asiakkaille:

- Asenna virustentorjuntaratkaisu, joka tarkistaa Internetistä saapuvat viestit virusten varalta, ennen kuin viestit pääsevät läpi reitittimestä. Tällöin sähköpostit tarkistetaan tunnettujen virusten varalta.
- Varmista, että tunnet vastaanotettujen asiakirjojen lähteen. Asiakirjoja ei pidä avata, elleivät ne ole sellaiselta henkilöltä, jota asiakas pitää luotettavana.
- Keskustele asiakirjan tekijän kanssa. Jos käyttäjät ovat hiukankin epävarmoja asiakirjan turvallisuudesta, heidän tulee ottaa yhteyttä asiakirjan tekijään.
- Käytä Microsoft Officen makrovirussuojausta. Officessa sovellukset varoittavat käyttäjää, jos asiakirja sisältää makroja. Tämän ominaisuuden avulla käyttäjä voi joko sallia tai estää makrojen käyttämisen, kun asiakirja avataan.
- Käytä virustentorjuntaohjelmistoa, joka havaitsee ja poistaa makrovirukset. Virustentorjuntaohjelmisto voi havaita asiakirjojen sisältämät makrovirukset, ja lisäksi se voi usein poistaa ne. Microsoft suosittelee sellaisen virustentorjuntaohjelmiston käyttämistä, jonka ICSA (International Computer Security Association) -järjestö on sertifioinut.

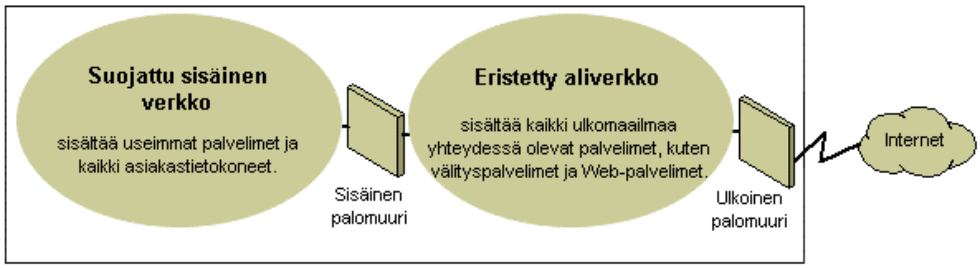
Lisätietoja viruksista ja tietokoneiden yleissuojauksesta on seuraavilla Microsoft Security -Web-sivuilla:

- Microsoft Security osoitteessa http://www.microsoft.com/security/default.asp.
- Microsoft TechNetin suojausasiakirjat http://www.microsoft.com/technet/security/Default.mspx.

Verkon suojausstrategiat

Internet-toimintaan käytetyn IP-ympäristön rakenteessa ja käyttöönotossa on otettava huomioon yksityisen ja julkisen verkon tarpeet, joten palomuurista on tullut tärkeä osa verkon yhtenäisyyden varmistamista. Palomuuri ei ole yksittäinen komponentti. NCSA:n (National Computer Security Association) määritelmän mukaan palomuuri on järjestelmä tai järjestelmäyhdistelmä, joka luo raja-alueen kahden tai useamman verkon välille. Käytössä on erilaisia termejä, mutta suomeksi tätä raja-aluetta voidaan kutsua eristetyksi aliverkoksi. Eristetty aliverkko suojaa intranet-verkkoa tai yrityksen lähiverkkoa (LAN) ulkopuolisilta hallitsemalla sitä, kuka voi käyttää verkkoa Internetistä tai muista suurista verkoista.

Seuraavassa kuvassa esitetään eristetty aliverkko, joka on palomuurien rajoittama ja joka sijaitsee yksityisverkon ja Internetin välissä taaten suojatun verkon:



Eristetyn aliverkon perusteet.

Organisaatiot hyödyntävät palomuureja suojauksessa eri tavoilla. IP-pakettien suodatus varmistaa vain heikon suojauksen, minkä lisäksi suojauksen ylläpitäminen on vaikeaa ja asiattomat tunkeutujat voivat helposti ohittaa sen. Sovellusyhdyskäytävät ovat pakettisuodatusta suojatumpia ja helpommin hallittavia, koska ne liittyvät vain joihinkin sovelluksiin, kuten tiettyyn sähköpostijärjestelmään. Piiritason yhdyskäytävät ovat tehokkaimpia, kun verkkosovelluksen käyttäjä on suurempi huolenaihe kuin sovelluksen välittämät tiedot. Välityspalvelin on monipuolinen suojaustyökalu, johon sisältyy sovellusyhdyskäytävä, anonyymien käyttäjien turvallinen käsittely ja muita palveluita. Seuraavassa on lisätietoja eri mahdollisuuksista:

- **IP-pakettien suodatus**
  IP-pakettien suodatus oli ensimmäinen palomuuritekniikan sovellus. Suodatus tutkii pakettien otsikoista lähde- ja kohdeosoitteet, TCP (Transmission Control Protocol) -yhteyskäytännön ja UDP (User Datagram Protocol) -yhteyskäytännön porttinumerot sekä muita tietoja. Pakettien suodatus on rajoittunut tekniikka, joka toimii parhaiten selkeissä suojatuissa ympäristöissä, joissa esimerkiksi mihinkään eristetyn aliverkon ulkopuolelta tulevaan ei luoteta ja kaikkeen eristetyn aliverkon sisäpuolella olevaan luotetaan. Viime vuosien aikana monet valmistajat ovat parantaneet paketinsuodatusmenetelmiä lisäämällä paketinsuodatusytimeen älykkäitä päätöksenteko-ominaisuuksia. Tämä paketinsuodatuksen uusi muoto tunnetaan lyhenteellä SPI (Stateful Protocol Inspection). Voit määrittää paketinsuodatuksen joko hyväksymään tietyntyyppiset paketit ja estämään kaikki muut, tai estämään tietyntyyppiset paketit ja hyväksymään kaikki muut.
- **Sovellusyhdyskäytävät**
  Sovellusyhdyskäytäviä käytetään, kun sovellusten varsinainen sisältö aiheuttaa suurimman huolenaiheen. Sovellusyhdyskäytävät ovat sovelluskohtauksia, mikä on niiden suurin vahvuus ja suurin heikkous: niiden sovittaminen tekniikan muutoksiin voi olla vaikeaa.
- **Piiritason yhdyskäytävät**
  Piiritason yhdyskäytävät ovat palomuurin läpi rakennettuja tunneleita, jotka yhdistävät toisella puolella olevat tietyt prosessit tai järjestelmät vastaaviin toisen puolen prosesseihin tai järjestelmiin. Piiritason yhdyskäytäviä kannattaa käyttää tilanteissa, joissa sovellusta käyttävä henkilö saattaa aiheuttaa suuremman riskin kuin sovelluksen sisältämät tiedot. Piiritason yhdyskäytävä eroaa pakettisuodattimesta siinä, että se voi muodostaa yhteyden kaistan ulkopuoliseen sovellukseen, joka voi lisätä tietoja.

- **Välityspalvelimet**
  Välityspalvelimet ovat monipuolisia suojaustyökaluja, joiden palomuuri- ja sovellusyhdyskäytävätoiminnot hallitsevat Internet-liikennettä lähiverkkoon ja lähiverkosta. Välityspalvelimet mahdollistavat myös asiakirjojen tallentamisen välimuistiin ja käytönhallinnan. Välityspalvelin voi parantaa suorituskykyä tallentamalla esimerkiksi suositun Web-sivuston tapaisia usein pyydettyjä tietoja välimuistiin ja välittämällä ne suoraan pyytäjälle. Välityspalvelin voi myös suodattaa ja hylätä pyyntöjä, joita omistaja ei pidä hyväksyttävinä. Tällaisia pyyntöjä voivat olla esimerkiksi luottamuksellisten tietojen luvattomat käyttöpyynnöt.

Varmista, että asiakas hyödyntää niitä palomuurin suojausominaisuuksia, joista on hyötyä hänelle. Sijoita eristetty aliverkko sellaiseen verkkotopologian kohtaan, jossa kaiken yritysverkon ulkopuolelta tulevan liikenteen on kuljettava ulkoisen palomuurin ylläpitämän eristetyn alueen läpi. Voit hienosäätää palomuurin käytönhallintaa asiakkaan tarpeiden mukaan, minkä lisäksi voit määrittää palomuurit raportoimaan kaikki asiattomat käyttöyritykset.

Voit vähentää sisäisessä palomuurissa tarvittavia avoimia portteja käyttämällä sovelluskerroksen palomuuria, esimerkiksi ISA Server 2000 -ratkaisua.

Lisätietoja TCP/IP:stä on Web-sivun http://www.microsoft.com/resources/documentation/WindowsServ/2003/all/deployguide/en-us/dnsbb_tcp_overview.asp kohdassa Designing a TCP/IP Network.

Langattomat verkot

Yleensä langattomat verkot on määritetty niin, että langattomien signaalien salakuuntelu onnistuu. Langattomat verkot saattavat olla alttiita joutumaan asiattomien ulkopuolisten käyttöön. Tämä johtuu muun muassa joidenkin langattomien laitteistojen oletusasetuksista, langattomien verkkojen käyttömahdollisuuksista sekä käytössä olevista salausmenetelmistä. Käytettävissä on määritysasetuksia ja työkaluja, joiden avulla langattoman verkon voi suojella salakuuntelulta. Muista kuitenkin, että ne eivät suojaa tietokoneita hakkereilta ja viruksilta, jotka pääsevät tietokoneisiin Internet-yhteyden kautta. On siis erittäin tärkeää käyttää palomuuria, joka suojelee tietokonetta asiattomilta Internet-tunkeilijoilta.

Lisätietoja langattoman verkon suojauksesta on Web-sivun http://support.microsoft.com/default.aspx?scid=kb;en-us;309369 kohdassa How to Make Your 802.11b Wireless Home Network More Secure.

Verkkosuojauksen esimerkkitilanteita

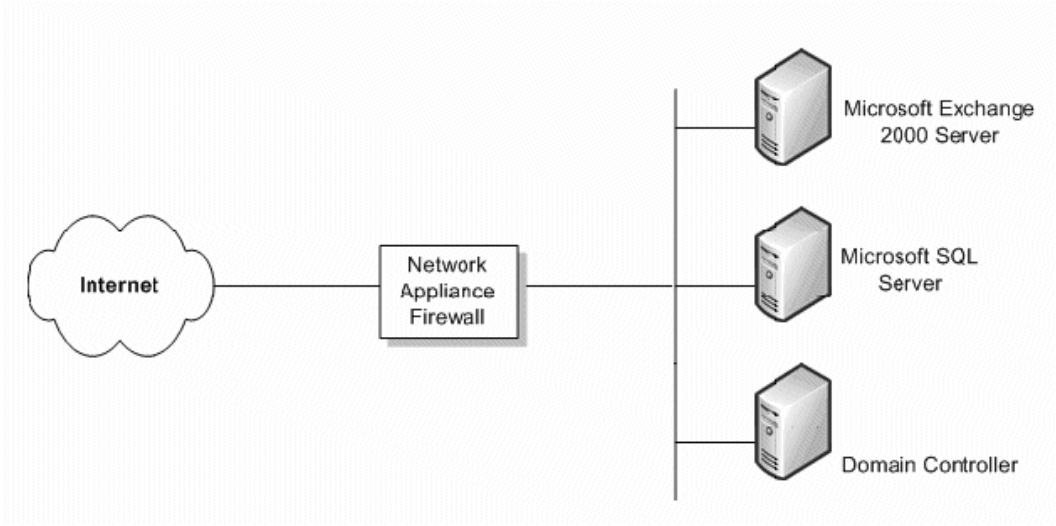
Asiakasorganisaation vaatima verkkosuojauksen taso määräytyy usean tekijän mukaan. Yleensä on tehtävä kompromissi budjetin ja yrityksen tietojen suojauksen välillä. Pienyrityksellä saattaa olla erittäin monimutkainen suojausrakenne, joka mahdollistaa parhaan mahdollisen verkkosuojauksen, mutta kaikilla pienyrityksillä ei välttämättä ole varoja tällaiseen suojaustasoon. Tässä osiossa tutkimme neljää esimerkkitilannetta ja annamme kuhunkin tilanteeseen liittyviä suosituksia, joiden avulla suojausta voi parantaa.

Ei palomuuria

Jos asiakkaalla on Internet-yhteys ilman palomuuria, käyttöön on otettava jokin verkkosuojauksen menetelmä. Saatavilla on yksinkertaisia palomuuriratkaisuja, joista saatava suojaus estää useimpien hyökkääjien aikeet.

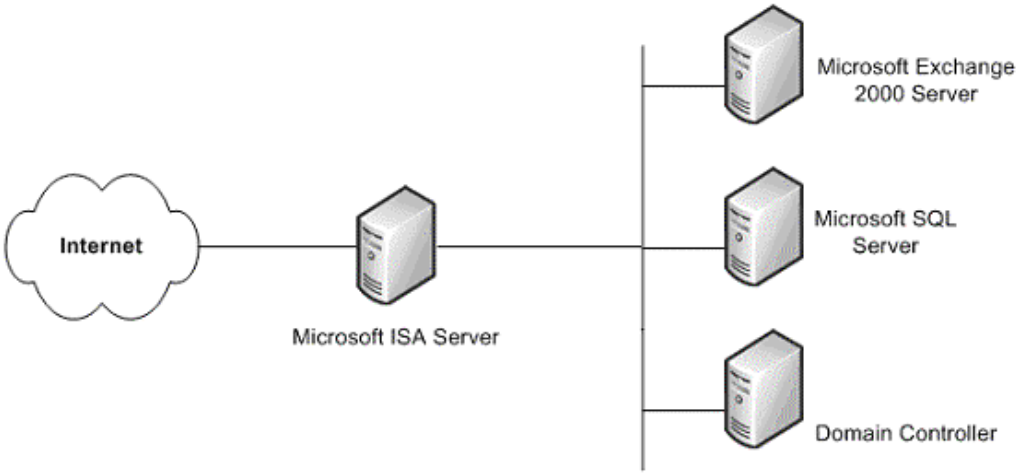
Yksi yksinkertainen palomuuri

Suojauksen suositeltu vähimmäistaso on yksi palomuuri Internetin ja asiakkaan tietojen välissä. Tällainen palomuuri ei anna minkäänlaista kehittynyttä suojausta, eikä sitä voi pitää kovin varmana. Se on kuitenkin parempi kuin ei mitään.



Yksinkertainen palomuuri.

Toivottavasti asiakkaan budjetti sallii turvallisemman ratkaisun, joka suojelee yrityksen tietoja paremmin. Eräs tällainen ratkaisu on ISA Server -palvelin. Lisäpalvelimen aiheuttamat kustannukset korvaa huomattavasti tavallista kuluttajapalomuuria parempi suojaus, sillä kuluttajapalomuuriin liittyy usein pelkästään verkko-osoitteiden muuntaminen (NAT) ja pakettien suodatus.



ISA Server -palvelinpalomuuri.

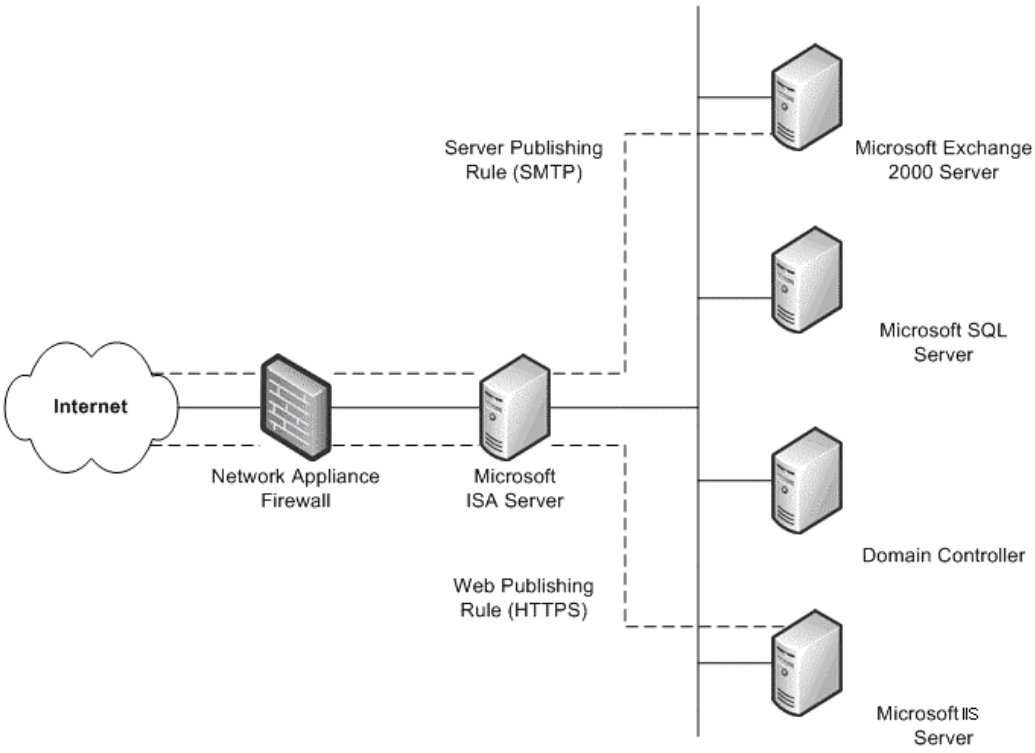
Tämä yhden palomuurin ratkaisu on peruspalomuuria suojatumpi, ja siihen liittyy Windowsille luotuja suojauspalveluita.

Yksi käytössä oleva palomuuri

Jos asiakkaalla on käytössään palomuuri, joka erottaa intranetin Internetistä, voit harkita sellaista lisäpalomuuria, johon liittyy useita tapoja määrittää sisäiset resurssit Internetiin.

Eräs tällainen menetelmä on Web-julkaiseminen. Tällöin ISA Server -palvelin otetaan käyttöön organisaation sen Web-palvelimen eteen, joka antaa käyttäjille Internetin käyttömahdollisuuden. Saapuvien Web-pyyntöjen yhteydessä ISA Server -palvelin voi tekeytyä Web-palvelimeksi ja täyttää asiakkaiden Web-sisältöpyynnöt välimuististaan. ISA Server -palvelin välittää pyyntöjä Web-palvelimelle vain, jos pyyntöjä ei voi täyttää välimuistista.

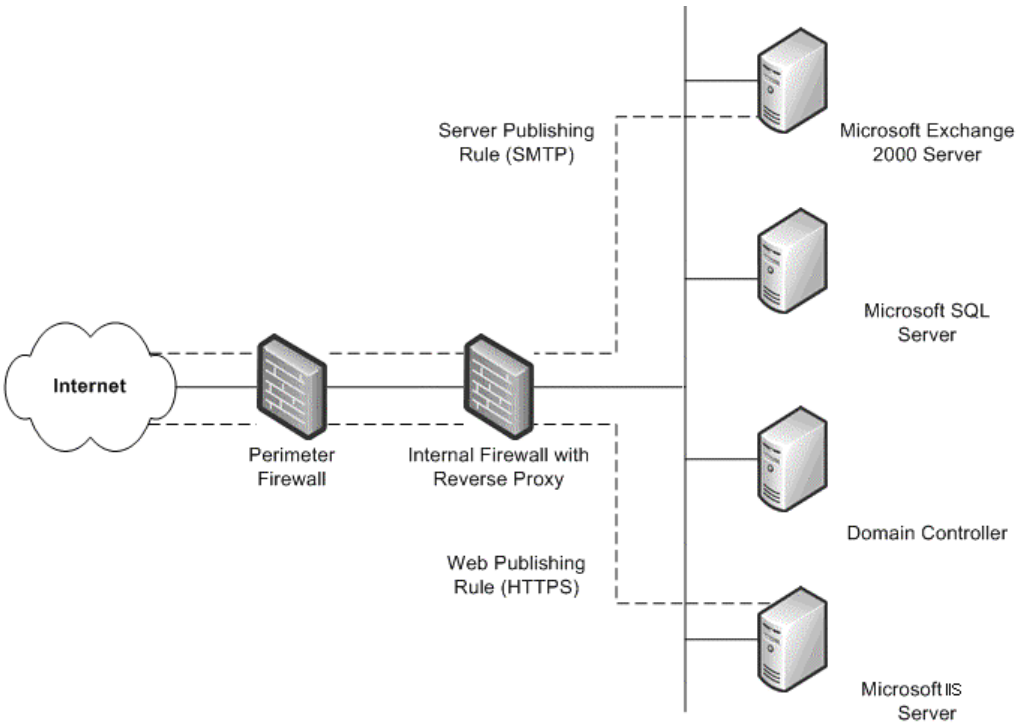
Toinen menetelmä on palvelinjulkaisu. ISA Server mahdollistaa sisäisten palvelimien julkaisemisen Internetiin niin, ettei sisäisen verkon suojaus vaarannu. Voit määrittää Web-julkaisuun ja palvelinjulkaisuun sääntöjä, jotka määrittävät, milloin pyynnöt lähetetään paikallisen verkon palvelimeen. Tällä tavalla sisäisten palvelimien suojaus tehostuu.



Käytössä oleva palomuuri, johon on lisätty ISA Server -palvelin.

Kaksi käytössä olevaa palomuuria

Neljännessä esimerkkitilanteessa organisaatiolla on käytössä kaksi palomuuria sekä eristetty aliverkko (DMZ). Ainakin yksi palvelin tuottaa palvelimen piilottavia välityspalvelinpalveluita, joten Internet-asiakkaat eivät käsittele intranetin palveluita suoraan. Sen sijaan jokin palomuureista, mieluiten sisäinen palomuuri, ottaa vastaan sisäisiin palvelimiin lähetetyt pyynnöt, tarkistaa paketit ja välittää ne sitten Internet-isännän puolesta.



Kaksi käytössä olevaa palomuuria.

Tämä esimerkkitilanne vastaa edeltävää esimerkkitilannetta toisen palomuurin lisäämisen jälkeen. Ainoa ero on siinä, että palvelimen piilottavaa välityspalvelinta tukeva sisäinen palomuuri ei ole ISA Server -palvelin. Tässä esimerkkitilanteessa kannattaa olla tiiviissä yhteydessä kunkin palomuurin valvojien kanssa, jotta suojauskäytäntöihin soveltuvat julkaisusäännöt voidaan määrittää.

Suojauskorjausten hallinta

Käyttöjärjestelmät ja sovellukset ovat usein todella monimutkaisia. Ne saattavat koostua miljoonista koodiriveistä, joiden kirjoittamiseen on osallistunut useita ohjelmoijia. Ohjelmiston luotettava toiminta on ehdottoman tärkeää, samoin kuin se, ettei ohjelmisto vaaranna tietotekniikkaympäristön suojausta tai vakautta. Ongelmien välttämiseksi ohjelmat testataan huolellisesti ennen julkaisua. Hyökkääjät kuitenkin etsivät ohjelmistoista jatkuvasti heikkouksia, joten kaikkiin tuleviin hyökkäyksiin varautuminen ei ole mahdollista.

Useissa organisaatioissa korjaustiedostojen hallinta on osa muutosten ja kokoonpanon hallintastrategiaa. Olipa organisaatio minkälainen ja minkäkokoinen tahansa, käytössä tulee ehdottomasti olla toimiva korjaustiedostojen hallintastrategia, vaikka organisaatiolla ei vielä olisikaan käytössä muutosten ja kokoonpanon hallintastrategiaa. Valtaosa tietokonejärjestelmiin kohdistuneista onnistuneista hyökkäyksistä tehdään sellaisiin järjestelmiin, joihin suojauskorjauksia ei ole asennettu.

Suojauskorjaukset ovat haaste useimmille organisaatioille. Kun ohjelmistossa on havaittu heikkous, hyökkääjät levittävät siitä nopeasti tietoa hakkeriyhteisöjen kautta. Kun Microsoftin ohjelmistossa ilmenee heikkouksia, Microsoft pyrkii julkaisemaan suojauskorjauksen mahdollisimman pian. Korjaustiedoston käyttöönottoa edeltävänä aikana asiakkaan suojaus saattaa olla huomattavasti heikentynyt.

Navision-ympäristössä tulee varmistaa, että asiakkaiden järjestelmään on asennettu kaikki uusimmat suojauskorjaukset. Varmista, että asiakas käyttää jotakin Microsoftin päivitysmenetelmää:

- **Microsoft Security Notification Service -palvelu**
  Microsoft Security Notification Service -palvelu on sähköpostiluettelo, joka antaa ilmoituksen aina, kun uusi päivitys on saatavilla. Nämä ilmoitukset muodostavat tärkeän osan proaktiivista suojausstrategiaa. Ilmoitukset ovat saatavilla myös TechNet Product Security Notification -Web-sivustolla: http://www.microsoft.com/technet/security/bulletin/notify.mspx.
- **Microsoftin automaattiset päivitykset**
  Windows voi ottaa suojauspäivitykset automaattisesti käyttöön tietokoneissa.
- **Microsoft Security Bulletin -sivuston hakutyökalu**
  Security Bulletin -sivuston hakutyökalu on saatavilla Security Bulletin Service -Web-sivulla: http://www.microsoft.com/technet/security/current.aspx. Asiakas voi valita tarvitsemansa päivitykset käytössä olevien käyttöjärjestelmän, sovellusten ja Service Pack -pakettien perusteella.
- **Microsoft Baseline Security Analyzer (MBSA)**
  Tämä graafinen työkalu on saatavilla Microsoft Baseline Security Analyzer -Web-sivustolla: http://www.microsoft.com/technet/security/tools/mbsahome.mspx. Työkalu vertaa tietokoneen nykytilaa Microsoftin ylläpitämään päivitysluetteloon. MBSA suorittaa myös perussuojaukseen liittyviä tarkistuksia ja tarkistaa esimerkiksi salasanan vahvuus- ja vanhenemisasetukset, vierailijatilien käytännöt sekä muita vastaavia käytäntöjä. MBSA hakee heikkouksia Microsoft IIS (Internet Information Services) -palveluista, SQL Server™ 2000:sta sekä Exchange 5.5-, Exchange 2000- ja Exchange Server 2003 -ohjelmista.
- **Microsoft Software Update Services (SUS) -palvelut**
  Tämä työkalu tunnettiin aiemmin nimellä Windows Update Corporate Edition, ja sen avulla yritykset voivat isännöidä paikallisissa tietokoneissa kaikki kriittiset päivitykset ja SRP (Security Rollup Package) -paketit, joita on saatavilla julkisessa Windows Update -sivustossa. Työkalu käyttää automaattisen päivitysasiakkaan (AU) uutta julkaisuversiota tehokkaan automaattisen lataus- ja asennusstrategian perustana. Uuteen AU-ohjelmapakettiin sisältyy Windows 2000- ja Windows Server 2003 -käyttöjärjestelmien asiakasohjelma ja mahdollisuus asentaa ladatut päivitykset automaattisesti. Lisätietoja Microsoft SUS -palveluista on sivulla http://www.microsoft.com/windows2000/windowsupdate/sus/default.asp.
- **Microsoft SMS (Systems Management Server) Software Update Services Feature Pack**
  SMS Software Update Services Feature Pack -paketissa on useita työkaluja, joiden avulla ohjelmistopäivityksiä voi entistä helpommin jakaa koko yritykseen. Pakettiin sisältyvät seuraavat työkalut: Security Update Inventory Tool, Microsoft Office Inventory Tool for Updates, Distribute Software Updates Wizard ja SMS Web Reporting Tool with Web Reports Add-in for Software Updates. Lisätietoja kustakin työkalusta on osoitteessa http://www.microsoft.com/smserver/downloads/20/featurepacks/suspack/.

Keskustele asiakkaiden kanssa kustakin työkalusta ja kehota heitä käyttämään niitä. Suojausongelmiin tulee reagoida mahdollisimman nopeasti niin, että ympäristön vakaus samalla säilyy.

SQL Server 2000 -palvelimen suojausasetukset

Navision toimii myös SQL Server 2000 -palvelimessa, joten asiakkaan SQL Server 2000 -asennuksen suojausta tulee parantaa mahdollisuuksien mukaan. Seuraavien ohjeiden mukaan voit parantaa SQL Serverin suojausta:

- Varmista, että viimeisin käyttöjärjestelmä ja viimeisimmät SQL Server 2000 Service Pack -paketit on asennettu. Uusimmat tiedot ovat Microsoft Security -Web-sivustolla osoitteessa http://www.microsoft.com/security/default.asp.
- Varmista tiedostojärjestelmätason suojausta varten, että kaikki SQL Server 2000 -tiedot ja järjestelmätiedostot on asennettu NTFS-osioihin. Tiedostojen tulee olla NTFS-käyttöoikeuksien perusteella vain järjestelmänvalvojien tai järjestelmätason käyttäjien käytettävissä. Tällöin käyttäjät eivät voi käyttää kyseisiä tiedostoja, kun MSSQLSERVER-palvelu ei ole käynnissä.
- Käytä toimialatiliä, jolle on määritetty vähäiset käyttöoikeudet, esimerkiksi NT Authority\Network Service -tiliä tai SQL Server 2000 -palvelun (MSSQLSERVER) LocalSystem-tiliä (suositellaan). Tilillä tulee olla mahdollisimman vähän toimialueen oikeuksia, ja sen tulee auttaa rajaamaan (mutta ei pysäyttämään) palvelimeen kohdistuva hyökkäys, jos suojaus on pettänyt. Toisin sanoen tilillä tulee olla vain toimialueen paikallisen käyttäjän tasoiset käyttöoikeudet. Jos SQL Server 2000 käyttää toimialueen valvojan tiliä palveluiden suorittamiseen, palvelimen suojauksen pettäminen johtaa koko toimialueen suojauksen pettämiseen. Voit muuttaa asetusta SQL Server Enterprise Managerin avulla. Ohjelma muuttaa tiedostojen, rekisterin ja järjestelmäoikeuksien käyttöoikeusluetteloita automaattisesti.
- Useimpien SQL Server 2000 -versioiden yhteydessä on asennettu kaksi oletustietokantaa: **Northwind** ja **pubs**. Molemmat tietokannat ovat mallitietokantoja testaamista, koulutusta ja yleisiä esimerkkejä varten. Niitä ei tule ottaa käyttöön tuotantojärjestelmässä. Kyseisten tietokantojen läsnäolo saattaa innoittaa hyökkäyksiin, joissa hyödynnetään oletusasetuksia ja oletuskokoonpanoa. Jos **Northwind**- ja **pubs**-tietokannat on asennettu SQL Server 2000 -tuotantotietokoneeseen, ne tulee poistaa.
- SQL Server 2000 -järjestelmän valvonta on oletusarvon mukaan poistettu käytöstä, joten järjestelmä ei valvo mitään tilanne-ehtoja. Hyökkäysten havaitseminen on näin ollen vaikeaa, ja hyökkääjät voivat saada jälkensä peitettyä. Järjestelmä tulee määrittää vähintään valvomaan epäonnistuneita sisäänkirjautumisyrityksiä.

Uusimmat SQL Server 2000:n suojaustiedot ovat osoitteessa http://www.microsoft.com/sql/techinfo/administration/2000/security/default.asp.

Tietoja Microsoft Business Solutionsista

Microsoft Business Solutions on Microsoftin osasto, joka tarjoaa useita integroituja kattavan liiketoiminnan sovelluksia ja palveluita, jotka auttavat pieniä, keskisuuria ja suuria yrityksiä parantamaan yhteyksiään asiakkaisiin, työntekijöihin, liikekumppaneihin ja toimittajiin. Microsoft Business Solutionsin sovellukset optimoivat strategiset liiketoiminnan prosessit taloudenhallinnassa, analysoinnissa, henkilöresurssien hallinnassa, projektinhallinnassa, asiakassuhteiden hallinnassa, kenttäpalveluiden hallinnassa, toimitusketjun hallinnassa, sähköisessä kaupankäynnissä, valmistuksessa ja jälleenmyynnin hallinnassa. Sovellukset on suunniteltu niin, että niiden tarjoama tieto auttaa asiakkaita menestymään liiketoiminnassaan. Lisätietoja Microsoft Business Solutionsista on osoitteessa http://www.microsoft.com/BusinessSolutions/