Microsoft Business Solutions

# Navision Security Hardening Guide

Publicēta 2004. gada oktobrī

Microsoft

# Satura rādītājs

# Ievads

Microsoft® Windows® sniedz modernu un standartizētu tīkla drošību. Drošība, šī vārda visplašākajā nozīmē, ietver plānošanu un kompromisu izvērtēšanu. Piemēram, datoru var ieslēgt seifa telpā un padarīt pieejamu tikai sistēmas administratoram. Šādu datoru var uzskatīt par drošu, taču tas nav īpaši lietderīgi, kamēr šis dators nav savienots ar kādu citu datoru. Ir jāapsver nepieciešamā rīcība, lai padarītu tīklu pēc iespējas drošāku, vienlaikus nezaudējot lietojamību.

Kaut arī lielākā daļa uzņēmumu veic pasākumus, lai novērstu ārējos uzbrukumus, un būvē ugunsmūrus, daudzi no tiem, kā kompensēt drošības pārrāvumu gadījumos, kad ļaunprātīgais lietotājs jau ir nokļuvis ugunsmūra iekšienē. Drošības pasākumi jūsu klienta vidē darbosies labi tad, ja drošības nolūkos lietotājiem nav jāveic pārāk daudz operāciju un darbību. Drošības politikas ieviešanā lietotāju lomai jābūt pēc iespējas vienkāršākai — pretējā gadījumā viņi meklē veidus, kā šo drošību apiet.

Tā kā Navision instalācijas lielums katrā gadījumā var būt stipri atšķirīgs, ir būtiski, lai tiktu apsvērtas katra klienta vajadzības un drošības efektivitāte tiktu izvērtēta attiecībā pret iesaistītajām izmaksām. Kā uzticams sava klienta padomdevējs izvērtējiet situāciju pēc vislabākās sirdsapziņas un iesakiet politiku, kas vienlaikus atbilst drošības prasībām un nerada slogu, kas galu galā varētu likt klientam no šīs politikas atteikties.

# Navision drošības ieteicamā prakse

Lai palielinātu Navision vides drošību, ir ieteicama šādu vispārīgu noteikumu ievērošana:

- Ja vēlaties palaist Navision Database Server kā pakalpojumu vai servera startēšanas laikā izmantot komandrindas parametru *installasservice*, jums jānodrošina, ka pakalpojums tiek palaists kā NT Authority\Network Service konts. NT Authority\Network Service konts pastāv tikai sistēmās Windows™ XP un Windows Server™ 2003. Ja izmantojat sistēmu Windows 2000 Server, jāveido konts ar vismazākajām pakalpojuma tiesībām; pretējā gadījumā pakalpojumam tiks piešķirts Local System konts. Šim kontam nekādā gadījumā nedrīkst būt vairāk tiesību kā parastam lietotāja kontam, vai arī tam ir jābūt domēna kontam, kas nav administratora konts ne domēnā, ne arī jebkurā lokālajā datorā.

  Neaizmirstiet NT Authority\Network Service kontam vai lietotāja kontam, ar kuru serveris darbojas, piešķirt lasīšanas un rakstīšanas piekļuvi datu bāzes failam(iem), lai lietotāji varētu pieslēgties datu bāzei.

  Lai NT Authority\Network Service kontam piešķirtu lasīšanas un rakstīšanas piekļuvi datu bāzes failam sistēmā Windows XP:

  1. Pārlūkā Windows Explorer atveriet mapi, kurā atrodas datu bāzes fails.
  2. Atlasiet datu bāzes failu, noklikšķiniet uz tā ar peles labo pogu un atlasiet Properties (Rekvizīti).
  3. Logā ***Properties*** (Rekvizīti) noklikšķiniet uz cilnes ***Security*** (Drošība) un zem lodziņa **Group and user names** (Grupas un lietotājvārdi) noklikšķiniet uz pogas Add (Pievienot).
  4. Logā ***Select Users, Computers, or Groups*** (Atlasiet Lietotāji, Datori vai Grupas) ievadiet *"Network Service"* un noklikšķiniet uz pogas OK (Labi).
  5. Loga ***Properties*** laukā **Group and user names** tiek pievienots elements NETWORK SERVICE.
  6. Atlasiet NETWORK SERVICE un laukā **Permissions** (Atļaujas) piešķiriet atļaujas *Read* (Lasīt) un *Write* (Rakstīt).
- Navision Application Service pakalpojums pēc noklusējuma darbojas kā NT Authority\Network Service, un tādējādi tam ir iespēja piekļūt Navision Database Server lokāli. Tomēr, ja vēlaties datu bāzes serverim piekļūt tīklā, Navision Application Server pakalpojums jāpalaiž kā Windows domēna konts, kuru pazīst Navision Database Server. Šis konts nedrīkst būt administrators ne domēnā, ne arī kādā lokālajā datorā.
- Ja lietojat programmas Navision SQL Server opciju, Microsoft SQL Server™ tiek palaists kā pakalpojums. Programmas Navision SQL Server opcijai nepieciešams, lai SQL Server varētu lietot pakalpojumu Active Directory un tādējādi iegūt Windows lietotāju grupu sarakstus autentifikācijas mērķiem. Tāpēc jānodrošina, ka pakalpojums SQL Server tiek izpildīts kā NT Authority\Network Service konts.

  Lai nodrošinātu, ka pakalpojums tiek izpildīts kā NT Authority\Network Service pakalpojums:

  1. Datorā, kurā uzstādīts SQL Server, atrodiet pakalpojumu MSSQLSERVER, noklikšķiniet uz tā ar peles labo pogu un atlasiet Properties.
  2. Logā ***Properties*** noklikšķiniet uz cilnes ***Log On*** (Pieteikšanās).
  3. Cilnes sadaļā ***Log on*** as (Pieteikties kā) noklikšķiniet uz This Account (Šis konts), ievadiet *NT Authority\NetworkService* un noklikšķiniet uz OK.

  Lai saņemtu plašāku informāciju par SQL Server drošību, apmeklējiet:

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

  un

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

- Ja serverī ir palaists Navision e-biznesa produkts, piemēram, Komercijas risinājums, jānodrošina, ka Komercijas risinājuma pieprasījumu serveris ir pareizi instalēts, izmantojot pakalpojumu noklusēto konta uzstādījumu. Noklusētā konta uzstādījuma nosaukums ir *CGRSUser*, un tas sniedz Komercijas risinājuma serverim piekļuvi minimālajam pārējo nepieciešamo pakalpojumu komplektam, ieskaitot pakalpojumu *MSSQLSERVER* un *BizTalk Service BizTalk Group*: *BizTalkServerApplication*, taču neietverot globālus konta uzstādījumus, kādus ietver, piemēram, konts *Local System*.
- Vienmēr lietojiet stipras paroles. Lai saņemtu plašāku informāciju par stiprām parolēm, skatiet sadaļu Stipras paroles.
- Lietojiet pieteikšanos ar Windows lietotājvārdu. Navision ļauj izveidot divu veidu lietotājvārdus — datu bāzes lietotājvārdus un Windows lietotājvārdus. Mēs iesakām lietot Windows lietotājvārdus, jo tie izmanto Windows autentifikāciju un ļauj realizēt piemērotu paroļu politiku.
- Paroles nedrīkst lietot atkārtoti. Bieži vien parole tiek izmantota vairākās sistēmās un domēnos. Piemēram, administrators, kas atbildīgs par divu domēnu uzturēšanu, abos domēnos izveido kontus Domain Administrator ar vienādām parolēm un domēnu datoros pat uzstāda lokālās administratora paroles, kas sakrīt ar domēna kontu paroli. Ja šādā gadījumā tiek kompromitēts kaut viens konts vai dators, tas var izraisīt visa domēna kompromitēšanu.
- Pēc Navision instalēšanas un datu bāzu izveides vai atjaunināšanas programmā jāizveido Windows lietotājvārds un jāpiešķir tam loma SUPER. Lietotājs SUPER veiks datu bāzes administrēšanu, pārvaldīs drošību utt. Piešķiriet šim lietotājvārdam stipru paroli. Šai parolei jābūt slepenai. Tai jāgarantē tāda pati drošība, kādu esat noteicis SQL Server parolei SA. Visu piekļuvi datu bāzei pārvalda loma SUPER, un tai nepieciešams visaugstākais aizsardzības līmenis. Lietotāja SUPER paroli drīkst zināt tikai sistēmas administratori.
- Visiem pārējiem lietotājiem, kas piekļūst Navision datu bāzei, programma būtu jālieto ar ierobežotām tiesībām. Tas nozīmē, ka tiem piešķirtās lomas ļauj piekļūt tikai tām funkcijām un iespējām, kas tiem nepieciešamas darba uzdevumu veikšanai.
- Nodrošiniet, ka importēt FOB failus, mainīt objektus, veidot un atjaunot datu bāzu dublējumus var tikai tie lietotāji, kuru loma uzņēmumā dod šādas tiesības.
- Regulāri dublējiet Navision datu bāzi un neaizmirstiet testēt dublējumus, lai garantētu, ka vēlāk tos varēs veiksmīgi atjaunot.
- Glabājiet dublējumus drošā vietā, lai samazinātu risku, ka tos var sabojāt uguns, dūmi, putekļi, augsta temperatūra, zibens vai dabas katastrofa (piemēram, zemestrīces).
- Kaut arī programmu Navision var izmantot vairākās Windows versijās, mēs iesakām lietot jaunākās operētājsistēmas ar vismodernākajām drošības funkcijām. Patlaban šādas operētājsistēmas ir Windows XP ar 2. servisa pakotni un Windows Server 2003.
- Lai lietotu visjaunākos drošības atjauninājumus, izmantojiet Windows atjaunināšanas pakalpojumu, kuru sniedz Windows 2000, Windows XP un Windows Server 2003. Izmantojiet Windows automātiskās atjaunināšanas funkciju, lai jūsu klientu datori vienmēr izmantotu jaunākos drošības ielāpus, servisa pakotnes un atjauninājumus.
- Sakaru uzturēšanai starp Navision klientiem un Navision datu bāzes serveri iesakām izmantot drošo TCPS protokolu. TCPS ir droša protokola TCP/IP versija, un tā izmanto Drošības atbalsta sniedzēja interfeisu (SSPI — Security Support Provider Interface) ar aktivizētu šifrēšanu un Kerberos autentifikāciju. TCPS ir Navision datu bāzes servera noklusētais protokols.
- Klientam jāizstrādā atjaunošanas plāns, kas pēc avārijas garantē ātru darba atsākšanu. Atjaunošanas plānam jārisina šādi jautājumi:
  - jaunu/pagaidu iekārtu iegāde.
  - dublējumu atjaunošana jaunajās sistēmās.
  - atjaunošanas plāna efektivitātes pārbaude.

## Fiziskā drošība

Fiziskā drošība ir absolūta nepieciešamība, jo to nevar aizstāt ar programmatūras drošības līdzekļiem. Ja, piemēram, tiek nozagts cietais disks, agrāk vai vēlāk tiek nozagti arī šajā diskā saglabātie faili. Izstrādājot drošības politiku kopā ar klientu, apspriediet šādus ar fizisko drošību saistītus jautājumus:

- Lielām instalācijām uzņēmumos, kuros ir atsevišķas IT nodaļas, serveru telpām un programmatūras glabāšanas vietām jābūt aizslēgtām.
- Šajā kategorijā ietilpst šādi datori:
  - Microsoft SQL Server 2000 serveris.
  - failu serveris, kurā atrodas Navision programmu faili.
- Neautorizēts personāls nedrīkst piekļūt datoriem.
- Neatkarīgi no datu slepenības jābūt uzstādītām pretzagļu signalizācijas sistēmām.
- Dublējumi ar kritiskajiem datiem jāglabā ārpus darba vietas ugunsdrošos konteineros.

## Darbinieki

Ieteicams ierobežot pārvaldības tiesības visos produktos un funkcijās. Pēc noklusējuma klienti saviem darbiniekiem piešķir tikai sistēmas funkciju lasīšanas tiesības, ja vien tiem sava darba pienākumu veikšanai nav nepieciešams vairāk tiesību. Korporācija Microsoft iesaka šādu vismazāko privilēģiju principu: piešķiriet lietotājiem tikai minimālās tiesības, kas nepieciešamas, lai piekļūtu datiem un funkcionalitātei.

Neapmierinātie un bijušie darbinieki rada draudus tīkla drošībai. Apspriežot drošību ar saviem klientiem, attiecībā uz darbiniekiem iesakiet šādu politiku:

- Veikt darbinieku iepriekšējās nodarbošanās izpēti.
- Būt gatavam saņemt “atriebību” no neapmierinātajiem darbiniekiem un bijušajiem darbiniekiem.
- Pārliecināties, vai, darbiniekam aizejot, tiek deaktivizēti visi atbilstošie Windows konti un paroles. Nedzēst lietotājus, bet saglabāt informāciju par tiem. Neizmantot atkārtoti lietotāju kontus.
- Apmācīt lietotājus, lai tie būtu modri un ziņotu par aizdomīgām aktivitātēm.
- Nesniegt tiesības automātiski. Ja lietotājiem nav nepieciešama piekļuve noteiktiem datoriem, datortelpām vai failu kopām, nodrošināt, ka lietotājiem šādas piekļuves nav.
- Apmācīt supervizorus, lai tie identificē un reaģē uz potenciālām darbinieku problēmām.
- Nodrošināt, ka darbinieki izprot savu lomu tīkla drošības uzturēšanā.
- Izsniegt rakstisku informāciju par uzņēmuma politiku katram darbiniekam.
- Neļaut lietotājiem instalēt darba devēja neakceptētu programmatūru.

## Administrators

Klienta sistēmas administratoriem ieteicams sekot līdzi jaunākajiem no Microsoft pieejamajiem drošības labojumiem. Uzbrucēji ļoti lietpratīgi kombinē nelielas kļūdas, lai radītu nopietnu ielaušanos tīklā. Administratoriem vispirms jāpārliecinās, vai katrs atsevišķais dators ir maksimāli drošs, un pēc tam jāpievieno drošības atjauninājumi un pretvīrusu programmatūra. Šajā rokasgrāmatā norādītas daudzas saites un resursi, kas ļauj iegūt vērtīgu informāciju un uzzināt ieteicamo praksi.

Arī komplicētība rada draudus tīkla drošībai. Jo komplicētāks ir tīkls, jo grūtāk ir to padarīt drošu vai izlabot, kad iebrucējs ir veiksmīgi tam piekļuvis. Administratora pienākums ir rūpīgi dokumentēt tīkla topogrāfiju, lai uzturētu to pēc iespējas vienkāršāku.

Drošība, pirmkārt, ir saistīta ar riska pārvaldību. Tā kā ar tehnoloģiju vien nepietiek, drošības nodrošināšanai nepieciešama tehnoloģijas un politikas kombinācija. Runājot citiem vārdiem, nekad netiks izlaists produkts, kuru var vienkārši izpakot un instalēt tīklā, lai tīkls nekavējoties iegūtu pilnīgu drošību. Drošība ir tehnoloģijas un politikas mijiedarbības rezultāts — t.i., tīkla drošības līmeni galu galā nosaka tehnoloģijas izmantošanas veids. Microsoft piedāvā tehnoloģiju un funkcijas, kas atbalsta drošību, taču vienīgi administrators ar jūsu palīdzību var noteikt, kuras politikas katram uzņēmumam ir pareizas. Drošība noteikti jāplāno agrīnā ieviešanas procesa fāzē. Jums jānoskaidro, kādus datus klients vēlas aizsargāt un ko viņš ir gatavs darīt šajā nolūkā.

Visbeidzot izstrādājiet rīcības plānu ārkārtas situācijā, pirms tāda rodas. Apvienojiet rūpīgu plānošanu ar stabilu tehnoloģiju, un jūsu klientam būs lieliska drošība.

Plašāku informāciju par drošību kopumā skatiet publikācijā “The Ten Immutable Laws of Security Administration” (Desmit nemainīgie drošības administrēšanas likumi):
http://www.microsoft.com/technet/archive/community/columns/security/essays/10salaws.mspx

kā arī rakstus par drošības pārvadību:
http://www.microsoft.com/technet/community/columns/secmgmt/smarch.mspx

## Serveru operētājsistēmu drošināšana

Lai arī ir daudz nelielu pasūtītāju, kuri nelieto serveru operētājsistēmas, ir svarīgi, lai jūs izprastu ieteicamo drošības praksi un varētu to darīt zināmu lielākiem pasūtītājiem, kuri darbojas sarežģītākā tīklu vidē. Jums arī jāzina, ka daudzas no šajā dokumentā aprakstītajām politikām un praksēm var viegli piemērot pasūtītājiem, kuri izmanto tikai klienta operētājsistēmas.

Tālāk izskaidrotā koncepcija attiecas gan uz produktu Microsoft Windows 2000 Server, gan Microsoft Windows Server 2003, lai arī šī informācija galvenokārt ir izgūta no Windows Server 2003 tiešsaistes palīdzības. Operētājsistēma Windows Server 2003 piedāvā spēcīgas drošības funkcijas. Windows Server 2003 tiešsaistes palīdzība ietver pilnīgu informāciju par visām drošības funkcijām un procedūrām.

Lai saņemtu papildinformāciju par Windows 2000 Server, apmeklējiet Windows 2000 Server drošības centru:
http://www.microsoft.com/technet/security/prodtech/win2000/default.mspx

kā arī izlasiet Windows 2000 Security Hardening Guide (Windows 2000 drošības uzlabošanas rokasgrāmata):
http://www.microsoft.com/technet/security/prodtech/win2000/win2khg/default.mspx

Lai saņemtu papildinformāciju par Windows Server 2003, *Windows Server 2003 Security Guide* (Windows Server 2003 drošības rokasgrāmata)
http://www.microsoft.com/technet/security/prodtech/win2003/w2003hg/sgch00.mspx

Windows servera galvenās drošības modeļa funkcijas ir autentifikācija, piekļuves kontrole un vienotā pieteikšanās:

- Autentifikācija ir process, kurā sistēma pārbauda lietotāja identitāti, pamatojoties uz pieteikšanās logā norādītajiem akreditācijas datiem. Lietotājvārds un parole tiek salīdzināti ar informāciju autorizācijas sarakstā. Ja sistēma atrod atbilstību, autorizācija nodrošina lietotājam piekļuvi atbilstoši līmenim, kas norādīts šī lietotāja atļauju sarakstā.
- Piekļuves kontrole ierobežo lietotāja piekļuvi informācijai vai datu apstrādes resursiem, pamatojoties uz lietotāja identitāti un to piederību dažādām iepriekš definētām grupām. Piekļuves kontroli sistēmas administratori parasti izmanto, lai kontrolētu lietotāju piekļuvi tīkla resursiem, piemēram, serveriem, direktorijiem un failiem. Šo kontroli parasti ievieš, piešķirot lietotājiem un grupām atļauju piekļūt noteiktiem objektiem.
- Izmantojot vienoto pieteikšanos, lietotājs vienreiz ar savu paroli piesakās Windows domēnā, un tam tiek piešķirta autentifikācija piekļūt jebkuram Windows domēnā esošam datoram. Vienotās pieteikšanās princips ļauj administratoriem ieviest paroļu autentifikāciju visā Windows tīklā, vienlaikus nodrošinot lietotājiem ērtu piekļuvi.

Nākamajās sadaļās šie trīs pamatprincipi aprakstīti plašāk.

## Autentifikācija

Autentifikācija ir fundamentāls sistēmas drošības aspekts. To izmanto, lai apstiprinātu jebkura lietotāja identitāti, kas mēģina pieteikties domēnā vai piekļūt tīkla resursiem. Lielās autentifikācijas sistēmu daļas vājais posms ir lietotāja parole.

Paroles ir pirmā aizsardzības līnija cīņā pret nesankcionētu piekļuvi domēnam un lokālajiem datoriem. Attiecībā uz parolēm iesakiet šādu praksi:

- Vienmēr lietojiet stipras paroles.
- Ja paroles jāpieraksta uz papīra, glabājiet šo papīru drošā vietā un iznīciniet to, kad tas vairs nav nepieciešams.
- Nevienam neizpaudiet savu paroli.
- Dažādiem lietotāju kontiem lietojiet atšķirīgas paroles.
- Mainiet paroles regulāri.
- Esiet piesardzīgs, izvēloties vietu, kur paroles tiek glabātas datoros.

## Stipras paroles

Paroļu loma organizācijas tīklu drošības uzturēšanā bieži vien tiek novērtēta par zemu vai netiek ņemta vērā vispār. Kā minēts iepriekš, paroles ir pirmā aizsardzības līnija cīņā ar nesankcionētu piekļuvi tīklam. Tādēļ jānodrošina, ka klienti dod saviem darbiniekiem norādījumus lietot stirpas paroles.

Taču paroļu uzlaušanas rīki turpina uzlaboties, un datori, kas tiek izmantoti paroļu uzlaušanai, ir jaudīgāki kā jebkad agrāk. Ja automatizētam paroļu uzlaušanas rīkam ļauj darboties pietiekami ilgi, tas var uzlauzt jebkuru paroli. Tomēr stiprās paroles ir daudz grūtāk uzlauzt nekā vājās paroles.

Stipru paroļu veidošanas vadlīnijas, kuras lietotājs var paturēt prātā, sk.

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

un

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

### Paroļu politikas definēšana

Palīdzot savam klientam definēt paroļu politiku, neaizmirstiet izveidot politiku, kas pieprasa visiem lietotāju kontiem izmantot stipras paroles. Vairākumam sistēmu pietiek, ja tiek ievēroti šādi Windows Server 2003 Security Guide (Windows Server 2003 drošības rokasgrāmata) minētie ieteikumi:

- Definējiet politikas uzstādījumu **Enforce password history** (Ievērot paroļu vēsturi), lai tiktu iegaumētas vairākas iepriekš lietotās paroles. Izmantojot šo politikas uzstādījumu, lietotāji pēc paroles derīguma termiņa beigām nevar izmantot kādu no iepriekšējām parolēm.

  Ieteicamais uzstādījums: 24.

- Definējiet politikas uzstādījumu **Maximum password age** (Maksimālais paroles vecums), lai klienta vidē paroļu derīguma termiņš pienāktu tik ātri, cik nepieciešams.

  Ieteicamais uzstādījums: starp 42 (pēc noklusējuma) un 90.

- Definējiet politikas uzstādījumu **Minimum password age** (Minimālais paroles vecums), lai paroles nevarētu mainīt, kamēr tās nav vairākas dienas vecas. Šis politikas uzstādījums darbojas kopā ar politikas uzstādījumu **Enforce password history**. Ja parolei ir noteikts minimālais vecums, lietotāji nevar nomainīt savas paroles vairākas reizes pēc kārtas, lai apietu politikas uzstādījumu **Enforce password history** un izmantotu sākotnējo paroli. Lai mainītu paroli, lietotājiem jāgaida norādītais dienu skaits.

  Ieteicamais uzstādījums: 2.

- Definēt politikas uzstādījumu **Minimum password length** (Paroles minimālais garums), lai paroles nebūtu īsākas par norādīto rakstzīmju skaitu. Garās paroles ar septiņām vai vairāk rakstzīmēm ir efektīvākas par īsajām. Ja tiek izmantots šis politikas uzstādījums, lietotāji nevar lietot tukšas paroles, un viņiem jāveido paroles, kas nav īsākas par norādīto rakstzīmju skaitu.
  Ieteicamais uzstādījums: 8.

- Aktivizējiet politikas uzstādījumu **Password must meet complexity requirements** (Parolei jāatbilst komplicētības nosacījumiem). Šis politikas uzstādījums pārbauda visas jaunās paroles, lai pārliecinātos, vai tās atbilst galvenajām stipru paroļu prasībām. Šis uzstādījums nodrošina, ka paroles rakstzīmes ietilpst vismaz trijās no četrām rakstzīmju kategorijām (augšējais reģistrs, apakšējais reģistrs, cipari

un no burtciparu simboliem atšķirīgās rakstzīmes) un ka šī parole neietver nevienu lietotājvārda, lietotāja vārda vai uzvārda daļu.

**Piezīme**
Šīm prasībām atbilstošās paroles ne vienmēr ir stipras paroles. Piemēram, šīm prasībām atbilst parole “Parole1”.

Ieteicamais uzstādījums: Jā.

- Pilnu šo prasību sarakstu skatiet Windows Server tiešsaistes palīdzības tēmā “Password Must Meet Complexity Requirements” (Parolēm jāatbilst komplicētības nosacījumiem).
- Saglabājiet paroles, izmantojot atgriezenisko šifrēšanu — atgriezenisko šifrēšanu lieto sistēmās, kur lietojumprogrammai jāpiekļūst vienkāršām teksta parolēm. Vairākumam ieviešamo programmu šis uzstādījums nav nepieciešams.

  Ieteicamais uzstādījums: Nē.

Plašāku informāciju skatiet Windows Server 2003 Security Guide:

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

### Kontu bloķēšanas politikas definēšana

Definējot kontu bloķēšanas politiku, jābūt piesardzīgam. Kontu bloķēšanas politiku nekad nevajag ieviest mazos uzņēmumos, jo tā var bloķēt arī autorizētu lietotāju piekļuvi, un tas klientam var dārgi maksāt.

Ja klients izlemj lietot kontu bloķēšanas politiku, uzstādiet uzstādījumam **Account lockout threshold policy** (Kontu bloķēšanas sliekšņa politika) pietiekami lielu vērtību, lai autorizēti lietotāji netiktu bloķēti vienkārši tādēļ, ka tie vairākkārt kļūdījušies, ievadot paroles.

Plašāku informāciju par kontu bloķēšanas politiku skatiet Windows Server tiešsaistes palīdzības tēmā “Account Lockout Policy Overview” (Kontu bloķēšanas politikas apskats).

Informāciju par kontu bloķēšanas politikas lietošanu un modificēšanu skatiet Windows Server tiešsaistes palīdzības tēmā “To Apply or Modify Account Lockout Policy” (Kā lietot vai modificēt kontu bloķēšanas politiku).

## Piekļuves kontrole

Windows tīklu un tā resursus (ieskaitot Navision) var padarīt drošus, izvērtējot lietotāju, lietotāju grupu un citu datoru tiesības tīklā. Vienu vai vairākus datorus var padarīt drošus, piešķirot lietotājiem vai grupām noteiktas lietotāju tiesības. Objektu, piemēram, failu vai mapi, var padarīt drošu, lietotājiem vai grupām piešķirot atļaujas veikt noteiktas darbības ar šo objektu. Piekļuves kontroles pamatjēdzieni ir šādi:

- atļaujas;
- objektu īpašnieki;
- atļauju mantojamība;
- lietotāju tiesības;
- objektu pārbaude.

## Atļaujas

Atļaujas nosaka lietotājam vai grupai piešķirto piekļuves tiesības veidu objektam vai objekta rekvizītam, piemēram, failiem, mapēm vai reģistra objektiem. Atļaujas lieto jebkuram drošam objektam, piemēram, failiem vai reģistra objektiem. Atļaujas var piešķirt jebkuram lietotājam, grupai vai datoram. Ieteicamā prakse ir piešķirt atļaujas grupām.

## Objektu īpašnieki

Kad tiek izveidots objekts, tam tiek piešķirts īpašnieks. Sistēmā Windows 2000 Server pēc noklusējuma īpašnieks ir objekta radītājs. Sistēmā Windows Server 2003 tas ir mainījies attiecībā uz objektiem, kurus izveidojuši grupas Administrators (Administratori) dalībnieki.

Ja grupas Administrators dalībnieks sistēmā Windows Server 2003 izveido objektu, par īpašnieku kļūst grupa Administrators, nevis atsevišķais objektu izveidojušais konts. Šo kārtību var mainīt, sadaļā Local Security Settings iepogai Microsoft Management Console (MMC) izmantojot uzstādījumu **System objects: Default owner for objects created by members of the Administrators group** (Sistēmas objekti: noklusētais īpašnieks objektiem, kurus izveidojuši grupas Administrators dalībnieki). Neatkarīgi no objektam uzstādītajām atļaujām objekta īpašnieks vienmēr šīs atļaujas var mainīt.

Plašāku informāciju skatiet Windows Server 2003 Security Guide tēmā “Ownership” (Īpašnieki).

## Atļauju mantojamība

Mantojamība ļauj administratoriem viegli piešķirt un pārvaldīt atļaujas. Tā liek konteinerā esošiem objektiem automātiski mantot visas konteinera mantojamās atļaujas. Ja, piemēram, mapē izveidojat failus, tie manto mapes atļaujas. Tiek mantotas tikai tās atļaujas, kuras atzīmētas kā mantojamas.

## Lietotāju tiesības

Lietotāju tiesības sniedz lietotājiem un grupām īpašas privilēģijas un pieteikšanās tiesības datoru vidē.

Informāciju par lietotāju tiesībām skatiet Windows Server tiešsaistes palīdzības tēmā “User Rights” (Lietotāju tiesības).

## Objektu pārbaude

Lietotāja piekļuvi objektiem var pārbaudīt. Pēc tam var skatīt drošības žurnālā reģistrētos notikumus, izmantojot programmu Event Viewer (Notikumu skatītājs).

Plašāku informāciju skatiet Windows Server 2003 Security Guide tēmā “Auditing” (Pārbaude).

### Piekļuves kontroles ieteicamā prakse

- Piešķiriet atļaujas grupām, nevis lietotājiem. Tā kā lietotāju kontu tieša uzturēšana ir neefektīva, atļauju piešķiršanai atsevišķiem lietotājiem ir jābūt kā izņēmumam.
- Īpašos gadījumos lietojiet atļauju rekvizītu Deny (Liegt). Piemēram, uzstādījumu Deny izmanto, lai lietotāju grupā izdalītu apakškopu, kuras dalībniekiem tiesības netiek piešķirtas.
- Nekad neliedziet tiesības uz objektu grupai Everyone (Ikviens). Liedzot ikvienam lietotāja atļauju uz šo objektu, tiek iekļauti arī administratori. Labāks risinājums būtu grupu Everyone izdzēst, kamēr vien citiem lietotājiem, grupām un datoriem tiek piešķirtas atļaujas uz šo objektu. Iegaumējiet, ka, ja nav definētas atļaujas, piekļuve ir liegta.
- Piešķiriet atļaujas uz objektu kokā, cik augstu vien iespējams, un pēc tam lietojiet mantojamību, lai izplatītu drošības uzstādījumus pa koku uz leju. Varat ātri un efektīvi lietot piekļuves kontroles uzstādījumus visiem vecākobjekta bērnelementiem vai apakškokiem. Šādi rīkojoties, ar vismazākajiem līdzekļiem tiek panākts vislielākais efekts. Noteiktajiem atļauju uzstādījumiem vajadzētu būt pietiekamiem attiecībā uz vairākumu lietotāju, grupu un datoru.
- Tieši noteiktas atļaujas atsevišķos gadījumos var ignorēt mantotās atļaujas. Mantotais atļauju rekvizīts Deny neliedz piekļuvi uz objektu, ja objektam ir tieši noteiktas atļaujas ieraksts Allow (Atļaut). Tieši noteiktām atļaujām ir priekšrocība pār mantotajām atļaujām — pat pār mantotu atļauju Deny.
- Attiecībā uz Active Directory® objektiem pārliecinieties, vai saprotat Active Directory objektiem raksturīgās ieteicamās prakses.

Plašāku informāciju skatiet Windows Server 2003 tiešsaistes palīdzības tēmā “Best Practices for Assigning Permissions on Active Directory Objects” (Ieteicamās atļauju piešķiršanas prakses Active Directory objektiem).

## Ārējais drošības ugunsmūris

Ugunsmūris ir aparatūra vai programmatūra, kas neļauj datu paketēm ienākt vai iziet no noteikta tīkla. Lai kontrolētu datplūsmu, ugunsmūra porti tiek atvērti vai slēgti informācijas paketēm. Ugunsmūris apskata konkrētus katras datu paketes datus: protokolu, pa kuru pakete tiek piegādāta, paketes nosūtītāju vai saņēmēju, paketē iekļautā satura tipu, kā arī porta numuru, pa kuru pakete tiek nosūtīta. Ja ugunsmūra konfigurācijā ir norādīts, ka norādītais protokols izvēlētajā portā jāakceptē, pakete tiek izlaista cauri. Izdevums Microsoft Windows Small Business Server 2003 Premium Edition tiek piegādāts komplektā ar ugunsmūra risinājumu Microsoft Internet Security and Acceleration (ISA) Server 2000. Izdevums Small Business Server Standard Edition arī ietver ugunsmūri.

# ISA Server 2004

Risinājums Internet Security and Acceleration (ISA) Server 2000 droši maršrutē pieprasījumus un atbildes starp interneta un klienta datoriem iekšējā tīklā.

ISA Server lokālā tīkla klientiem darbojas kā droša vārteja uz internetu. Pārējiem dalībniekiem sakaru ceļš caur ISA Server datoru ir atklāts. Interneta

lietotājs ugunsmūra servera darbību neizjūt, ja vien viņš nemēģina piekļūt pakalpojumam vai doties uz Web vietu, kurai ISA Server dators liedzis piekļuvi. Interneta serveris, kuram piekļūst, saņem ISA Server datora pieprasījumus, it kā pieprasījumu būtu izveidojusi klienta lietojumprogramma.

Ja izvēlaties interneta protokola (IP) fragmentu filtrēšanu, pakešu fragmentu filtrēšanai tiek aktivizēti pakalpojumi Web Proxy un Firewall. Filtrējot pakešu fragmentus, visas fragmentētās IP paketes tiek atmestas. Labi zināms uzbrukums ietver fragmentētu pakešu sūtīšanu, lai pēc tam šīs paketes pārkārtotu, ka tās var nodarīt sistēmai kaitējumu.

Ugunsmūris ISA Server ietver ielaušanās noteikšanas procedūru, kas identificē pret tīklu veikto uzbrukumu mēģinājumus un veic konfigurētu darbību (vai brīdinājumu) kopumu.

Ja ISA Server datorā ir instalēts Internet Information Services (IIS) serveris, tas jākonfigurē nelietot portus, kurus ISA Server ugunsmūris izmanto izejošajiem Web pieprasījumiem (pēc noklusējuma — 8080) un ienākošajiem Web pieprasījumiem (pēc noklusējuma — 80). Piemēram, varat noteikt, ka IIS serverim jāpārrauga ports 81, un pēc tam konfigurēt ISA Server datoru, lai tas pārsūta Web pieprasījumus uz lokālā datora (kurā darbojas IIS) portu 81.

Ja starp ISA Server un IIS lietotajiem portiem rodas konflikts, uzstādīšanas programma aptur IIS publicēšanas pakalpojumu. Pēc tam varat izmainīt IIS pārraugāmo portu un restartēt IIS publicēšanas serveri.

### ISA Server politikas

Varat definēt ISA Server politiku, kas nosaka ienākošo un izejošo piekļuvi. Web vietu un satura kārtulas nosaka, kādām Web vietām un saturam var piekļūt. Protokolu kārtulas norāda, vai konkrētais protokols ir pieejams ienākošajiem un izejošajiem sakariem.

Varat veidot Web vietu un satura kārtulas, protokolu kārtulas, Web publicēšanas kārtulas un IP pakešu filtrus. Šīs politikas nosaka procedūru, kā ISA Server klienti veido interneta sakarus, kā arī atļautos sakaru veidus.

## Pretvīrusu aizsardzība

Datorvīruss ir izpildāms fails, kas izveidots ar nolūku sevi pavairot, izdzēst vai sabojāt datu failus un programmas un palikt neidentificētam. Patiesībā vīrusi bieži tiek pārrakstīti un pielāgoti, lai tos nevarētu identificēt. Vīrusus bieži nosūta kā e-pasta pielikumus. Lai pretvīrusu programmas meklētu jaunos un modificētos vīrusus, tās nemitīgi jāatjaunina. Vīrusi ir galvenais datorvandālisma veids.

Pretvīrusu programmatūra ir īpaši izstrādāta, lai atrastu vīrusu programmas un novērstu to darbību. Tā kā jaunas vīrusu programmas tiek radītas nepārtraukti, daudzi pretvīrusu produktu veidotāji saviem pircējiem piedāvā periodiski

atjaunināt programmatūru. Microsoft iesaka nekavējoties ieviest klienta vidē pretvīrusu programmatūru.

Vīrusu programmatūra parasti tiek instalēta katrā no šīm trijām vietām: lietotāju darbstacijās, serveros, kā arī tīkla vietā, pa kuru organizācijā ienāk (un dažos gadījumos — iziet) e-pasts.

## Vīrusu veidi

Ir trīs galvenie datorsistēmas inficējošo vīrusu veidi: sāknēšanas sektora vīrusi, failus inficējošie vīrusi un Trojas zirga programmas.

### Sāknēšanas sektora vīrusi

Datoram startējoties, pirms operētājsistēmas vai citu startēšanas failu ielādes tas skenē cietā diska sāknēšanas sektoru. Sāknēšanas sektora vīruss ir veidots tā, ka tas aizstāj cietā diska sāknēšanas sektoros esošo informāciju ar savu kodu. Ja dators ir inficēts ar sāknēšanas sektora vīrusu, vispirms atmiņā tiek ielasīts vīrusa kods. Kad vīruss ir iekļuvis atmiņā, tas var sevi pavairot citos inficētajā datorā izmantotajos diskos.

### Failus inficējošie vīrusi

Visbiežāk sastopamais vīrusu veids ir failus inficējošais vīruss, kas pievienojas izpildprogrammas failam, papildinot faila kodu ar savējo. Vīrusa kods parasti tiek pievienots tā, ka tas netiek identificēts. Kad inficētais fails tiek palaists, vīruss var pievienoties citiem izpildāmajiem failiem. Ar šo vīrusa veidu inficētajiem failiem parasti ir paplašinājums .com, .exe vai .sys.

Daži failus inficējošie vīrusi ir izstrādāti noteiktām programām. Programmu tipi, kuri bieži tiek pakļauti vīrusiem, ir pārklājuma (.ovl) vai dinamisko saišu bibliotēku (.dll) faili. Lai arī šie faili netiek palaisti, izpildāmie faili tos izsauc. Vīruss tiek nodots izsaukuma brīdī.

Kaitējums datiem notiek, kad vīruss tiek iedarbināts. Vīrusu var iedarbināt, ja tiek palaists inficētais fails vai arī izpildās konkrēts vides uzstādījums (piemēram, iestājas noteikts sistēmas datums).

### Trojas zirga programmas

Trojas zirga programma nav gluži vīruss. Galvenā atšķirība starp vīrusu un Trojas zirga programmu ir tā, ka Trojas zirga programma sevi nepavairo — tā tikai iznīcina cietajā diskā esošo informāciju. Trojas zirga programma maskējas kā parasta programma, piemēram, spēle vai utilīta. Taču, to palaižot, tiek iznīcināti vai sabojāti dati.

## Pretvīrusu aizsardzības ieteicamās prakses

Makro vīrusu izplatīšanos var novērst. Šeit sniegti daži padomi, kā novērst inficēšanos. Iepazīstiniet ar tiem savus klientus:

- Instalējiet pretvīrusu aizsardzības risinājumu, kas skenē no interneta ienākošos ziņojumus pirms to nodošanas maršrutētājam. Tādējādi tiek nodrošināts, ka e-pasta ziņojumos tiek veikta pretvīrusu skenēšana.
- Pārliecinieties, vai saņemto dokumentu nosūtītājs ir zināms. Nevajadzētu atvērt dokumentus, kurus nav nosūtījusi klienta uzticības cienīga persona.
- Aprunājieties ar dokumenta autoru. Ja lietotāji nav pārliecināti, ka dokuments ir drošs, tiem vajadzētu sazināties ar personu, kas dokumentu izveidoja.
- Lietojiet Microsoft Office makro pretvīrusu aizsardzību. Office lietojumprogrammas brīdina lietotāju, ka dokumentā ir makro. Šī funkcija ļauj lietotājam dokumenta atvēršanas laikā aktivizēt vai deaktivizēt makro.
- Izmantojiet pretvīrusu skenēšanas programmatūru, lai atrastu un noņemtu makro vīrusus. Pretvīrusu skenēšanas programmatūra var atrast dokumentā vīrusus un bieži vien arī atbrīvot dokumentu no tiem. Korporācija Microsoft iesaka lietot pretvīrusu programmatūru, kuru ir sertificējusi Starptautiskā datoru drošības asociācija (International Computer Security Association — ICSA).

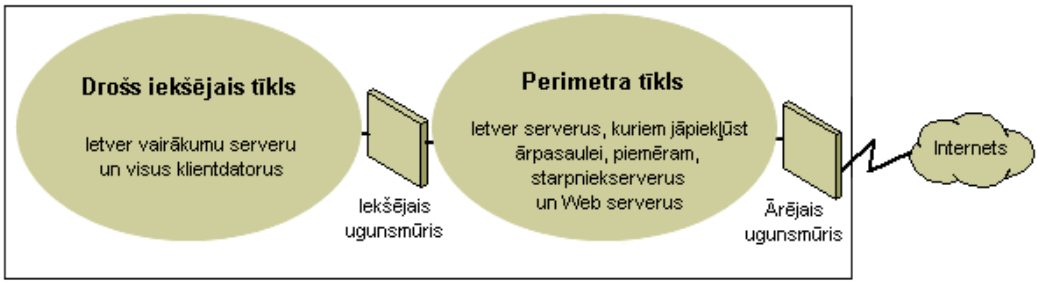
Plašāku informāciju par vīrusiem un datoru drošību kopumā skatiet šādās Microsoft drošības Web vietās:

- Microsoft drošība: http://www.microsoft.com/security/default.asp
- Drošības dokumentācija Microsoft TechNet Web vietā: http://www.microsoft.com/technet/security/Default.mspx

## Tīkla drošības stratēģijas

Tā kā pirms IP starptīklošanas vides izstrādes un ieviešanas jāsaskaņo privātie un ar publisko tīklu saistītie apsvērumi, ugunsmūris ir kļuvis par galveno komponentu tīkla integritātes nodrošināšanā. Ugunsmūris nav viens komponents. Nacionālā datoru drošības asociācija (National Computer Security Association — NCSA) definē ugunsmūri kā "sistēmu vai sistēmu kombināciju, kas veido robežu starp diviem vai vairākiem tīkliem". Lai arī tiek izmantoti atšķirīgi termini, šī robeža tiek saukta arī par perimetra tīklu. Perimetra tīkls pasargā iekštīklu vai uzņēmuma lokālo tīklu (local area network — LAN) no iebrukumiem, kontrolējot piekļuvi no interneta vai citiem lieliem tīkliem.

Šajā diagrammā ir parādīts perimetra tīkls, kas atdalīts ar ugunsmūriem un novietots starp privāto tīklu un internetu, lai privāto tīklu padarītu drošu.




**Principiālā perimetra tīkla shēma**

Organizācijām ir atšķirīga pieeja ugunsmūru izmantošanā, lai panāktu drošību. IP pakešu filtrēšana sniedz nepietiekamu drošību, tā ir neērti pārvaldāma

un viegli pārvarama. Lietojumprogrammu vārtejas ir drošākas par pakešu filtriem un ir vieglāk pārvaldāmas, jo tās attiecas tikai uz dažām noteiktām lietojumprogrammām, piemēram, konkrētu e-pasta sistēmu. Shēmu vārtejas ir visefektīvākās, ja lielāka uzmanība ir jāpievērš tīkla lietojumprogrammas lietotājam, nevis datiem, kurus lietojumprogramma apstrādā. Starpniekserveris ir visaptverošs drošības rīks, kas ietver lietojumprogrammu vārteju, drošu piekļuvi anonīmiem lietotājiem un citus pakalpojumus. Šeit sniegta informācija par šīm atšķirīgajām iespējām:

- **IP pakešu filtrēšana**
  IP pakešu filtrēšana bija pirmā ugunsmūra tehnoloģijas realizācija. Pakešu virsrakstos tiek pārbaudītas avota un adresāta adreses, pārraides vadības protokola (Transmission Control Protocol — TCP) un lietotāja datagrammu protokola (UDP) portu numuri, kā arī cita informācija. Pakešu filtrēšana ir ierobežota tehnoloģija, kas vislabāk strādā caurredzamas drošības vidēs, kur, piemēram, visi ārpus perimetra tīkla esošie dati tiek uzskatīti par neuzticamiem, bet visi iekšpusē esošie dati — par uzticamiem. Pēdējos gados vairāki izstrādātāji ir uzlabojuši pakešu filtrēšanas metodi, pievienojot pakešu filtrēšanas kodolam inteliģentas lēmumu pieņemšanas funkcijas, tādējādi radot jaunu pakešu filtrēšanas formu, ko dēvē par *protokolu stāvokļa pārbaudi* (stateful protocol inspection). Izmantojot pakešu filtrēšanu, var konfigurēt, ka noteikta veida paketes jāakceptē, bet visas pārējās jānoraida, vai arī noteikta veida paketes jānoraida, bet visas pārējās jāakceptē.
- **Lietojumprogrammu vārtejas**
  Lietojumprogrammu vārtejas izmanto, ja vislielākā uzmanība jāpievērš lietojumprogrammas faktiskajam saturam. Piesaiste konkrētām lietojumprogrammām ir vienlaikus priekšrocība un ierobežojums, jo šādas vārtejas nav viegli pielāgojamas tehnoloģijas izmaiņām.
- **Shēmu vārtejas**
  Shēmu vārtejas ir tuneļi, kas iebūvēti ugunsmūrī un savieno specifiskus procesus vai sistēmas vienā galā ar specifiskiem procesiem vai sistēmām otrā galā. Shēmu vārtejas vislietderīgāk ir izmantot situācijās, kad persona, kas izmanto lietojumprogrammu, potenciāli rada lielāku risku nekā lietojumprogrammā apstrādājamā informācija. Shēmu vārtejas atšķirībā no pakešu filtriem spēj izveidot savienojumu ar ārpus joslas esošu lietojumprogrammu shēmu, kurā var būt ietverta papildu informācija.
- **Starpniekserveri**
  Starpniekserveri ir visaptveroši drošības rīki ar ugunsmūra un lietojumprogrammu vārtejas funkcionalitāti, kas pārvalda lokālajā tīklā ienākošo un no tās izejošo datplūsmu. Starpniekserveri ļauj arī kešot dokumentus un kontrolēt piekļuvi. Starpniekserveris var uzlabot veiktspēju, kešojot un tieši iesniedzot bieži pieprasītus datus, piemēram, populāru Web vietu. Starpniekserveris var arī filtrēt un atmest pieprasījumus, kurus īpašnieks uzskata par nepiemērotiem, piemēram, nesankcionētas piekļuves pieprasījumus īpašnieka failiem.

Nodrošiniet, ka klients izmanto tās ugunsmūra drošības funkciju priekšrocības, kas viņam var būt noderīgas. Tīkla topoloģijā novietojiet perimetra tīklu vietā, kur atrodas ārējā ugunsmūra uzturētais perimetrs un kura jāšķērso visai no korporatīvā tīkla ārpuses nākošajai datplūsmai. Varat pielāgot piekļuvi ugunsmūrim tā, ka tas atbilst klienta vajadzībām, kā arī konfigurēt ugunsmūri tā, ka tas ziņo par jebkuru nesankcionētas piekļuves mēģinājumu.

Lai minimizētu portu daudzumu, kuri jāatver iekšējā ugunsmūrī, varat izmantot lietojumprogrammu līmeņa ugunsmūri, piemēram, ISA Server 2000.

Plašāku informāciju par TCP/IP skatiet rakstā “Designing a TCP/IP Network” (TCP/IP tīkla izstrāde)
http://www.microsoft.com/resources/documentation/WindowsServ/2003/all/deployguide/en-us/dnsbb_tcp_overview.asp

## Bezvadu tīkli

Pēc noklusējuma bezvadu tīklu konfigurācija pieļauj bezvadu signālu “noklausīšanos”. Ja ļaunprātīga nepiederoša persona iegūst piekļuvi, šādi tīkli var izrādīties viegli ievainojami dažu bezvadu aparatūras noklusēto uzstādījumu, bezvadu tīklu pieejamības un pašreizējo šifrēšanas metožu dēļ. Pastāv konfigurācijas opcijas un rīki, kas var pasargāt no “noklausīšanās”, taču paturiet prātā, ka tie nedara neko, lai pasargātu datorus no urķiem un vīrusiem, kas ienāk pa interneta savienojumu. Tāpēc ir ārkārtīgi svarīgi iekļaut ugunsmūri, lai datorus internetā pasargātu no nevēlamiem iebrucējiem.

Papildu informāciju par bezvadu tīklu aizsardzību skatiet rakstā “How to Make Your 802.11b Wireless Home Network More Secure” (Kā padarīt 802.11b bezvadu mājas tīklu drošāku): http://support.microsoft.com/default.aspx?scid=kb;en-us;309369

## Tīkla drošības scenāriji

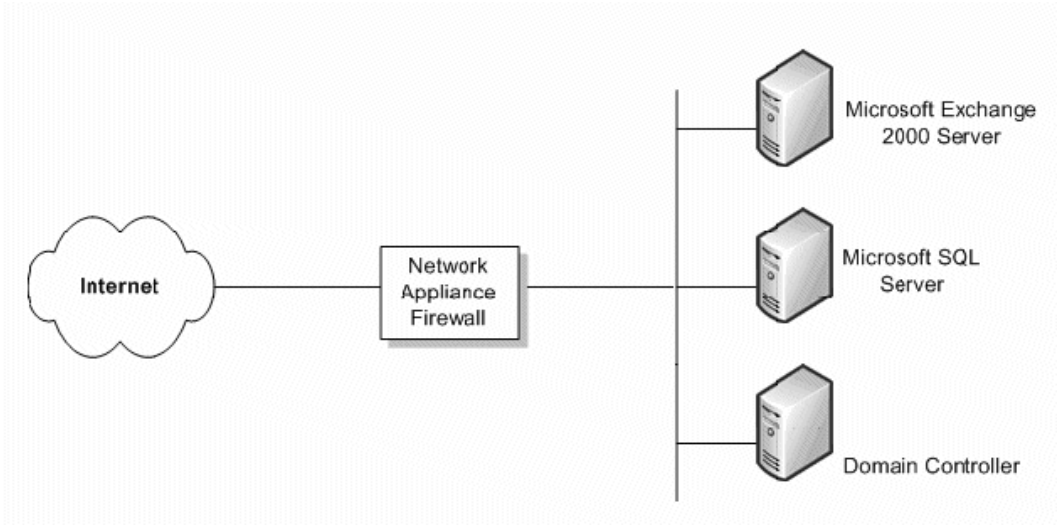
Klienta organizācijai nepieciešamās tīkla drošības līmenis ir atkarīgs no vairākiem faktoriem. Parasti galvenais uzdevums ir panākt kompromisu starp budžetu un nepieciešamību pasargāt uzņēmuma datus. Maziem uzņēmumiem var uzstādīt ļoti komplicētu drošības struktūru, kas sniedz visaugstāko iespējamo tīkla drošības līmeni, taču mazi uzņēmumi parasti nevar atļauties tāda līmeņa drošību. Šajā sadaļā ir aplūkoti četri scenāriji un sniegti ieteikumi par katru no tiem. Šie scenāriji piedāvā atšķirīgus drošības līmeņus.

### Bez ugunsmūra

Ja klientam ir interneta savienojums, taču nav ugunsmūra, ir jāievieš kāds tīkla drošības līdzeklis. Tās ir vienkāršas tīkla ugunsmūra šaurierīces, kas sniedz pietiekamu drošību, lai atturētu vairākumu potenciālo urķu.

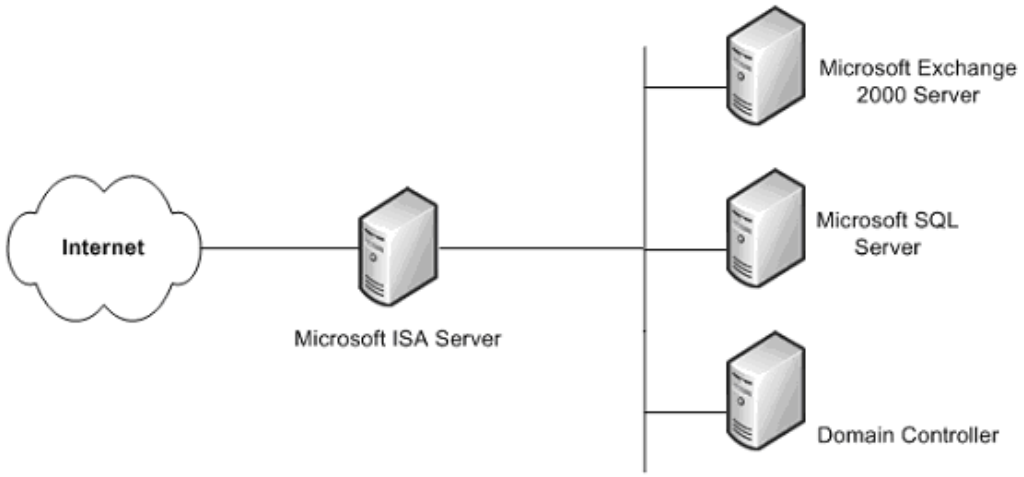
### Viens vienkāršs ugunsmūris

Minimālais ieteicamais drošības līmenis ir viens ugunsmūris starp internetu un jūsu klienta datiem. Šis ugunsmūris īpaši neuzlabo drošību, tāpēc tas nav uzskatāms par pietiekami drošu. Taču tas ir labāk nekā nekas.




**Vienkāršs ugunsmūris**

Cerams, ka klienta budžets ļauj uzstādīt drošāku risinājumu, kas pasargās uzņēmuma datus. Viens no tādiem risinājumiem ir ISA Server. Papildu serveris attaisno pieaugušās izmaksas, sniedzot ievērojami augstāku drošības līmeni nekā vidusmēra ugunsmūris, kas parasti piedāvā tikai tīkla adrešu translēšanu (network address translation — NAT) un pakešu filtrēšanu.




**ISA Server ugunsmūris**

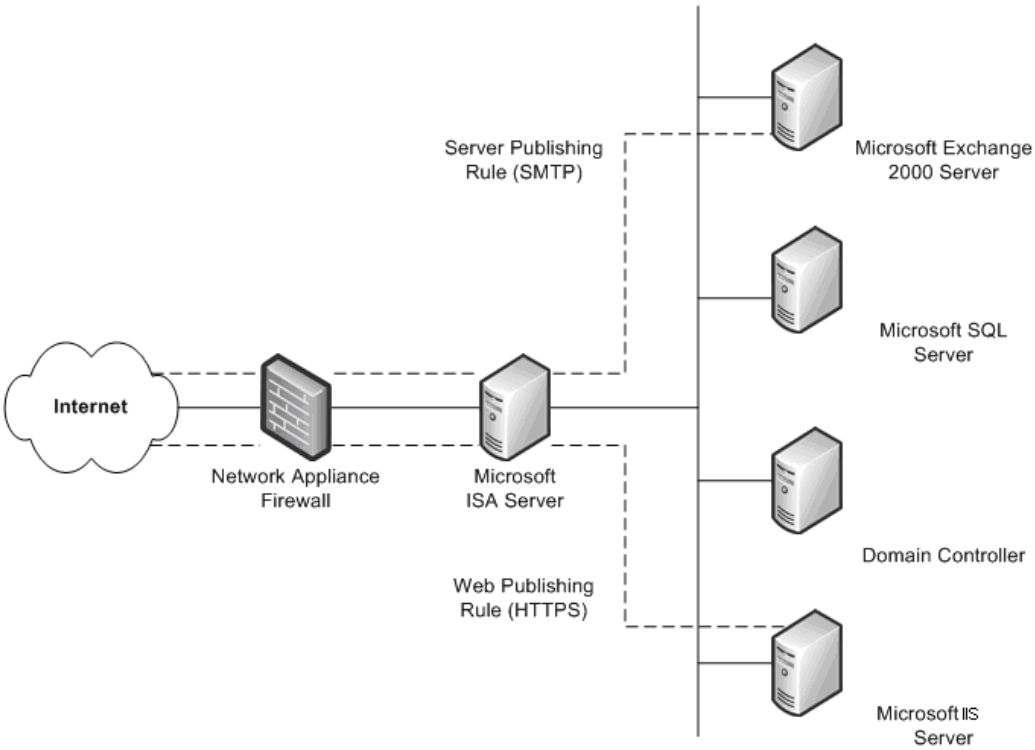
Šeit parādītais viena ugunsmūra risinājums ir drošāks nekā sākotnējā līmeņa ugunsmūra šaurierīce un piedāvā sistēmai Windows raksturīgus drošības pakalpojumus.

## Viens esošs ugunsmūris

Ja klientam jau ir uzstādīts ugunsmūris, kas atdala iekštīklu no interneta, ieteicams pievienot papildu ugunsmūri, kas sniedz vairākas iespējas iekšējo resursu konfigurēšanai attiecībā uz internetu.

Viens no šādiem paņēmieniem ir Web publicēšana. To izmanto, ja ISA Server ir izvietots pirms organizācijas Web servera, kas sniedz piekļuvi interneta lietotājiem. Ienākot Web pieprasījumiem, ISA Server funkcionē kā Web serveris un izpilda klienta Web satura pieprasījumus no kešatmiņas. ISA Server pārsūta pieprasījumus uz Web serveri tikai tad, ja pieprasījumu nevar apkalpot, izmantojot kešatmiņu.

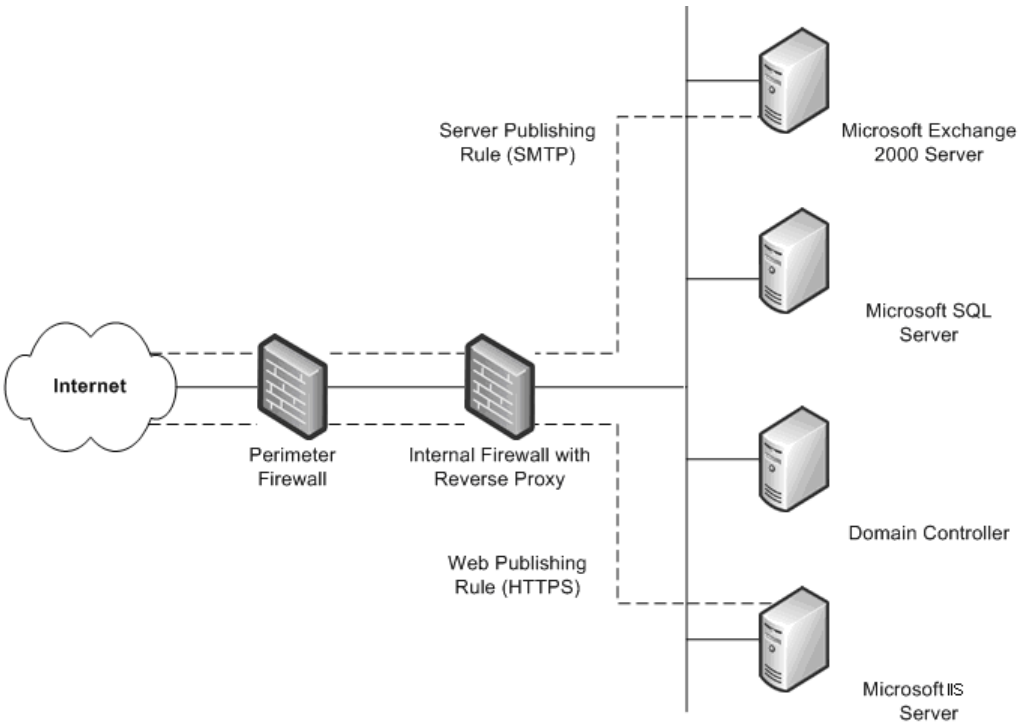
Cits paņēmiens ir servera publicēšana. ISA Server ļauj internetā publicēt iekšējos serverus, nekompromitējot iekšējo tīklu drošību. Varat konfigurēt Web publicēšanas un serveru publicēšanas noteikumus, kas nosaka, kuri pieprasījumi jānosūta lokālajā tīklā esošam serverim, un tādējādi iekšējiem serveriem sniedz uzlabotu drošību.




**Esošs ugunsmūris ar pievienotu ISA Server**

## Divi esoši ugunsmūri

Ceturtajā scenārijā organizācijai ir divi ugunsmūri ar izveidotu perimetra tīklu (demilitarizētā zona). Viens vai vairāki serveri nodrošina reversā starpniekservera pakalpojumus, lai interneta klienti nepiekļūtu iekštīkla serveriem tieši. Tā vietā viens no ugunsmūriem (ideālajā gadījumā — iekšējais ugunsmūris) pārtver iekšējiem serveriem paredzētos pieprasījumus, pārbauda šīs paketes un pēc tam pārsūta tās interneta resursdatora vietā.




**Divi esoši ugunsmūri**

Šis scenārijs ir līdzīgs iepriekšējam scenārijam pēc otrā ugunsmūra pievienošanas. Vienīgā atšķirība ir tā, ka iekšējais ugunsmūris, kas atbalsta reverso starpniekserveri, nav ISA Server. Lai šajā scenārijā atbilstoši drošības politikai definētu serveru publicēšanas kārtulas, jums cieši jāsadarbojas ar katra konkrētā ugunsmūra administratoriem.

## Drošības ielāpu pārvaldība

Operētājsistēmas un lietojumprogrammas bieži vien ir ārkārtīgi sarežģītas. Tās var sastāvēt no miljoniem koda rindu, kuras rakstījuši dažādi programmētāji. Ir svarīgi, lai programmatūra darbotos uzticami un nekompromitētu IT vides drošību un stabilitāti. Lai minimizētu problēmu rašanos, programmas pirms izlaišanas tiek pamatīgi testētas. Taču uzbrucēji nepārtraukti cenšas atrast programmatūras vājās vietas, un paredzēt visus nākotnē iespējamos uzbrukumus nav iespējams.

Daudzās organizācijās ielāpu pārvaldība ir daļa no vispārējās izmaiņu un konfigurēšanas vadības stratēģijas. Taču neatkarīgi no organizācijas veida un lieluma ir svarīgi, lai būtu labas ielāpu pārvaldības stratēģija, pat ja organizācijā vēl nav ieviesta izmaiņu un konfigurēšanas vadība. Vairākums veiksmīgo uzbrukumu tiek veikti pret datorsistēmām, kurās nav instalēti drošības ielāpi.

Drošības ielāpi vairākumam organizāciju rada specifisku izaicinājumu. Parasti, tikko programmatūrā tiek atklāta vājā vieta, uzbrucēji šo informāciju ātri izplata urķu aprindās. Kad korporācijas Microsoft programmatūrā tiek atklāts drošības trūkums, tā cenšas nekavējoties izlaist ielāpu. Kamēr ielāps nav instalēts, drošības līmenis, no kura klients ir atkarīgs un uz kuru paļaujas, var ievērojami pazemināties.

Navision vidē jānodrošina, ka visur klientu sistēmās ir instalēti jaunākie drošības ielāpi. Pārliecinieties, vai klients izmanto kādu no Microsoft piedāvātajām tehnoloģijām. Tādas ir vairākas:

- **Microsoft drošības ziņojumu pakalpojums**
  Drošības ziņojumu pakalpojums ir e-pasta kopa, kurā tiek izplatīta informācija par atjauninājumiem, tiklīdz tie ir pieejami. Šie ziņojumi kalpo kā vērtīgs profilaktiskās drošības stratēģijas elements. Tie ir pieejami arī TachNet produktu drošības ziņojumu Web vietā: http://www.microsoft.com/technet/security/bulletin/notify.mspx

- **Microsoft automātiskā atjaunināšana**
  Sistēma Windows var automātiski instalēt jūsu datoros drošības atjauninājumus.

- **Microsoft drošības biļetenu meklēšanas rīks**
  Drošības biļetenu meklēšanas rīks ir pieejams drošības biļetena pakalpojuma Web vietā: http://www.microsoft.com/technet/security/current.aspx. Klients pats var noteikt nepieciešamos jauninājumus atkarībā no operētājsistēmas, lietojumprogrammām un servisa pakotnēm, kuras tas pašlaik izmanto.

- **Microsoft Baseline Security Analyzer (MBSA)**
  Microsoft Baseline Security Analyzer Web vietā ir pieejams šis grafiskais rīks: http://www.microsoft.com/technet/security/tools/mbsahome.mspx. Šis rīks darbojas, salīdzinot datora pašreizējo stāvokli ar Microsoft uzturēto atjauninājumu sarakstu. Pakalpojums MBSA arī pārbauda vairākus drošības pamata uzstādījumus — paroļu stiprumu un derīguma termiņus, viesu kontu politikas, kā arī dažus citus. Pakalpojums MBSA meklē Microsoft Internet Information Services (IIS), SQL Server™ 2000, Exchange 5.5, Exchange 2000 un Exchange Server 2003 vājās vietas.

- **Microsoft programmatūras atjaunināšanas pakalpojumi (Software Update Services — SUS)**
  Šis rīks, kas iepriekš bija pazīstams ar nosaukumu Windows Update Corporate Edition (Windows atjaunināšanas korporatīvais risinājums), ļauj uzņēmumiem lokālajos datoros hostēt visus kritiskos atjauninājumus un drošības atjauninājumu pakotnes (security rollup packages — SRPs), kas publiski pieejamas Web vietā Windows Update. Šis rīks strādā kopā ar jaunajiem automātiskās atjaunināšanas (automatic updates — AU) klientiem, veidojot pamatu jaudīgai automātiskās lejupielādes un instalēšanas stratēģijai. Jaunais AU klienta komplekts ietver operētājsistēmu Windows 2000 un Windows Server 2003 klientu, un tam ir iespēja automātiski instalēt lejupielādētos atjauninājumus. Plašāku informāciju par Microsoft SUS skatiet http://www.microsoft.com/windows2000/windowsupdate/sus/default.asp

- **Microsoft Systems Management Server (SMS) programmatūras atjaunināšanas pakalpojumu funkcionalitātes pakotne**
  SMS programmatūras atjaunināšanas pakalpojumu funkcionalitātes pakotnē ir vairāki rīki, lai atvieglotu programmatūras atjauninājumu ieviešanu visā uzņēmumā. Rīki ir šādi: jauninājumu uzskaites rīks Security Update Inventory Tool, Office atjauninājumu uzskaites rīks Microsoft Office Inventory Tool for Updates, atjauninājumu ieviešanas vednis Distribute Software Updates Wizard, kā arī pārskatu veidošanas rīks SMS Web Reporting Tool ar programmatūras atjauninājumu pievienojumprogrammu Web Reports. Plašāku informāciju par Microsoft SUS skatiet http://www.microsoft.com/smserver/downloads/20/featurepacks/suspack/

Pārrunājiet ar klientiem šo rīku izmantošanas iespējas un mudiniet viņus šos rīkus lietot. Ir svarīgi, lai drošības jautājumi tiktu atrisināti pēc iespējas ātrāk, vienlaikus saglabājot vides stabilitāti.

# SQL Server 2000 drošības uzstādījumi

Tā kā programma Navision tiek izmantota arī SQL Server 2000 vidē, ir svarīgi veikt pasākumus, kas uzlabotu klienta SQL Server 2000 instalācijas drošību. Lai uzlabotu SQL Server drošību, rīkojieties šādi:

- Pārliecinieties, vai ir instalēta jaunākā operētājsistēma un SQL Server 2000 servisa pakotnes un atjauninājumi. Plašāku informāciju meklējiet Microsoft Security Web vietā http://www.microsoft.com/security/default.asp
- Attiecībā uz failu drošību sistēmas līmenī pārliecinieties, vai visi SQL Server 2000 dati un sistēmfaili tiek instalēti NTFS nodalījumos. Nodrošiniet, lai šiem failiem varētu piekļūt tikai administratori un sistēmas līmeņa lietotāji ar NTFS atļaujām. Tas aizsargās pret lietotājiem, kas piekļūst šiem failiem laikā, kad nav palaists pakalpojums MSSQLSERVER.
- Pakalpojumam SQL Server 2000 (MSSQLSERVER) izmantojiet domēna kontu ar nelielām tiesībām, piemēram, NT Authority\Network Service vai LocalSystem (ieteicams). Šim kontam jāpiešķir minimālas tiesības domēnā, lai tādējādi ierobežotu (bet neapturētu) uzbrukumu serverim kompromitēšanas gadījumā. Citiem vārdiem sakot, kontam domēnā jāpiešķir tikai lokālās lietotāju līmeņa tiesības. Ja SQL Server 2000 pakalpojumu veikšanai izmanto kontu Domain Administrator, servera kompromitēšanas gadījumā izraisīs visa domēna kompromitēšanu. Lai mainītu šo uzstādījumu, izmantojiet programmu SQL Server Enterprise Manager. Piekļuves kontrolsaraksti (Access control lists — ACLs) failiem, reģistram un lietotāju tiesībām tiks mainīti automātiski.
- Vairākums programmatūras SQL Server 2000 redakciju tiek instalēts ar divām noklusētajām datu bāzēm **Northwind** un **pubs**. Abas datu bāzes ir piemēra datu bāzes, ko izmanto testēšanai, apmācībai un demonstrēšanai. Šīs datu bāzes nav jāievieš uzņēmuma sistēmā. Apziņa, ka ir uzstādītas šīs datu bāzes, var veicināt uzbrucēja vēlmi meklēt vājās vietas, lietojot noklusētos uzstādījumus un konfigurāciju. Ja SQL Server 2000 datorā ir uzstādītas datu bāzes **Northwind** un **pubs**, tās ir jāizdzēš.
- SQL Server 2000 auditēšana pēc noklusējuma ir deaktivizēta, tādēļ nekādi nosacījumi netiek pārbaudīti. Tas sarežģī iebrukuma konstatāciju un palīdz uzbrucējam slēpt pēdas. Aktivizējiet vismaz neveiksmīgo pieteikšanās mēģinājumu pārbaudes.

Jaunāko ar SQL Server 2000 saistīto drošības informāciju skatiet http://www.microsoft.com/sql/techinfo/administration/2000/security/default.asp

# Par Microsoft Business Solutions

Korporācijas Microsoft apakšvienība Microsoft Business Solutions piedāvā plašu integrētu, vispusīgu biznesa lietojumprogrammu un pakalpojumu klāstu, kas maziem, vidējiem un lieliem uzņēmumiem palīdz veidot ciešāku saikni ar klientiem, darbiniekiem, partneriem un piegādātājiem. Microsoft Business Solutions radītās lietojumprogrammas optimizē finanšu pārvaldības, analīzes, cilvēkresursu, projektu, klientu attiecību, servisa, piegādes ķēžu, e-komercijas, ražošanas un tirdzniecības pārvaldības stratēģiskos biznesa procesus. Lietojumprogrammas ir veidotas tā, lai klienti varētu izvērtēt savu biznesu un sekmētu turpmākos panākumus. Plašāku informāciju par Microsoft Business Solutions meklējiet šeit: http://www.microsoft.com/BusinessSolutions/

Šī ir dokumenta sagatavošanas versija, un pirms galējā šeit aprakstītās programmatūras laidiena tā būtiski mainīties.

Šajā dokumentā iekļautā informācija atspoguļo korporācijas Microsoft viedokli par izklāstītajiem jautājumiem publikācijas brīdī. Tā kā korporācijai Microsoft ir jāreaģē uz mainīgo tirgus situāciju, šis dokuments nav uzskatāms par saistošu korporācijai Microsoft, kā arī korporācija Microsoft nevar garantēt pēc publicēšanas datuma sniegtās informācijas precizitāti.

Šim materiālam ir tikai informatīvs raksturs. ŠAJĀ DOKUMENTĀ MICROSOFT NESNIEDZ NE TIEŠAS, NE NETIEŠAS GARANTIJAS.

Atbilstība piemērojamajiem autortiesību likumiem ir lietotāja atbildība. Neierobežojot autortiesībās noteiktās tiesības, nevienu šī dokumenta daļu nedrīkst pavairot, saglabāt vai ievietot teksta izgūšanas sistēmā, pārsūtīt jebkādā formā un izmantojot jebkādus līdzekļus (elektroniskus, mehāniskus, fotokopēšanu, ierakstīšanu vai citus) nekādiem mērķiem bez korporācijas Microsoft skaidri izteiktas rakstiskas atļaujas.

Korporācijai Microsoft var būt patenti, patentu pieteikumi, autortiesības vai citas intelektuālā īpašuma tiesības, kas skar šī dokumenta saturu. Ja tas nav norādīts korporācijas Microsoft rakstiskā licences līgumā, šī dokumenta pielāgošana nepiešķir licenci uz šiem patentiem, preču zīmēm, autortiesībām vai citu intelektuālo īpašumu.

© 2003 Microsoft Business Solutions ApS (Dānija). Visas tiesības paturētas.

Microsoft, Great Plains, Navision ir Microsoft Corporation vai Great Plains Software, Inc. Software Corporation, vai Microsoft Business Solutions ApS, vai to filiāļu reģistrētas preču zīmes vai preču zīmes ASV un/vai citās valstīs. Great Plains Software, Inc. un Microsoft Business Solutions ApS ir korporācijas Microsoft meitasuzņēmumi. Šajā materiālā minēto reālo uzņēmumu un produktu nosaukumi, iespējams, ir to īpašnieku preču zīmes. Piemēros minētie uzņēmumi, organizācijas, produkti, personas un notikumi ir izdomāti. Nav paredzēts, lai piemēri radītu, un tiem nav jārada asociācijas ar kādu reālu uzņēmumu, organizāciju, produktu, personu vai notikumu.