Microsoft Business Solutions

Navision Security Hardening Guide

Išleista: 2004 m. spalio mėn.

Microsoft

Turinys

Įvadas

Microsoft® Windows® teikia modernią standartais paremtą tinklo saugą. Plačiausia prasme sauga apima planavimą ir reikiamo rezultato siekimą. Pavyzdžiui, kompiuteris gali būti užrakintas saugykloje ir prieinamas tik vienam sistemos administratoriui. Gal šis kompiuteris ir saugus, tačiau jis nelabai naudingas, nes nėra prijungtas prie jokio kito kompiuterio. Jums reikia kaip įmanoma apsaugoti tinklą nesumažinant gaunamos naudos.

Dauguma organizacijų rengiasi antpuoliams iš išorės ir kuria užkardas, tačiau daug įmonių neatsižvelgia į galimybę sumažinti saugos pažeidimus, kai įsilaužėlis peržengia užkardą. Kliento aplinkoje saugos priemonės bus efektyvios jeigu vartotojams nereikės imtis daugybės procedūrų, kad darbai būtų atliekami saugiai. Saugos strategijas taikyti turėtų būti kaip įmanoma paprasčiau, kitaip vartotojai ras mažiau saugių būdų tvarkyti reikalus.

Programos „Navision“ diegimo dydis gali labai skirtis, todėl svarbu gerai apmąstyti kiekvieno kliento poreikius ir įvertinti saugos priemonių, kurios gali daug kainuoti, efektyvumą. Būdami patikimi kliento patarėjai, siūlykite patikimiausią sprendimą ir strategiją, atitinkančius kliento saugos poreikius, nesukurdami naštos, kuri atbaidys klientą nuo saugos strategijos naudojimo.

Geriausia „Navision“ saugos praktika

Toliau pateikiamos bendrosios taisyklės padės padidinti „Navision“ aplinkos saugą:

- Jeigu norite paleisti „Navision Database Server“ kaip paslaugą arba naudoti *installasservice* komandos eilutės parametrą paleisdami serverį, turėtumėte užtikrinti, kad paslauga naudojasi „NT Authority\Network Service abonentą“. „NT Authority\ Network Service“ abonementas egzistuoja tik Windows™ XP ir Windows Server™ 2003. Jeigu naudojate sistemą „Windows 2000 Server“, turėtumėte sukurti abonentą su mažai privilegijų naudotis paslauga, kitaip paslauga bus priskirta „Local System“ abonentui. Šis abonentas turi turėti bent jau tokias pat privilegijas kaip įprastas abonentas vartotojas arba būti domeno abonentas, t. y., ne domeno ar kokio nors kito vietinio kompiuterio administratorius.

  Prisiminkite, kad „NT Authority\Network Service“ abonentui arba abonentui vartotojui, kuris naudojasi serveriu, turėsite suteikti įrašymo ir nuskaitymo prieigą prie duomenų bazės failo(-ų), kad užtikrintumėte, jog vartotojai gali prisijungti prie duomenų bazės.

  Norėdami suteikti „NT Authority\Network Service“ abonentui nuskaitymo ir įrašymo prieigą prie duomenų bazės failo sistemoje „Windows XP“:

  1. Atidarę „Windows Explorer“, atsidarykite aplanką, kuriame yra duomenų bazės failas.
  2. Pažymėkite duomenų bazės failą, spustelėkite dešinįjį pelės klavišą ir pasirinkite Savybės.
  3. Lange ***Savybės*** spustelėkite skirtuką ***Sauga*** ir lauke **Grupės ir vartotojų vardai** spustelėkite Pridėti.
  4. Lange ***Pasirinkite vartotojus, kompiuterius arba grupes*** įveskite *Network Service* ir spustelėkite Gerai.
  5. NETWORK SERVICE buvo pridėtas prie lauko **Grupės ir vartotojų vardai** lange ***Savybės***.
  6. Pasirinkite NETWORK SERVICE ir lauke **Leidimai** suteikite leidimą *nuskaityti* ir *įrašyti*.
- „Navision Application Server“ paslauga pagal numatytuosius nustatymus veikia kaip „NT Authority\Network Service“ abonementas, dėl to vietoje suteikiama prieiga prie „Navision Data Base“ serverio. Tačiau turite užtikrinti, kad tinkle „Navision Application Server“ paslauga veikia kaip „Windows“ domeno abonementas, kurį atpažįsta „Navision Database Server“, jeigu norite, kad jis turėtų prieigą prie duomenų bazės serverio. Šis abonementas neturi priklausyti administratoriui ir turi nebūti nei domene, nei kokiame nors vietiniame kompiuteryje.
- Jeigu naudojate SQL serverio pasirinktį, „Navision“, Microsoft SQL Server™ veikia kaip paslauga. SQL serverio pasirinktis programoje „Navision“ reikalauja, kad SQL serveris galėtų tikrinti „Active Directory“ ir gauti „Windows“ vartotojų grupių sąrašus autentifikuoti. Turite užtikrinti, kad SQL serverio paslauga veikia kaip „NT Authority\Network Service“ abonementas.

  Norėdami užtikrinti, kad tarnyba veikia kaip „NT Authority\Network Service“:

  1. SQL serverio kompiuteryje raskite MSSQLSERVER tarnybą, spustelėkite dešinį pelės klavišą ir pasirinkite Savybės.
  2. ***Savybių*** lange spustelėkite skirtuką ***Prisijungti***.
  3. Skirtuko lape ***Prisijungti***, lauke Prisijungti kaip, spustelėkite Šis abonentas, įveskite *NT Authority\NetworkService* ir spustelėkite Gerai.

  Norėdami gauti daugiau informacijos apie SQL serverio saugą, aplankykite svetaines:

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

  ir

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

- Jeigu naudojate „Navision“ el. verslo produktą, tokį kaip „Commerce Gateway“, turėtumėte užtikrinti, kad „Commerce Gateway Request“ serveris įdiegtas tinkamai su numatytaisiais šių tarnybų abonementų nustatymais. Numatytasis abonemento nustatymas vadinamas *CGRSUser* ir leidžia „Commerce Gateway“ serveriui naudoti mažiausią reikiamą kitų tarnybų skaičių, tarp jų *MSSQLSERVER* tarnybą ir *BizTalk Service BizTalk Group*: Į *BizTalkServerApplication* neįtraukti jokie bendrieji abonemento nustatymai, nors jie įtraukti į *Local System* abonentą.
- Visada naudokite sudėtingus slaptažodžius. Norėdami gauti daugiau informacijos apie sudėtingus slaptažodžius, skaitykite skyrių Sudėtingi slaptažodžiai.
- Naudokite sistemos „Windows“ įėjimo laukus. Programa „Navision“ leidžia sukurti dviejų rūšių įėjimo vardus – duomenų bazės įėjimo vardus ir sistemos „Windows“ įėjimo vardus. Rekomenduojame naudoti sistemos „Windows“ įėjimo vardus, nes tuomet naudojamas sistemos „Windows“ autentifikavimas ir galite pritaikyti reikiamą slaptažodžių strategiją.
- Slaptažodžiai neturėtų būti naudojami iš naujo. Dažnai slaptažodžiai iš naujo naudojami sistemoje ir domenuose. Pavyzdžiui, administratorius, atsakingas už du domenus, galėtų sukurti domeno administratoriaus abonementus su tais pačiais slaptažodžiais ir net nustatyti tokius pačius vietinio administratoriaus slaptažodžius kaip domeno kompiuteriuose, kurie jungiasi prie to paties domeno. Šiuo atveju, įsilaužus į vieną kompiuterį, būtų galima įsilaužti į visą domeną.
- Įdiegę programą „Navision“ ir sukūrę duomenų bazes arba jas atnaujinę, turėtumėte sukurti sistemos „Windows“ įėjimo vardą ir priskirti jam SUPER vaidmenį programoje „Navision“. Šis SUPER vartotojas administruos duomenų bazę, saugą ir t. t. Šiam įėjimo vardui suteikite sudėtingą slaptažodį. Šis slaptažodis turėtų būti laikomas paslaptyje. Taip turėtų būti suteikiama tokia pati sauga kaip su SA slaptažodžiu SQL serveryje. Visą prieigą prie duomenų bazės tvarko SUPER vaidmuo ir jam reikia naudoti aukščiausią saugos lygmenį. SUPER vartotojo slaptažodį turėtų žinoti tik sistemos administratoriai.
- Visi kiti vartotojai, kurie turi prieigą prie „Navision“ duomenų bazės, turėtų naudotis mažesnėmis teisėmis. Tai reiškia, kad programoje „Navision“ jiems turi būti priskiriami vaidmenys, kurie suteikia jiems prieigą prie ypatybių ir funkcijų, kurių reikia atliekant užduotis įmonėje.
- Užtikrinkite, kad tik tie įmonės darbuotojai, kuriems tikrai reikia, galėtų importuoti FOB failus, keisti objektus ir kurti bei atkurti atsargines duomenų bazės kopijas.
- Reguliariai kurkite atsargines „Navision“ duomenų bazės kopijas ir nepamirškite jų išbandyti ir įsitikinti, kad jos gali būti sėkmingai atkurtos.
- Saugokite atsargines kopijas saugioje vietoje, kad jos būtų apsaugotos nuo ugnies, dūmų, dulkių, aukštos temperatūros, žaibų ir stichinių nelaimių (pvz., žemės drebėjimo).
- Nors programa „Navision“ gali veikti keliose sistemos „Windows“ versijose, rekomenduojame naudoti naujausią operacinę sistemą su pačiomis naujausiomis apsaugos funkcijomis. Dabar tokios sistemos yra „Windows XP“ su 2 pakeitimų paketu ir „Windows Server 2003“.
- Naudokite sistemos „Windows“ atnaujinimo paslaugą, teikiamą sistemose „Windows 2000“, „Windows XP“ ir „Windows Server 2003“, kad galėtumėte pritaikyti pačius naujausius saugos naujinimus. Naudodami sistemos „Windows“ automatinio atnaujinimo funkciją užtikrinsite, kad kliento kompiuteriuose įdiegti naujausi saugos pataisymai, pakeitimų paketai ir atnaujinimai.
- Ryšiui tarp „Navision“ klientų ir „Navision“ duomenų bazės serverio rekomenduojame naudoti TCPS saugos protokolą. TCPS yra saugi TCP/IP versija ir naudoja „Security Support Provider Interface“ (SSPI) su įjungtu šifravimu ir Kerberos autentifikavimu. TCPS yra numatytasis „Navision“ duomenų bazės serverio protokolas.

- Klientas turėtų turėti sistemos atkūrimo planą, kuris užtikrina greitą paslaugų atnaujinimą įvykus nelaimei. Sistemos atkūrimo plane turėtų būti numatyta:
  - Naujos ar laikinos įrangos gavimas.
  - Sistemos atkūrimas naujose sistemose.
  - Išbandymą, ar sistemos atkūrimo planas tikrai veikia.

Fizinė sauga

Fizinė sauga yra būtina ir jos negalima painioti su programinės įrangos sauga. Pavyzdžiui, jei pavagiamas kietasis diskas su juo bus pavogti ir jame esantys duomenys. Kurdami saugos strategiją su klientu aptarkite šias fizinės saugos temas:

- Diegdami daug programų tam skirtuose IT skyriuose, užtikrinkite, kad serverių patalpos ir patalpos, kuriose laikoma programinė įranga, būtų užrakintos.
- Šią kategoriją sudaro ši įranga:
  - „Microsoft SQL Server 2000“ serveris
  - Failų serveris, kuriame yra programos „Navision“ apdorojami failai.
- Užtikrinkite, kad pašaliniai asmenys negalėtų naudotis kompiuteriais.
- Įdiekite apsaugos signalizaciją, nesvarbu, kokios svarbos duomenys saugomi.
- Atsarginės svarbių duomenų kopijas saugokite kitoje patalpoje ugniai atspariuose seifuose.

Darbuotojai

Naudinga apriboti administravimo teises naudotis visais produktais ir funkcijomis. Numatyta, kad klientai turėtų suteikti savo darbuotojams teisę tik skaityti sistemos funkcijas, nebent jų darbui reikia daugiau teisių. Microsoft siūlo laikytis mažiausios privilegijos principo: vartotojams suteikite kuo mažiau teisių pasiekti duomenis ir naudotis funkcijomis.

Nepatenkinti ir buvę darbuotojai kelia grėsmę tinklo saugai. Aptardami saugą su klientais pasiūlykite darbuotojams taikyti tokią strategiją:

- Prieš įdarbinant patikrinti asmenį.
- Tikėtis keršto iš nepatenkintų ir buvusių darbuotojų.
- Įsitikinti, kad išeidamas darbuotojas panaikino visus susijusius „Windows“ abonementus ir slaptažodžius. Ataskaitos tikslais nepanaikinti vartotojų. Abonementus naudoti tik vieną kartą.
- Išmokyti vartotojus būti dėmesingus ir pranešti apie įtartiną veiklą.
- Nesuteikti teisių automatiškai. Jeigu vartotojams nėra būtina prieiga prie konkrečių kompiuterių, kompiuterių patalpų ar failų rinkinių, užtikrinti, kad jie tokios prieigos neturėtų.
- Išmokyti prižiūrėtojus nustatyti ir spręsti galimas darbuotojų problemas.
- Įsitikinti, kad darbuotojai supranta savo vaidmenį saugant tinklą.
- Kiekvienam darbuotojui įteikti įmonės strategijos kopiją.
- Neleisti vartotojams diegti programinės įrangos, kurios neleidžia diegti darbdavys.

Administratorius

Siūlome jūsų klientų sistemos administratoriams susipažinti su naujaisiais „Microsoft“ saugos patobulinimais. Įsilaužėliai naudodamiesi smulkiomis klaidelėmis gali suplanuoti stambų įsilaužimą į tinklą. Visų pirma

administratoriai turėtų užtikrinti, kad kiekvienas kompiuteris kaip galima geriau apsaugotas, o tada įdiegti saugos naujinius ir naudoti antivirusinę programinę įrangą. Šiame vadove teikiama daug saitų ir išteklių, kad galėtumėte rasti vertingos informacijos ir geriausių patarimų.

Sudėtingumas yra dar vienas dalykas, į kurį reikia atsižvelgti apsaugant tinklą. Kuo sudėtingesnis tinklas, tuo sunkiau jį apsaugoti arba pataisyti, jeigu įsilaužėliui pavyktų į jį patekti. Administratorius turėtų kruopščiai pildyti dokumentus apie tinklą ir stengtis tai atlikti kaip įmanoma paprasčiau.

Sauga tiesiogiai susijusi su rizikos valdymo. Vien technologija neapsaugosite. Saugą sudaro technologijos ir strategijos derinys. Kitais žodžiais tariant, niekada nebus tokio produkto, kurį išėmę iš pakuotės ir įdiegę iškart tobulai apsaugosite tinklą. Sauga yra technologijos ir strategijos derinys , tai yra tinklo saugos lygis priklauso nuo to, kaip naudojamos technologijos. „Microsoft“ siūlo į saugumą orientuotas technologijas ir funkcijas, bet tik administratorius, jūsų padedamas, gali nustatyti tinkamą strategiją kiekvienai organizacijai. Planuokite ir taikykite saugos metodus nuo pat pradžių. Pasistenkite gerai suprasti, ką nori apsaugoti jūsų klientas ir ką jis pasirengęs daryti, kad tai pasiektų.

Galiausiai, pasiruoškite netikėtumams, kol jie dar neįvyko. Kruopštų planavimą suderinkite su patikimomis technologijomis ir jūsų klientas bus puikiai apsaugotas.

Norėdami gauti bendros informacijos apie saugą, žr. „Dešimt nepakeičiamų saugos administravimo nurodymų” svetainėje:
http://www.microsoft.com/technet/archive/community/columns/security/essays/10salaws.mspx

ir straipsniuose apie saugos tvarkymą svetainėje:
http://www.microsoft.com/technet/community/columns/secmgmt/smarch.mspx

Serverio operacinės sistemos sauga

Nors dauguma smulkesnių klientų neturi serverio operacinės sistemos, svarbu, kad suprastumėte ir galėtumėte pritaikyti geriausią saugos lygį dirbdami su didesniais klientais didesniuose tinkluose. Nepamirškite, kad dauguma strategijų ir praktikų, aprašytų šiame dokumente, gali būti lengvai pritaikomos tiems klientams, kurie turi tik kliento operacines sistemas.

Šio skyriaus turinys gali būti pritaikomas „Microsoft Windows 2000 Server“ ir „Microsoft Windows Server 2003“ produktams, nors ši informacija paimta daugiausia iš „Windows Server 2003“ žinyno tinkle. „Windows Server 2003“ siūlo didelį saugos funkcijų pasirinkimą. „Windows Server 2003“ žinyne tinkle yra visa informacija apie saugos funkcijas ir veiksmus.

Norėdami gauti daugiau informacijos apie „Windows 2000 Server“, apsilankykite „Windows 2000 Server“ saugos centrą svetainėje:
http://www.microsoft.com/technet/security/prodtech/win2000/default.mspx

ir perskaitykite „Windows 2000“ saugos sugriežtinimo vadovą:
http://www.microsoft.com/technet/security/prodtech/win2000/win2khg/default.mspx

Norėdami daugiau informacijos apie „Windows Server 2003“, aplankykite *Windows Server 2003 Security Guide* svetainę:
http://www.microsoft.com/technet/security/prodtech/win2003/w2003hg/sgch00.mspx

Pradiniai Windows serverio saugos žingsniai yra autentifikavimas,prieigos kontrolė ir vienetinis registravimasis:

- Autentifikavimas yra procesas, kuriuo sistema patvirtina vartotojo ID atsižvelgdama į jų registravimosi įrašą. Vartotojo vardas ir slaptažodis palyginamas su leidimus turinčių asmenų sąrašu. Jeigu sistema randa atitikmenį, leidžiama vartotojo prieiga pagal šiam vartotojui nustatytas sąlygas.
- Prieigos kontrolė apriboja vartotojo prieigą prie informacijos ar kompiuterinių išteklių pagal vartotojo ID ir jo priklausymą įvairioms iš anksto nustatytoms grupėms. Prieigos kontrolę dažniausiai naudoja sistemos administratoriai, kad galėtų kontroliuoti vartotojų prieigą prie tinklo išteklių, tokių kaip serveriai, katalogai ir failai. Dažniausiai tai daroma suteikiant vartotojams ir grupėms leidimą prieiti prie konkrečių objektų.
- Vieno karto registravimasis leidžia prisijungti prie sistemos „Windows“ domeno, naudojant vieną slaptažodį, ir naudotis bet kuriuo sistemos „Windows“ domeno kompiuteriu. Vienas registravimasis leidžia administratoriams autentifikuoti slaptažodį visame sistemos „Windows“ tinkle, o galutiniai vartotojai turi lengvą prieigą.

Tolesniuose skyriuose pateikti išsamesni šių trijų funkcijų aprašymai.

Autentifikavimas

Autentifikavimas – svarbiausia sistemos saugos dalis. Ji naudojama bet kokiam vartotojui, bandančiam prisiregistruoti prie domeno ar prisijungti prie tinklo išteklių, patvirtinti. Daugelio autentifikavimo sistemų silpnoji grandis yra vartotojo slaptažodis.

Slaptažodžiai yra pirmoji gynybinė linija prieš neleistiną prieigą prie domeno ir vietinių kompiuterių. Siūlome naudotis šiais praktiškais patarimais apie slaptažodžius:

- Visada naudokite sudėtingus slaptažodžius.
- Jeigu slaptažodį reikia užsirašyti ant popieriaus lapo, saugokite jį saugioje vietoje ir sunaikinkite, kai tik nebereikės.
- Niekada niekam nesakykite slaptažodžių.
- Visiems vartotojų abonementams naudokite skirtingus slaptažodžius.
- Reguliariai keiskite slaptažodžius.
- Apgalvotai ir atsargiai saugokite slaptažodžius kompiuteriuose.

Sudėtingi slaptažodžiai

Dažnai neįvertiname, slaptažodžių svarbos organizacijos tinklo saugumui. Kaip jau minėta, slaptažodžiai yra pirmoji gynybinė linija prieš neleistiną prieigą prie jūsų tinklo. Turėtumėte įsitikinti, ar jūsų klientai nurodo savo darbuotojams naudoti sudėtingus slaptažodžius.

Slaptažodžių atspėjimo programos nuolat tobulėja, o kompiuteriai, naudojami slaptažodžiams atspėti, galingi kaip niekuomet. Turint pakankamai laiko, automatizuotas slaptažodžių atspėjimo įrankis gali atspėti bet kokį slaptažodį. Tačiau atspėti sudėtingus slaptažodžius yra daug sunkiau negu paprastus.

Daugiau informacijos, kaip kurti sudėtingus slaptažodžius, kuriuos galėtų prisiminti vartotojas, ieškokite

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

ir

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

Slaptažodžių strategijos kūrimas

Padėdami savo klientui nustatyti slaptažodžių strategiją, nepamirškite sukurti strategiją, reikalaujančią, kad visi klientų abonementai būtų apsaugoti sudėtingais slaptažodžiais. Daugumoje sistemų turėtų užtekti „Windows Server 2003“ saugos vadove pateikiamų patarimų:

- Nustatykite strategijos **Naudoti slaptažodžių istoriją** nustatymus, kurią naudojant prisimenami keli ankstesni slaptažodžiai. Pagal šią strategiją vartotojai, pasibaigus slaptažodžio galiojimo laikui, nebegali naudoti to paties slaptažodžio.

  Siūlomas nustatymas: 24

- Nustatykite strategijos **Ilgiausias laikas, kai prisimenamas slaptažodis**, nustatymą taip, kad slaptažodžiai galiotų tiek laiko, kiek reikia kliento darbui.

  Siūlomas nustatymas: tarp 42 (numatytasis) ir 90.

- Nustatykite strategijos **Trumpiausias laikas, kai prisimenamas slaptažodis**, nustatymą taip, kad slaptažodžio nebūtų galima pakartoti tol, kol praeis nustatytas dienų skaičius. Šis strategijos nustatymas veikia kartu su strategijos **Naudoti slaptažodžių istoriją** nustatymu. Jeigu nustatytas trumpiausias slaptažodžio prisiminimo laikas, vartotojai negali kartoti keičiamų slaptažodžių, kad apeitų strategijos **Naudoti slaptažodžių istoriją** nustatymą, ir tada vėl naudoti seno slaptažodžio. Vartotojai, prieš pakeisdami savo slaptažodžius, turi palaukti nustatytą dienų skaičių.

  Siūlomas nustatymas: 2.

- Nustatykite strategijos **Trumpiausias slaptažodis** nustatymą, pagal kurį slaptažodį turi sudaryti bent jau nurodytas simbolių skaičius. Ilgi slaptažodžiai, kuriuos sudaro septyni ir daugiau simbolių, dažniausiai yra sudėtingesni už trumpus. Pagal šį strategijos nustatymą, vartotojai negali naudoti „tuščio“ slaptažodžio – jie turi sukurti slaptažodį, kurį sudarytų bent jau nurodytas simbolių skaičius.

  Siūlomas nustatymas: 8.

- Suaktyvinkite strategijos **Slaptažodis turi atitikti sudėtingumo reikalavimus** nustatymą. Šis strategijos nustatymas tikrina visus naujus slaptažodžius ar jie atitinka pagrindinius sudėtingo slaptažodžio reikalavimus. Šis nustatymas užtikrina, kad slaptažodžiai yra sudaryti bent iš trijų kiekvienos iš keturių kategorijų simbolių (didžiųjų raidžių, mažųjų raidžių, skaičių ir nei skaitinių, nei raidinių simbolių) ir kad juose nėra vartotojo vardo dalies bei vartotojo vardo ar pavardės dalies.

  Pastaba
  Slaptažodžiai, atitinkantys šiuos reikalavimus, nebūtinai yra labai sudėtingi. Pavyzdžiui, slaptažodis „Slaptažodis1“ atitinka šiuos reikalavimus.

  Siūlomas nustatymas: Taip

- Norėdami gauti visą šių reikalavimų sąrašą, eikite į „Windows Server“ žinyną tinkle ir skaitykite „Slaptažodis turi atitikti sudėties reikalavimus“.

- Slaptažodžius saugokite naudodami grįžtamąjį kodavimą. Grįžtamasis kodavimas naudojamas sistemose, kuriose programos reikalauja prieigos prie nekoduotų tekstinių slaptažodžių. Dažniausiai tokio kodavimo nereikia.

  Siūlomas nustatymas: Ne.

Daugiau informacijos ieškokite „Windows Server 2003“ saugos vadove:

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

Abonemento blokavimo strategijos nustatymas

Apdairiai nustatykite abonementų blokavimo strategiją. Abonemento blokavimas niekada neturėtų būti nustatomas smulkiajame versle, nes gali būti blokuojami prieigą turintys vartotojai, o tai gali brangiai kainuoti jūsų klientui.

Jeigu klientas nusprendžia taikyti abonemento blokavimo strategiją, **Abonemento blokavimo strategijos ribai** nustatykite gana didelį bandymų prisijungti neužblokuojant vartotojo abonemento skaičių, nes vartotojas gali keli kartus neteisingai įvesti savo slaptažodį.

Daugiau informacijos apie abonemento blokavimo strategiją ieškokite „Windows Server“ žinyne tinkle, straipsnyje „Abonemento blokavimo strategijos apžvalga“.

Informacijos apie abonementų blokavimo strategijos taikymą ar keitimą ieškokite „Windows Server“ žinyne tinkle, straipsnyje „Kaip taikyti arba keisti abonementų blokavimo strategiją“.

Prieigos kontroliavimas

„Windows“ tinklas ir jo ištekliai (tarp jų ir programa „Navision“) gali būti apsaugoti, atsižvelgiant į tai, kokias teises tinkle turi vartotojai, vartotojų grupės ir kiti kompiuteriai. Kompiuterį ar daugelį kompiuterių galite apsaugoti suteikdami vartotojams arba vartotojų grupėms konkrečias vartotojo teises. Tokį objektą kaip failas ar aplankas galite apsaugoti vartotojams arba grupėms priskirdami teises atlikti konkrečius veiksmus su tuo objektu. Pagrindiniai sėkmingos prieigos kontrolės veiksniai:

- Teisės
- objektų nuosavybė
- teisių paveldėjimas
- vartotojo teisės
- objekto tikrinimas

Teisės

Teisės nurodo prieigos tipą, kuris suteiktas vartotojui arba vartotojų grupei, kad šie galėtų pasiekti objektą arba objekto turinį, pvz., failus, aplankus ir registro objektus. Teisės taikomos visiems apsaugotiems objektams, pvz., failams arba registro objektams. Teisės gali būti suteikiamos bet kuriam vartotojui, grupei ar kompiuteriui. Naudinga grupėms suteikti teises.

Objektų nuosavybė

Sukurtam objektui priskiriamas savininkas. Pagal numatytuosius nustatymus „Windows 2000 Server“, savininkas yra objekto kūrėjas. „Windows Server 2003“ tai pasikeitė tiems objektams, kuriuos sukuria administratorių grupės narys.

Administratorių grupės nariui sukūrus objektą sistemoje „Windows Server 2003“, savininku tampa administratorių grupė, o ne vienas jį sukūręs abonentas. Šis nustatymas gali būti pakeistas naudojant „Local Security Settings Microsoft Management Console“ (MMC) pridėtinį įrankį, nustatant nustatymą **Sistemos objektai: Objektų, sukurtų administratorių grupės narių, numatytasis savininkas.** Kad ir kokios teisės būtų nustatytos objektui, savininkas gali bet kada pakeisti šio objekto teises.

Daugiau informacijos ieškokite „Windows Server“ žinyne tinkle, straipsnyje „Nuosavybė“.

Teisių paveldėjimas

Paveldėjimas leidžia administratoriams nesunkiai suteikti ir tvarkyti teises. Naudojant šią funkciją, nustatytoje vietoje esantys objektai automatiškai paveldi visas paveldimas šios vietos teises. Pavyzdžiui, jeigu aplanke sukuriate failus, jie paveldi to aplanko teises. Paveldimos tik tos teisės, kurios pažymėtos kaip paveldimos.

Vartotojo teisės

Vartotojo teisės vartotojams ir vartotojų grupėms suteikia konkrečias privilegijas ir prisijungimo teises jūsų kompiuteriuose.

Daugiau informacijos apie vartotojo teises ieškokite „Windows Server“ žinyne tinkle, straipsnyje „Vartotojo teisės“.

Objekto tikrinimas

Galite tikrinti vartotojo prieigą prie objektų. Galite peržiūrėti su sauga susijusius įvykius saugos registre naudodamiesi įvykių peržiūra.

Daugiau informacijos ieškokite „Windows Server“ žinyne tinkle straipsnyje „Tikrinimas“.

Geriausi būdai kontroliuoti prieigą

- Teises suteikite grupėms, o ne atskiriems vartotojams. Tvarkyti atskirus vartotojų abonementus nėra saugu, todėl suteikti teises atskiram vartotojui galima tik išimtinai.
- Tam tikrais atvejais naudokite (Deny permissions) teisių Uždraudimą. Pavyzdžiui, galite naudoti teisių Uždraudimą, kad pašalintumėte iš grupės vieną narį, kuriam suteiktos (Allow permissions) teisės Leidžiama.
- Niekada neuždrauskite visos grupės prieigos prie objekto. Jeigu uždrausite visų prieigą prie objekto, į šią grupę bus įtraukti ir administratoriai. Geresnis sprendimas būtų pašalinti

grupę Visi, jeigu kitiems vartotojams, grupėms ar kompiuteriams suteikiate teisę naudoti objektą. Nepamirškite, kad jeigu nesuteikta jokių teisių, prieiga neleidžiama.

- Suteikite leidimus kuo toliau medžio struktūroje ir taikykite paveldimumą, kad visame medyje būtų taikomi saugos nustatymai. Galite lengvai ir efektyviai taikyti prieigos kontrolės nustatymus visoms išvestinėms pagrindinio medžio šakoms. Taip darydami pasieksite didžiausią efektyvumą naudodami mažiausiai pastangų. Teisių, kurias suteikiate, nustatymai turėtų būti vienodi daugumai vartotojų, grupių ir kompiuterių.
- Atviros teisės kartais gali būti svarbesnės už paveldėtas teises. Paveldėtos uždraudimo (Deny) teisės neuždraudžia prieigos prie objekto, jeigu objektas turi atvirą leidimo (Allow) teisę. Atviros teisės yra svarbesnės už paveldėtas teises, net už paveldėtas uždraudimo (Deny) teises.
- Norėdami suteikti teises Active Directory® objektams, įsitikinkite, kad žinote, kas geriausiai tinka konkretiems „Active Directory“ objektams.

Daugiau informacijos ieškokite „Windows Server 2003“ žinyne tinkle, straipsnyje „Geriausi būdai suteikti teises „Active Directory“ objektams“.

Išorinės saugos užkarda

Užkarda yra techninė arba programinė įranga, kuri neleidžia duomenų paketams patekti į konkretų tinklą, taip pat neleidžia jų pašalinti. Kad būtų kontroliuojamas duomenų srautas, užkardos prievadai būna atviri arba uždari informaciniams paketams. Užkarda atsižvelgia į kelias informacijos rūšis kiekviename duomenų pakete: protokolą, per kurį pristatomas duomenų paketas, iš kur paketas siunčiamas arba kas yra jo siuntėjas, duomenų, esančių pakete, tipą ir prievado numerį, į kurį siunčiamas paketas. Jeigu užkarda nustatyta taip, kad priimtų nurodytą protokolą per tam tikrą prievadą, paketui leidžiama patekti į vidų. „Microsoft Windows Small Business Server 2003 Premium Edition“ teikiamas su „Microsoft Internet Security and Acceleration (ISA) Server 2000“, kaip užkardą. „Small Business Server Standard Edition“ taip pat turi užkardą.

ISA Server 2004

„Internet Security and Acceleration (ISA) Server 2000“ vidiniame tinkle saugiai teikia užklausas ir atsakymus tarp interneto ir kliento kompiuterių.

„ISA Server“ veikia kaip saugūs Interneto šliuzai kliento kompiuteriams vietiniame tinkle. „ISA Server“ kompiuterį ryšio maršrute gali matyti kitos šalys. Interneto vartotojas neturėtų pastebėti, kad veikia užkardos serveris, nebent vartotojas mėgintų prieiti prie paslaugų arba prisijungti prie svetainės, prie kurios ISA kompiuteris nesuteikia prieigos. Interneto serveris, prie kurio bandoma prisijungti, užklausą iš ISA Server kompiuterio supranta užklausą iš kliento programos.

Pasirinkę interneto protokolo (IP) fragmentų filtravimą, įjungsite tarpinio voratinklio serverio (Web Proxy) ir užkardos paketų fragmentų filtravimo paslaugas. Filtruojant paketų fragmentus, atmetami visi fragmentuoti IP paketai. Gerai žinomą ataką sudaro fragmentuotų paketų siuntimas ir paskui jų surinkimas taip, kad jie galėtų padaryti žalos sistemai.

„ISA Server“ turi įsilaužimo nustatymo mechanizmą, kuris nustato laiką, kada bandoma įsilaužti į tinklą, ir atlieka konfigūruotų veiksmų (arba perspėjimų) seką, jeigu vykdoma ataka.

Jeigu „ISA Server“ kompiuteryje įdiegtos interneto informacijos paslaugos (IIS), turite sukonfigūruoti jį taip, kad nebūtų naudojami tie prievadai, kuriuos „ISA Server“ naudoja siunčiamoms voratinklio užklausoms (pagal numatytuosius nustatymus – 8080) ir gaunamoms interneto užklausoms (pagal numatytuosius nustatymus – 80). Pavyzdžiui, galite nustatyti IIS, kad šis stebėtų 81 prievadą ir tada konfigūruoti ISA Server kompiuterį taip, kad šis nukreiptų Interneto užklausas į vietinio kompiuterio 81 prievadą, kuriame veikia IIS.

Jeigu atsiranda nesklandumų tarp prievadų, kuriuos naudoja „ISA Server“ ir IIS, nustatymo programa nutraukia IIS skelbimo paslaugą. Galite nustatyti taip, kad IIS stebėtų kitą prievadą, ir iš naujo paleisti IIS skelbimo paslaugą.

„ISA Server“ strategijos

Galite nustatyti „ISA Server“ strategiją, kuri reguliuoja gavimo ir siuntimo prieigą. Svetainės ir turinio taisyklės nustato, prie kurių svetainių ir turinių turima prieiga. Protokolo taisyklės nurodo, ar yra prieiga prie konkretaus protokolo siuntimo ir gavimo ryšiui.

Galite kurti svetainių ir turinio taisykles, protokolo taisykles, interneto skelbimo taisykles ir IP paketų filtrus. Šios strategijos nustato, kaip „ISA Server“ klientai jungiasi prie interneto ir koks ryšys leidžiamas.

Apsauga nuo virusų

Kompiuterio virusas yra paleidžiamasis failas, sukurtas, kad daugintųsi, naikintų ar pažeistų duomenų failus bei programas ir nebūtų aptiktas radimo. Tiesą sakant, virusai dažnai perrašomi ir pataisomi taip, kad jų surasti negalima. Virusai dažnai siunčiami kaip el. laiškų priedai. Apsaugos nuo virusų programos turi būti nuolat atnaujinamos, kad galėtų rasti naujus ir pakeistus virusus. Virusai yra pagrindinė kompiuterinio vandalizmo priemonė.

Programinė apsaugos nuo virusų įranga sukurta specialiai tam, kad surastų virusines programas ir neleistų jų paleisti. Naujos virusinės programos kuriamos nuolat, todėl daug apsaugos nuo virusų produkcijos kūrėjų savo programinės įrangos klientams siūlo reguliarius naujinius. „Microsoft“ primygtinai rekomenduoja įdiegti programinę apsaugos nuo virusų įrangą kliento aplinkoje.

Programinė apsaugos nuo virusų įranga dažniausiai diegiama šiose trijose vietose: vartotojų kompiuteriuose, serveriuose ir tinkle, kuriame gaunami (o kartais siunčiami) organizacijos el. laiškai.

Virusų tipai

Yra trys pagrindiniai virusų, kurie užkrečia kompiuterių sistemas, tipai: įkrovos sektoriaus virusai, failus užkrečiantys virusai ir Trojos arklių programos.

Įkrovos sektoriaus virusai

Paleidus kompiuterį, prieš įkeldamas operacinę sistemą ar kitus paleisties failus, jis tikrina įkrovos sektorių kietajame diske. Įkrovos sektoriaus virusas sukurtas taip, kad pakeistų įkrovos sektoriaus informaciją kietajame diske savo kodu. Kai kompiuteris užkrečiamas įkrovos sektoriaus virusu, viruso kodas pats pirmas nuskaitomas į atmintį. Kai virusas patenka į atmintį, jis gali išplisti kituose naudojamuose užkrėsto kompiuterio diskuose.

Failus užkrečiantys virusai

Labiausiai paplitęs virusų tipas yra failus užkrečiantys virusai. Jis prisijungia prie paleidžiamos programos pridėdamas savo kodą prie paleidžiamojo failo. Viruso kodas dažniausiai pridedamas taip, kad virusas nebūtų aptiktas. Paleidus užkrėstą failą virusas gali prisijungti prie kitų paleidžiamųjų failų. Dažniausiai šio tipo virusu užkrėsti failai turi .com, .exe arba .sys failo vardo plėtinį.

Kai kurie failus užkrečiantys virusai sukurti užkrėsti konkrečias programas. Programų tipai, kurioms dažnai taikomi virusai yra perdengimo failai (.ovl) ir dinaminio saito bibliotekos (.dll) failai. Nors šie failai nepaleidžiami, paleidžiamieji failai juos iškviečia. Virusas plinta iškviečiant.

Žala duomenims padaroma paleidus virusą. Virusu užkrečiama paleidžiant užkrėstą failą arba kai atitinkami konkretūs aplinkos nustatymai (tokie kaip konkreti sistemos data).

Trojos arklių programos

Trojos arklys iš tikrųjų nėra virusas. Pagrindinis požymis, pagal kurį galima atskirti virusą ir Trojos arklio programą, yra tas, kad Trojos arklio programa nesidaugina, ji tik sunaikina informaciją kietajame diske. Trojos arklio programa apsimeta teisėta programa, pvz., žaidimu ar paslaugų programa. Jį paleidus duomenys gali būti sinaikinti arba perrašyti.

Geriausi apsaugos nuo virusų būdai

Makrokomandų virusų galima išvengti. Štai keli patarimai, kaip išvengti užkrėtimo, kuriais galite pasidalyti su klientais:

- Įdiekite programinę apsaugos nuo virusų įrangą, kuri tikrintų gaunamus internetu pranešimus, ar juose nėra virusų, prieš pranešimams pereinant per maršrutizatorių. Taip el. laiškai tikrinami, ar juose nėra nuo žinomų virusų.
- Žinokite šaltinį, iš kurio gavote dokumentus. Jeigu dokumentai nėra iš patikimo kliento, jų atidaryti nereikėtų.
- Pasikalbėkite su dokumentą sukūrusiu asmeniu. Jeigu vartotojai nėra įsitikinę, kad dokumentas saugus, jie turėtų susisiekti su dokumentą sukūrusiu asmeniu.

- Naudokite „Microsoft Office“ apsaugą nuo makrokomandų virusų. Programa „Office“ perspėja vartotoją, jeigu dokumente yra makrokomandų. Ši funkcija leidžia vartotojui atidarant dokumentą makrokomandas leisti arba blokuoti .
- Norėdami rasti ir pašalinti makrokomandų virusus, naudokite virusų skenavimo programinę įrangą. Virusų skenavimo programinė įranga gali rasti ir dažnai gali pašalinti virusus iš dokumentų. „Microsoft“ rekomenduoja naudoti programinę apsaugos nuo virusų įrangą, kurią sertifikavo Tarptautinė kompiuterių saugos asociacija (ICSA)

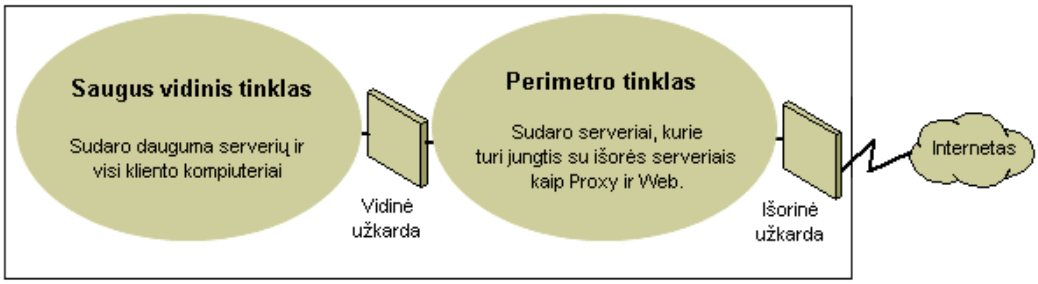
Daugiau informacijos apie virusus ir apie bendrą kompiuterių saugą ieškokite šiose „Microsoft“ saugos svetainėse:

- „Microsoft“ sauga: http://www.microsoft.com/security/default.asp
- Saugos dokumentacija „Microsoft TechNet“ http://www.microsoft.com/technet/security/Default.mspx

Tinklo saugos strategijos

Kuriant ir naudojant IP aplinką tarp tinklų reikia derinti privačių ir viešų tinklų poreikius, todėl užkarda tapo pagrindine tinklo saugos priemone. Užkarda nėra vienintelis komponentas. Nacionalinė kompiuterių saugos asociacija (NCSA) užkardą apibūdina kaip sistemą arba sistemų kombinaciją, kuri sudaro sieną tarp dviejų ar daugiau tinklų. Nors naudojami skirtingi terminai, ši siena dažnai vadinama perimetro tinklu. Perimetro tinklas apsaugo intranetą ar vietinį įmonės tinklą (LAN) nuo įsilaužimo kontroliuodamas prieigą iš interneto ar kitų stambių tinklų.

Toliau esančioje diagramoje parodytas užkardų supamas perimetro tinklas, esantis tarp asmeninio tinklo ir interneto, kad būtų apsaugotas privatusis tinklas:



Pagrindinis perimetro tinklas

Organizacijose skiriasi užkardų, skirtų apsaugai teikti, naudojimo būdai. IP paketų filtravimo teikiama apsauga yra silpna, ją sunku ir nepatogu valdyti, lengva įveikti. Programų šliuzai yra saugesni nei paketų filtrai, juos paprasčiau valdyti, kadangi jie susieti tik su keliomis konkrečiomis programomis, pvz., su tam tikra el. pašto sistema. Grandinės šliuzai naudingiausi, kai tinklo programos vartotojas yra svarbesnis nei duomenys, kuriuos perduoda ta programa. Proxy serveris yra visapusė apsaugos priemonė, kurioje įtrauktas programos šliuzas, saugi anoniminių vartotojų prieiga ir kitos paslaugos. Čia pateikiama informacijos apie šias skirtingas pasirinktis:

- **IP paketų filtravimas**
  IP paketų filtravimas buvo pirmasis užkardų technologijos realizavimas. Paketų antraštėse tikrinami šaltinio ir paskirties adresai, „Transmission Control Protocol“ (TCP) ir „User Datagram Protocol“ (UDP) prievadų numeriai ir kita informacija. Paketų filtravimas yra ribota technologija, kuri geriausiai veikia skaidrios apsaugos aplinkose, kur, pvz., viskas už tinklo ribų nepatikima, o viskas tinkle – patikima. Pastaraisiais metais įvairūs tiekėjai patobulino paketų filtravimo būdą, prie paketų filtravimo branduolio pridėdami intelektualias sprendimų priėmimo priemones ir sukurdami naują paketų filtravimo formą, vadinamą *pastovia protokolo inspekcija.* Galite konfigūruoti paketo filtravimą taip, kad būtų priimami konkretūs paketų tipai, o visi kiti atmetami, arba kad būtų atmetami konkretūs paketų tipai, o visi kiti priimami.
- **Programų šliuzai**
  Programų šliuzai naudojami, kai faktinis programos turinys yra didžiausios svarbos. Tai, kad jie skirti konkrečioms operacijoms, yra ir jų pranašumas, ir trūkumas, kadangi jie sunkiai pritaikomi prie technologijos pakitimų.
- **Grandinės šliuzai**
  Grandinės šliuzai yra tuneliai, sukurti užkardose, jungiančiose konkrečius procesus arba sistemas vienoje pusėje su procesais arba sistemomis kitoje pusėje. Grandinės šliuzus labiausiai tinka naudoti situacijose, kai asmuo, naudojantis programą, yra potencialiai pavojingesnis nei informacija, esanti programoje. Grandinės šliuzas skiriasi nuo paketų filtro galimybe jungtis prie išorinės programos schemos, kuri gali pridėti papildomos informacijos.
- **Proxy serveriai**
  Proxy serveriai yra visapusės apsaugos priemonės, į kurias įtrauktos užkardos ir programų šliuzo funkcijos, valdančios interneto srautą į ir iš LAN. Proxy serveriai taip pat pateikia dokumentų talpyklinius mainus ir prieigos valdymą. Proxy serveris gali pagerinti našumą atlikdamas dažnai reikalaujamų duomenų talpyklinius mainus ir tiesiogiai pateikdamas tuos duomenis, pvz., populiarų interneto puslapį. Proxy serveris taip pat gali filtruoti ir atmesti užklausas, kurias savininkas laiko netinkamomis, pvz., nelegalios prieigos prie savininko failų užklausą.

Įsitikinkite, kad klientas išlošia naudodamas tas užkardos saugos ypatybes, kurios gali jam padėti. Perimetro tinklas tinklo topologijoje turėtų būti tokioje vietoje, kur visi srautai iš už bendro tinklo ribų turi pereiti per perimetrą, kurį palaiko išorinė užkarda. Galite tiksliai nustatyti užkardos prieigos valdymą, kad būtų patenkinti kliento poreikiai, ir sukonfigūruoti užkardas, kad būtų pranešama apie visus nelegalios prieigos bandymus.

Norėdami sumažinti prievadų, reikalingų vidinei užkardai atidaryti, skaičių, galite naudoti programos sluoksnio užkardą, pvz. „ISA Server 2000“.

Daugiau informacijos apie TCP/IP rasite straipsnyje „TCP/IP tinklo kūrimas“, esančiame:
http://www.microsoft.com/resources/documentation/WindowsServ/2003/all/deployguide/en-us/dnsbb_tcp_overview.asp

Belaidžiai tinklai

Numatyta, kad belaidžiai tinklai paprastai yra sukonfigūruoti taip, kad leistų slapta sekti belaidžio ryšio signalus. Juos gali pažeisti piktybinis pašalinis asmuo, bandantis gauti prieigą dėl numatytųjų nustatymų tam tikroje kurioje belaidėje techninėje įrangoje, prieinamumo, kurį siūlo belaidis tinklas, ir esamų šifravimo būdų. Yra konfigūracijos pasirinkčių ir priemonių, galinčių apsaugoti nuo slapto sekimo, tačiau turėkite omeny, kad tai neapsaugos kompiuterių nuo

hakerių ir virusų, patenkančių per interneto ryšį. Dėl šios priežasties ypač svarbu įtraukti užkardą, kad kompiuteriai būtų apsaugoti nuo nepageidaujamų įsibrovėlių internete.

Daugiau informacijos apie belaidžio tinklo apsaugą rasite straipsnyje „Kaip padaryti belaidį 802.11b namų tinklą saugesnį“, esančiame: http://support.microsoft.com/default.aspx?scid=kb;en-us;309369

Tinklo apsaugos scenarijai

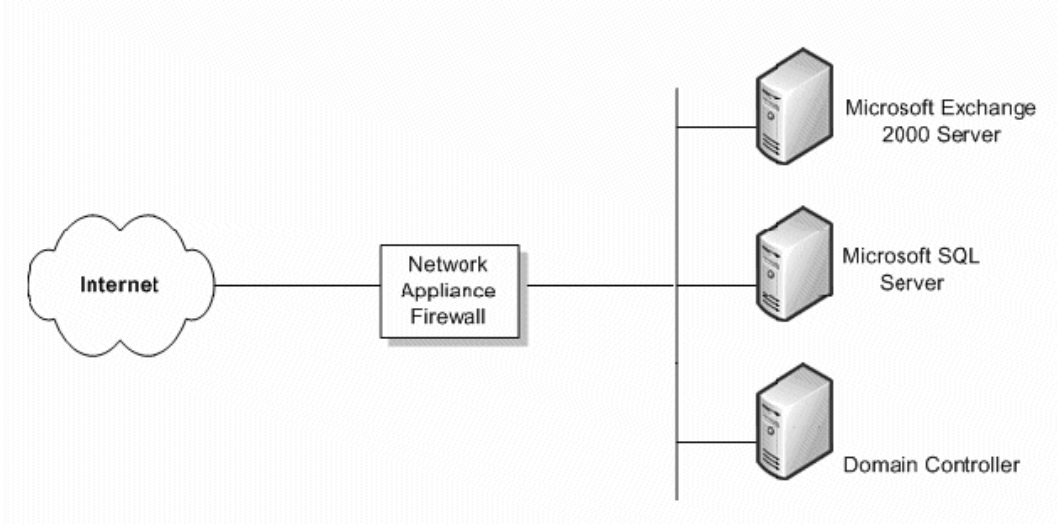
Tinklo apsaugos, kurios reikalauja kliento organizacija, lygis priklauso nuo keleto veiksnių. Dažniausiai tenka prieiti prie kompromiso dėl skiriamo biudžeto ir poreikio apsaugoti įmonės duomenis. Užsiimant smulkiu verslu galima turėti sudėtinę saugos struktūrą, kuri gali teikti aukščiausią įmanomą tinklo apsaugos lygį, tačiau smulkiojo verslo biudžeto gali neužtekti tokio lygio apsaugai įsigyti. Šiame skyriuje apžvelgsime keturis scenarijus ir kiekviename skyriuje pateiksime rekomendacijas dėl skirtingų apsaugos lygių.

Nėra užkardos

Jei jūsų klientas turi ryšį su internetu, tačiau neturi užkardos, reikia pritaikyti kai kuriuos tinklo apsaugos reikalavimus. Yra paprastų tinklo užkardos įtaisų, teikiančių pakankamą apsaugą, kad atbaidytų daugumą potencialių hakerių.

Viena paprasta užkarda

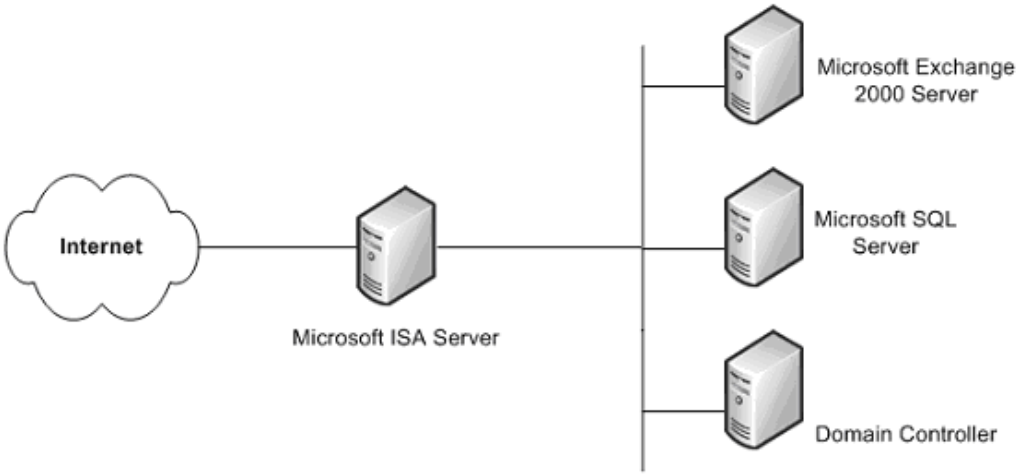
Minimalus rekomenduojamas saugos lygis yra viena užkarda tarp interneto ir jūsų kliento duomenų. Ši užkarda neteikia jokio padidintos apsaugos lygio ir neturėtų būti laikoma labai saugia. Tačiau tai geriau negu nieko.



Paprasta užkarda

Reikia tikėtis, kad kliento biudžetas leis pritaikyti saugesnį sprendimą įmonės duomenims apsaugoti. Vienas iš tokių sprendimų yra „ISA Server“. Už didesnę šio papildomo serverio kainą teikiama daug geresnė apsauga nei naudojant

paprastą vartotojo užkardą, kadangi paprastai ji teikia tik tinklo adreso vertimą (NAT) ir paketų filtravimą.



„ISA Server“ užkarda

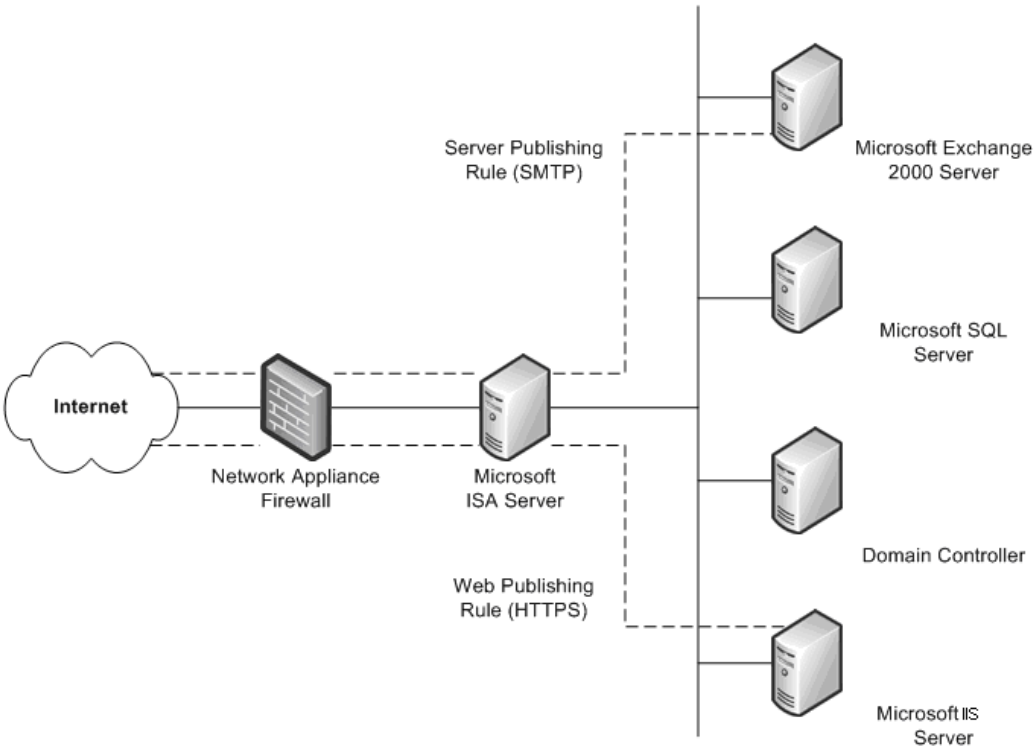
Šis vienas užkardos sprendimas daug saugesnis nei pradedančiųjų užkardos įtaisas, jis teikia apsaugos paslaugas, skirtas operacinei sistemai „Windows“.

Viena užkarda

Jei klientas turi užkardą, kuri skiria intranetą nuo interneto, galite nuspręsti prijungti papildomą užkardą, kuri leidžia keliais būdais konfigūruoti vidinius resursus į internetą.

Vienas iš tokių būdų yra skelbimas voratinklyje. Tada „ISA Server“ pateikiamas prieš organizacijos voratinklio serverį, kuris teikia prieigą interneto vartotojams. Gaunant voratinklio užklausas, „ISA Server“ gali pavaizduoti voratinklio serverį į išorinį pasaulį ir tokiu būdu patenkinti kliento poreikius gauti voratinklio turinį iš jo talpyklos. „ISA Server“ persiunčia užklausas į voratinklio serverį tik tada, kai užklausų negalima pateikti iš jo talpyklos.

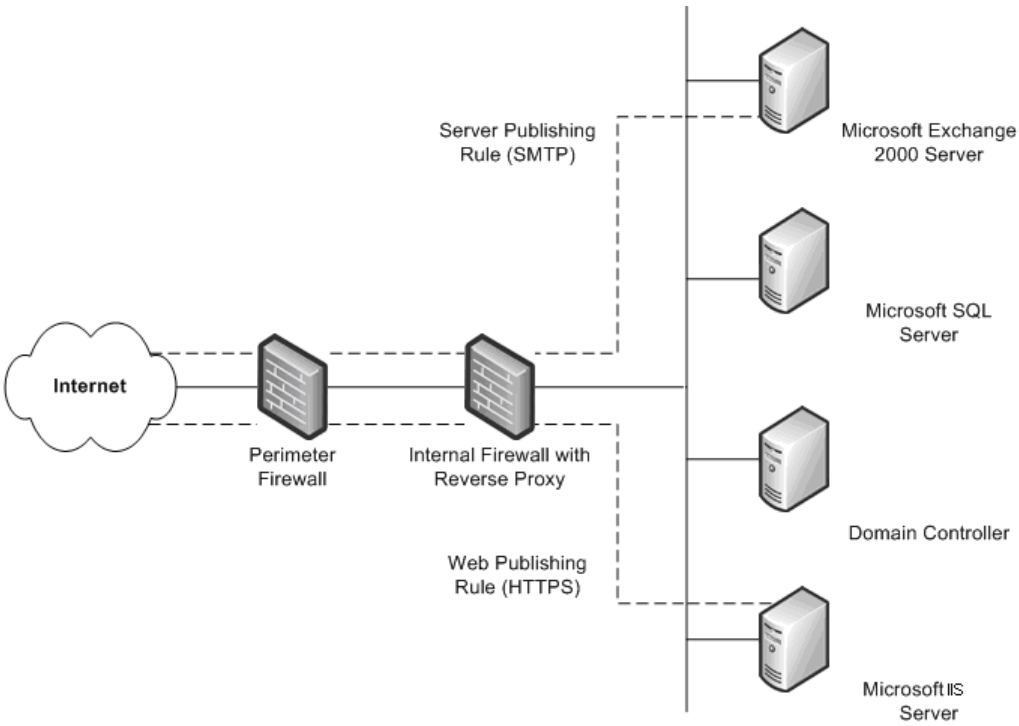
Kitas būdas yra skelbimas serveryje. „ISA Server“ leidžia skelbti vidinius serverius internete nepažeidžiant vidinio tinklo apsaugos. Galite konfigūruoti skelbimo voratinklyje ir serveryje taisykles, nustatančias, kurios užklausos turi būti siunčiamos į vietinio tinklo serverį, ir tokiu būdu teikiančias išsamesnį vidinių serverių apsaugos sluoksnį.



Užkarda su pridėtu „ISA Server

Dvi užkardos

Ketvirtasis scenarijus tinka, kai organizacija turi dvi užkardas su nustatytu perimetro tinklu (DMZ). Vienas arba daugiau šių serverių pateikia atvirkštines proxy serverio paslaugas, taigi interneto klientai neprieina prie intraneto serverių tiesiogiai. Vietoj to viena iš užkardų, geriausiu atveju vidinė, perima vidinių serverių tinklo užklausas, patikrina tuos paketus ir tada persiunčia juos pagrindinio interneto kompiuterio vartotojo vardu.



Dvi užkardos

Šis scenarijus panašus į anksčiau pateiktą scenarijų pridėjus antrą užkardą. Vienintelis skirtumas tas, kad vidinė užkarda, palaikanti atvirkštinį proxy serverį, nėra „ISA Server“. Pagal šį scenarijų turėtumėte dirbti glaudžiai su kiekvienos užkardos valdytojais, kad nustatytumėte serverio skelbimo taisykles, pridedamas prie saugos strategijos.

Apsaugos pataisų valdymas

Operacinės sistemos ir programos dažnai būna labai sudėtingos. Jos gali būti sudarytos iš milijonų kodų eilučių, jas dažnai rašo daug skirtingų programuotojų. Ypač svarbu, kad programinė įranga veiktų patikimai ir nekompromituotų IT aplinkos saugumo ar stabilumo. Norint išvengti nesklandumų, programos atidžiai tikrinamos prieš išleidžiant. Tačiau pažeidėjai nuolat stengiasi aptikti silpnas programinės įrangos vietas, todėl numatyti visas būsimas atakas neįmanoma.

Daugelyje organizacijų valdant pataisymus formuojama dalis visų pakeitimų ir konfigūracijos valdymo strategijos. Tačiau, neatsižvelgiant į organizacijos pobūdį ir dydį, gyvybiškai svarbu turėti gerą pataisų valdymo strategiją, net jei organizacijos dar neturi efektyvių pakeitimų ir konfigūracijos valdymo. Dauguma sėkmingų atakų prieš kompiuterių sistemas įvyksta tose sistemose, kuriose neįdiegti apsaugos pataisymai.

Apsaugos pataisymai pateikia konkretų iššūkį daugeliui organizacijų. Aptikus programinės įrangos silpnąją vietą, pažeidėjai sparčiai išplatina informaciją apie ją visoje hakerių bendruomenėje. Kai „Microsoft“ programinėje įrangoje aptinkama silpna vieta, siekiama išleisti apsaugos pataisymą kiek įmanoma greičiau. Kol pataisa neišleidžiama, apsaugos, nuo kurios yra priklausomas klientas ir kuria jis pasitiki, lygis gali smarkiai sumažėti.

Dirbdami „Navision“ aplinkoje turite būti tikri, kad jūsų klientai turi naujausius apsaugos pataisymus, įdiegtus visoje jų sistemoje. Įsitikinkite, kad klientas naudoja vieną iš technologijų, kurias pateikia „Microsoft“. Jos yra tokios:

- **„Microsoft Security Notification Service“**
  „Security Notification Service“ yra el. pašto adresų sąrašas, pateikiantis pranešimus, kai tik atsiranda atnaujinimas. Šie pranešimai yra naudinga veiksnios apsaugos strategijos dalis. Juos taip pat galima rasti „TechNet Product Security Notification“ tinklalapyje: http://www.microsoft.com/technet/security/bulletin/notify.mspx
- **„Microsoft Automatic Updates“**
  „Windows“ gali automatiškai taikyti apsaugos atnaujinimus jūsų įrenginiams.
- **„Microsoft Security Bulletin Search Tool“**
  Apsaugos skelbimų paieškos priemonę rasite „Security Bulletin Service“ tinklalapyje: http://www.microsoft.com/technet/security/current.aspx. Klientas gali nustatyti, kurie atnaujinimai reikalingi, pagal operacinę sistemą, programas ir veikiančius paslaugų paketus.
- **„Microsoft Baseline Security Analyzer“ (MBSA)**
  Šią grafinę priemonę rasite „Microsoft Baseline Security Analyzer“ tinklalapyje: http://www.microsoft.com/technet/security/tools/mbsahome.mspx. Ši priemonė veikia palygindama esamą kompiuterio būseną su atnaujinimų, kuriuos tvarko „Microsoft“, sąrašu. MBSA taip pat atlieka kai kuriuos pagrindinius apsaugos patikrinimus, pvz., slaptažodžio patvarumo ir galiojimo datos nustatymų, svečių abonementų strategijų ir keleto kitų sričių. MBSA taip pat ieško pažeidžiamų vietų „Microsoft Internet Information Services“ (IIS), „SQL Server™ 2000“, „Exchange 5.5“, „Exchange 2000“ ir „Exchange Server 2003“.
- **„Microsoft Software Update Services“ (SUS)**
  Ši priemonė, anksčiau vadinta „Windows“ atnaujinimų bendru leidimu, leidžia įmonėms taikyti vietiniams kompiuteriams visus svarbius atnaujinimus ir apsaugos paketus (SRPs), kuriuos galima rasti viešame „Windows“ atnaujinimų tinklalapyje. Ši priemonė veikia su nauju automatinio atnaujinimo (AU) klientų leidimu, kad suformuotų galingos automatinio atsisiuntimo ir diegimo strategijos pagrindą. Naujame AU klientų rinkinyje įtrauktas „Windows 2000“ ir „Windows Server 2003“ operacinių sistemų klientas, jame yra galimybė automatiškai diegti atsisiųstus atnaujinimus. Daugiau informacijos apie „Microsoft SUS“ ieškokite:
  http://www.microsoft.com/windows2000/windowsupdate/sus/default.asp
- **Microsoft sistemų valdymo serverio (SMS) programinės įrangos atnaujinimo paslaugų priemonių paketas**
  SMS programinės įrangos atnaujinimo paslaugų priemonių pakete yra keletas priemonių, skirtų palengvinti programinės įrangos atnaujinimų išleidimą į apyvartą visoje įmonėje. Šiose priemonėse įtraukta apsaugos atnaujinimo atsargų priemonė, „Microsoft Office“ atsargų priemonė, skirta atnaujinimams, programinės įrangos atnaujinimų paskirstymo vedlys ir SMS voratinklio ataskaitų kūrimo priemonė su voratinklio ataskaitų priedu, skirtu programinės įrangos atnaujinimams. Daugiau informacijos apie kiekvieną priemonę rasite:
  http://www.microsoft.com/smserver/downloads/20/featurepacks/suspack/

Pasišnekėkite su savo klientais apie kiekvieną iš šių priemonių ir paskatinkite jas naudoti. Labai svarbu, kad į apsaugos problemas būtų atsižvelgiama kiek įmanomo greičiau, tuo pat metu palaikant aplinkos stabilumą.

„SQL Server 2000“ apsaugos nustatymai

Kadangi programa Navision taip pat veikia SQL Server 2000, svarbu, kad imtumėtės priemonių kliento SQL Server 2000 diegimo saugumui padidinti. Šie žingsniai padės pagerinti SQL Server apsaugą:

- Įsitikinkite, kad įdiegti naujausi operacinės sistemos ir „SQL Server 2000“ paslaugų paketai ir atnaujinimai. Naujausios informacijos ieškokite „Microsoft Security“ tinklalapyje: http://www.microsoft.com/security/default.asp.
- Dirbdami su failų sistemos lygio apsauga įsitikinkite, kad visi „SQL Server 2000“ duomenys ir sistemos failai įdiegti NTFS skaidiniuose. Failai turėtų būti prieinami tik administratoriams arba sistemos lygio vartotojams su NTFS leidimais. Tai neleis vartotojams prieiti prie tų failų, kai neveikia paslauga MSSQLSERVER.
- Naudokite mažai teisių turinčio domeno abonementą, pvz., NT įgaliojimo\tinklo paslaugos arba vietinės sistemos (rekomenduojama) abonementą, skirtą „SQL Server 2000“ paslaugai (MSSQLSERVER). Šio abonemento teisės domene turėtų būti minimalios, jis turėtų padėti sulaikyti (bet nesustabdyti) atakas prieš serverį kompromitavimo atveju. Kitaip sakant, šis abonementas turėtų turėti tik vietinio vartotojo lygio leidimus domene. Jei „SQL Server 2000“ naudoja domeno administratoriaus abonementą, serverio kompromitavimas sukels viso domeno kompromitavimą. Norėdami pakeisti šį nustatymą, naudokite „SQL Server“ įmonės tvarkytuvą pakeitimui atlikti. Prieigos valdymo sąrašai (ACLs), esantys failuose, registras ir vartotojo teisės bus automatiškai pakeisti.
- Dauguma „SQL Server 2000“ leidimų įdiegti dviejose numatytosiose duomenų bazėse – **Northwind** ir **pubs**. Abi duomenų bazės yra pavyzdinės duomenų bazės, naudojamos bandymams, mokymams ir bendriesiems pavyzdžiams. Jos neturėtų būti pateiktos produkcijos sistemoje. Žinodami, kad yra šios duomenų bazės, pažeidėjai gali bandyti atlikti bandymus, kuriuose įtraukti numatytieji nustatymai ir numatytoji konfigūracija. Jei produkcijos „SQL Server 2000“ kompiuteryje yra duomenų bazės **Northwind** ir **pubs**, jas reikėtų pašalinti.
- „SQL Server 2000“ sistemos auditas išjungtas pagal numatytuosius nustatymus, todėl nėra jokio sąlygų audito. Tai trukdo aptikti įsibrovimą ir padeda pažeidėjams paslėpti savo pėdsakus. Mažų mažiausiai turėtumėte įjungti nepavykusių prisijungimų auditą.

Didžiąją dalį naujausios „SQL Server 2000“ apsaugos informacijos rasite: http://www.microsoft.com/sql/techinfo/administration/2000/security/default.asp

Apie „Microsoft Business Solutions“

„Microsoft Business Solutions“, „Microsoft“ padalinys, siūlo platų spektrą integruotų, tiesioginių verslo programų ir paslaugų, skirtų padėti smulkiems, vidutiniams ir įmonių verslams glaudžiau ir efektyviau bendradarbiauti su klientais, darbuotojais, partneriais ir tiekėjais. „Microsoft Business Solutions“ programos optimizuoja strateginius verslo procesus finansų valdymo, analizės, personalo valdymo, projektų valdymo, ryšių su vartotojais valdymo, duomenų rinkimo valdymo, tiekimo grandinės valdymo, el. komercijos, gamybos ir mažmeninių pardavimų valdymo srityje. Programos sukurtos pateikti supratimą ir padėti klientams pasiekti verslo sėkmės aukštumas. Daugiau informacijos apie „Microsoft Business Solutions“ rasite:
http://www.microsoft.com/BusinessSolutions/