Microsoft Business Solutions

Navision Security Hardening Guide

Publisert: Oktober 2004

Microsoft

Innholdsfortegnelse

Innledning 1

Gode fremgangsmåter for Navision-sikkerhet 2

Fysisk sikkerhet 4

De ansatte 4

Administratoren 5

Sikre serveroperativsystemet 5
- Godkjenning 6
- Sterke passord 7
- Tilgangskontroll 9
- Ekstern sikkerhetsbrannmur 10

ISA Server 2004 11
- Regler for ISA Server 11

Beskyttelse mot virus 12
- Virustyper 12
- Gode fremgangsmåter for beskyttelse mot virus 13

Strategier for nettverkssikkerhet 13
- Trådløse nettverk 15
- Scenarier for nettverkssikkerhet 15

Administrasjon av sikkerhetsoppdateringer 18

Sikkerhetsinnstillinger for SQL Server 2000 20

Microsoft Business Solutions 21

Innledning

Microsoft® Windows® gir avansert standardbasert nettverkssikkerhet. I videste forstand omfatter sikkerhet planlegging og vurdering av kompromisser. En datamaskin kan for eksempel låses inn i et hvelv og bare gjøres tilgjengelig for én systemansvarlig. Denne datamaskinen er nok sikker, men den er ikke særlig nyttig fordi den ikke er koblet til andre datamaskiner. Du må vurdere hvordan du kan gjøre nettverket så sikkert som mulig uten at det går på bekostning av brukervennligheten.

De fleste organisasjoner tar høyde for eksterne angrep og setter opp brannmurer, men mange selskaper vurderer ikke hvordan de skal redusere risikoen for sikkerhetsbrudd når ondsinnede brukere kommer seg innenfor brannmuren. Sikkerhetstiltak som innføres i kundens miljø, vil fungere godt hvis brukerne ikke må gjennom for mange prosedyrer for å utføre arbeidet på en sikker måte. Det bør være så enkelt som mulig for brukerne å implementere sikkerhetsregler, for ellers er det vanlig at de prøver å finne andre, mindre sikre måter å gjøre arbeidsoppgavene på.

Ettersom størrelsen på Navision-installasjoner kan variere en stor del, er det viktig å vurdere behovene til hver kunde nøye og veie sikkerhetens effektivitet opp mot kostnadene som vil påløpe. Som kundens betrodde rådgiver må du bruke din gode dømmekraft og anbefale regler som dekker kundens sikkerhetsbehov uten at de blir en byrde som til syvende og sist fører til at kunden slutter å følge reglene.

Gode fremgangsmåter for Navision-sikkerhet

De generelle reglene nedenfor kan bidra til å øke sikkerheten for Navision-miljøet.

- Hvis du vil kjøre Navision Database Server som en tjeneste eller bruke kommandolinjeparameteren *installasservice* når du starter serveren, må du sørge for at tjenesten kjører som kontoen NT-myndighet\nettverkstjeneste. Kontoen NT-myndighet\nettverkstjeneste finnes bare på Windows™ XP og Windows Server™ 2003. Hvis du kjører Windows 2000 Server, må du opprette en konto med færrest mulig rettigheter for tjenesten, for ellers tilordnes tjenesten en lokal systemkonto. Denne kontoen bør maksimalt ha de samme rettighetene som kontoen for vanlige brukere, eller den bør være en domenekonto som ikke er en administrator i domenet eller på en lokal datamaskin.

  Du må huske å gi lese- og skrivetilgang til databasefilen(e) for kontoen NT-myndighet\nettverkstjeneste eller brukerkontoen som serveren kjører under, for å sikre at brukerne kan koble til databasen.

  Slik gir du kontoen NT-myndighet\nettverkstjeneste lese- og skrivetilgang til en databasefil på Windows XP:

  1. I Windows Utforsker går du til mappen som databasefilen ligger i.
  2. Merk databasefilen, høyreklikk den, og klikk Egenskaper.
  3. I ***Egenskaper***-vinduet klikker du kategorien ***Sikkerhet***, og deretter klikker du Legg til i feltet **Gruppe- eller brukernavn**.
  4. Skriv inn *Nettverkstjeneste* i vinduet ***Velg brukere, datamaskiner eller grupper***, og klikk OK.
  5. NETTVERKSTJENESTE er lagt til i feltet **Gruppe- eller brukernavn** i ***Egenskaper***-vinduet.
  6. Velg NETTVERKSTJENESTE, og gi det *Lese*- og *Skrive*-tillatelse i **Tillatelser**-feltet.
- Tjenesten Navision Application Server kjører som standard som kontoen NT-myndighet\nettverkstjeneste, og dermed får den tilgang til Navision Database Server lokalt. I et nettverk må du imidlertid kontrollere at tjenesten Navision Application Server kjører som en Windows-domenekonto som gjenkjennes av Navision Database Server, hvis du vil at den skal ha tilgang til databaseserveren. Denne kontoen bør ikke være en administrator i domenet eller på en lokal datamaskin.
- Hvis du kjører SQL Server-alternativet for Navision, kjører Microsoft SQL Server™ som en tjeneste. SQL Server-alternativet for Navision krever at SQL Server kan slå opp i Active Directory for å få lister over Windows-brukergrupper til godkjenningsformål. Du må derfor sikre at SQL Server-tjenesten kjører som kontoen NT-myndighet\nettverkstjeneste.

  Slik sikrer du at tjenesten kjører som kontoen NT-myndighet\nettverkstjeneste:

  1. Finn MSSQLSERVER-tjenesten på datamaskinen som kjører SQL Server, høyreklikk den, og klikk Egenskaper.
  2. Klikk kategorien ***Logg på*** i ***Egenskaper***-vinduet.
  3. I kategorien ***Logg på*** klikker du Denne kontoen under Logg på som, angir *NT-myndighet\nettverkstjeneste* og klikker OK.

  Hvis du vil ha mer informasjon om sikkerhet i forbindelse med SQL Server, kan du besøke følgende webområder:

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

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

- Hvis du kjører et Navision E-business-produkt som Commerce Gateway, må du sikre at Commerce Gateway Request Server er installert på riktig måte med standardinnstillingen for konto for tjenestene. Standardinnstillingen for konto heter *CGRSUser* og gir Commerce Gateway Server tilgang til det minste settet med andre tjenester som den krever, inkludert *MSSQLSERVER*-tjenesten og *BizTalk Service BizTalk Group: BizTalkServerApplication*, og inkluderer ingen globale kontoinnstillinger slik kontoen *Lokalt system* gjør.
- Bruk alltid sterke passord. Hvis du vil ha mer informasjon om sterke passord, se delen Bruk forskjellige passord for alle brukerkontoer.
- Bruk Windows-pålogging. I Navision kan du opprette to typer påloggінger – Databasepålogging og Windows-pålogging. Vi anbefaler at du bruker Windows-pålogging, ettersom denne påloggingstypen bruker Windows-godkjenning og lar deg gjennomføre skikkelige passordregler.
- Passord bør ikke brukes om igjen. Det er ofte vanlig å bruke passord om igjen på tvers av systemer og domener. En administrator som har ansvaret for to domener, kan for eksempel opprette domeneadministratorkontoer for hvert domene, som bruker det samme passordet, og til og med angi lokale administratorpassord for domenedatamaskiner som er de samme på tvers av domenet. Hvis én konto eller datamaskin blir utsatt for angrep, kan det i slike tilfeller føre til at hele domenet blir utsatt.
- Når Navision er installert og databasene er opprettet, eller oppdatert, må du opprette en Windows-pålogging og tilordne den SUPER-rollen i Navision. Denne superbrukeren håndterer databaseadministrasjon, sikkerhet og så videre. Gi denne påloggingen et sterkt passord. Dette passordet må forbli konfidensielt. Det bør få samme beskyttelse som du gir passordet for systemansvarlig i SQL Server. All databasetilgang håndteres av SUPER-rollen og krever det høyeste beskyttelsesnivået. Bare de systemansvarlige bør kjenne til passordet for superbrukeren.
- Alle de andre brukerne som har tilgang til Navision-databasen, bør kjøre med færrest mulig rettigheter. Det betyr at de bør tilordnes roller i Navision som bare gir dem tilgang til funksjonene de trenger for å utføre oppgavene sine i selskapet.
- Du må sikre at bare de brukerne som har roller i selskapet som krever det, skal kunne importere FOB-filer, utforme objekter på nytt samt opprette og gjenopprette sikkerhetskopier av databasen.
- Ta regelmessige sikkerhetskopier av Navision-databasen, og husk å teste sikkerhetskopiene for å sikre at de kan gjenopprettes.
- Lagre sikkerhetskopiene på et sikkert sted for å begrense skadene ved brann, røykutvikling, støv, høye temperaturer, lynnedslag og naturkatastrofer (for eksempel jordskjelv).
- Selv om Navision kan kjøres på flere versjoner av Windows, anbefaler vi at du bruker de nyeste operativsystemene med de mest oppdaterte sikkerhetsfunksjonene. Det er for øyeblikket Windows XP, Service Pack 2 og Windows Server 2003.
- Bruk Windows Update-tjenesten som følger med Windows 2000, Windows XP og Windows Server 2003, til å bruke de nyeste sikkerhetsoppdateringene. Bruk funksjonen Automatiske oppdateringer i Windows til å holde alle datamaskinene til kunden oppdatert med de nyeste sikkerhetsoppdateringene, serviceoppgraderingene og oppdateringene.
- Vi anbefaler at du bruker sikkerhetsprotokollen TCPS til å kommunisere mellom Navision-klientene og Navision Database Server. TCPS er en sikker versjon av TCP/IP og bruker Security Support Provider Interface (SSPI) med kryptering aktivert og Kerberos-godkjenning. TCPS er standardprotokollen for Navision Database Server.

- Kunden bør ha en gjenopprettingsplan for katastrofer som sikrer rask gjenopptakelse av tjenester etter en katastrofe. En gjenopprettingsplan bør inneholde følgende temaer:
  - Anskaffelse av nytt/midlertidig utstyr.
  - Gjenoppretting av sikkerhetskopier på nye systemer.
  - Testing av at gjenopprettingsplanen faktisk fungerer.

Fysisk sikkerhet

Fysisk sikkerhet er svært viktig ettersom det ikke er mulig å supplere den med programvaresikkerhet. Hvis for eksempel en harddisk blir stjålet, blir dataene på harddisken også stjålet. Diskuter følgende temaer for fysisk sikkerhet når du utvikler regler med kunden:

- I store selskaper med egne IT-avdelinger er det viktig å sikre at serverrom og steder der programvare oppbevares, er låst.
- Følgende maskiner inngår i denne kategorien:
  - Microsoft SQL Server 2000-serveren
  - Filserveren som de kjørbare Navision-filene ligger på.
- Ikke la uautoriserte brukere få tilgang til datamaskinene.
- Sikre at innbruddsalarmer er installert, uavhengig av hvor sensitive dataene er.
- Sikre at sikkerhetskopier av viktige data lagres borte fra arbeidsstedet, og at de lagres i brannsikre beholdere.

De ansatte

Det er lurt å begrense administrative rettigheter på tvers av alle produkter og funksjoner. Som standard bør kunder bare gi de ansatte lesetilgang til systemfunksjoner, med mindre de trenger større tilgang for å utføre arbeidet sitt. Microsoft anbefaler å følge prinsippet med færrest mulig rettigheter: gi brukerne bare de rettighetene som er nødvendige for å få tilgang til data og funksjoner.
Misfornøyde og tidligere ansatte er en trussel mot nettverkssikkerhet. Når sikkerhet diskuteres med kundene, er det lurt å anbefale følgende regler med hensyn til ansatte:

- Undersøk bakgrunnen til arbeidssøkere før de ansettes.
- Forvent at misfornøyde ansatte og tidligere ansatte vil "hevne seg".
- Kontroller at alle tilknyttede Windows-kontoer og -passord deaktiveres når en ansatt slutter. Av rapporteringshensyn må brukere ikke slettes. Ikke bruk kontoene på nytt.
- Lær opp brukerne til å være på vakt og rapportere mistenkelig aktivitet.
- Ikke gi rettigheter automatisk. Hvis brukerne ikke trenger å ha tilgang til bestemte datamaskiner, datamaskinrom eller filsett, må du sikre at de ikke har tilgang.
- Lær opp overordnede til å oppdage og reagere på potensielle problemer med ansatte.
- Kontroller at ansatte forstår rollene sine i å opprettholde nettverkssikkerhet.
- Gi en kopi av selskapets regler til alle ansatte.
- Ikke la brukerne installere programvare som ikke er godkjent av arbeidsgiverne.

Administratoren

Vi anbefaler at kundenes systemansvarlige holder seg oppdatert med de siste feilrettingsfilene for sikkerhet fra Microsoft. Ondsinnede brukere er dyktige til å kombinere små feil for å utføre omfattende inntrenging på et nettverk. Administratorer må først sikre at alle datamaskinene er så sikre som mulig, og deretter må de legge til sikkerhetsoppdateringer og bruke antivirusprogramvare. Mange koblinger og ressurser er angitt i denne veiledningen. Disse skal hjelpe deg med å finne verdifull informasjon og gode fremgangsmåter.

Kompleksitet er et annet kompromiss i forbindelse med sikring av nettverket. Jo mer sammensatt nettverket er, jo vanskeligere er det å sikre eller reparere det når en inntrenger har fått tilgang. Administratoren bør dokumentere nettverkstopografien grundig og ha som mål at den skal være så enkel som mulig.

Sikkerhet har hovedsakelig med risikostyring å gjøre. Ettersom teknologi ikke er et universalmiddel, må teknologi og regler kombineres for å oppnå sikkerhet. Med andre ord vil det aldri finnes et produkt du bare kan pakke ut og installere på nettverket, som øyeblikkelig oppnår perfekt sikkerhet. Sikkerhet er et resultat av både teknologi og regler. Det vil si at det er måten teknologien brukes på som bestemmer sikkerhetsnivået for et nettverk. Microsoft leverer teknologi og funksjoner som setter sikkerhet i høysetet, men bare administratoren, med veiledning fra deg, kan fastsette riktige regler for hver organisasjon. Husk å planlegge sikkerhet tidlig i implementerings- og distribusjonsprosessen. Skaff deg forståelse av hva kunden ønsker å beskytte og hva vedkommende er villig til å gjøre for å beskytte dette.

Utvikle til slutt planer for håndtering av krisesituasjoner før de oppstår. Kombiner grundig planlegging med kraftig teknologi, og kunden vil ha solid sikkerhet.

Hvis du vil ha mer informasjon om sikkerhet generelt, se The Ten Immutable Laws of Security Administration på følgende webområde:
http://www.microsoft.com/technet/archive/community/columns/security/essays/10salaws.mspx.

og artiklene om sikkerhetsadministrasjon på følgende webområde:
http://www.microsoft.com/technet/community/columns/secmgmt/smarch.mspx

Sikre serveroperativsystemet

Selv om du opplever at mange mindre kunder ikke har et serveroperativsystem, er det viktig at du forstår og kan kommunisere gode fremgangsmåter for sikkerhet til større kunder som har mer sammensatte nettverksmiljøer. Du må også være klar over at mange av reglene og fremgangsmåtene som er beskrevet i dette dokumentet, enkelt kan brukes på kunder som bare har klientoperativsystemer.

Konseptene i denne delen gjelder både for Microsoft Windows 2000 Server- og Microsoft Windows Server 2003-produkter, selv om denne informasjonen hovedsakelig er hentet fra den elektroniske hjelpen for Windows Server 2003. Windows Server 2003 inneholder et robust sett med sikkerhetsfunksjoner. Den elektroniske hjelpen for Windows Server 2003 inneholder fullstendig informasjon om alle sikkerhetsfunksjonene og fremgangsmåtene.

Hvis du vil ha mer informasjon om Windows 2000 Server, kan du besøke Windows 2000 Server Security Center på http://www.microsoft.com/technet/security/prodtech/win2000/default.mspx.

og lese Windows 2000 Security Hardening Guide på følgende webområde: http://www.microsoft.com/technet/security/prodtech/win2000/win2khg/default.mspx

Hvis du vil ha mer informasjon om Windows Server 2003, se *Windows Server 2003 Security Guide* på http://www.microsoft.com/technet/security/prodtech/win2003/w2003hg/sgch00.mspx.

De viktigste funksjonene i sikkerhetsmodellen for Windows Server er godkjenning, tilgangskontroll og enkel pålogging:

- Godkjenning er prosessen systemet bruker til å bekrefte identiteten til en bruker ved hjelp av legitimasjonsbeskrivelsene. Brukerens navn og passord vurderes opp mot en godkjent liste. Hvis systemet får et treff, får brukeren tilgang i den grad som er angitt i tillatelseslisten for den aktuelle brukeren.
- Tilgangskontrollen begrenser brukertilgangen til informasjon eller databehandlingsressurser basert på brukerens identitet og vedkommendes medlemskap i forskjellige forhåndsdefinerte grupper. Tilgangskontroll brukes vanligvis av systemansvarlige til å kontrollere hvilken tilgang brukerne har til nettverksressurser som servere, kataloger og filer. Dette implementeres vanligvis ved å gi brukere og grupper tillatelse til å åpne bestemte objekter.
- Enkel pålogging gjør at brukeren kan logge på Windows-domenet én gang, ved hjelp av ett passord, og bli godkjent på alle datamaskiner i Windows-domenet. Enkel pålogging gjør administratorer i stand til å implementere passordgodkjenning på tvers av Windows-nettverket, samtidig som det bli enklere for sluttbrukere å få tilgang.

Delene nedenfor inneholder mer detaljerte beskrivelser av disse tre hovedfunksjonene.

Godkjenning

Godkjenning er en grunnleggende del av systemsikkerhet og brukes til å bekrefte identiteten til alle brukere som prøver å logge på et domene eller få tilgang til nettverksressurser. Det svake leddet i de fleste godkjenningssystemer er brukerens passord.

Passord er den første beskyttelsen mot uautorisert tilgang til domenet og lokale datamaskiner. Anbefal følgende gode fremgangsmåter for passord:

- Bruk alltid sterke passord.
- Hvis passord må skrives ned på papir, må papiret lagres på et sikkert sted og ødelegges når det ikke lenger er bruk for det.

- Del aldri passord med andre.
- Bruk forskjellige passord for alle brukerkontoer.
- Endre passord regelmessig.
- Vær forsiktig med hvor passord lagres på datamaskinene.

Sterke passord

Det er vanlig å undervurdere og overse hvilken rolle passord spiller i sikringen av nettverket til en organisasjon. Som nevnt tidligere er passord den første beskyttelsen mot uautorisert tilgang til nettverket. Du må derfor sikre at kundene instruerer de ansatte om å bruke sterke passord.

Verktøyene som brukes til å løse passord, blir imidlertid stadig bedre, og datamaskinene som brukes til å løse passord, er kraftigere enn noen gang. Verktøyene for automatisk løsing av passord kan løse alle passord bare de får nok tid på seg. Sterke passord er likevel mye vanskeligere å løse enn svake passord.

Hvis du vil se retningslinjer for hvordan du oppretter sterke passord som brukeren kan huske, se følgende webområder:

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

og

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

Definere passordregler

Når du hjelper kunden med å definere passordregler, må du huske å lage regler som krever at alle brukerkontoer har sterke passord. For de fleste systemer er det nok å følge anbefalingene i sikkerhetsveiledningen for Windows Server 2003:

- Definer policyinnstillingen **Tving passordlogg**, slik at flere tidligere passord huskes. Med denne policyinnstillingen kan ikke brukere bruke det samme passordet når passordet utløper.

  Anbefalt innstilling: 24

- Definer policyinnstillingen **Maksimal passordalder** slik at passord utløper så ofte som nødvendig for kundens miljø.

  Anbefalt innstilling: mellom 42 (standardinnstillingen) og 90.

- Definer policyinnstillingen **Minimal passordalder** slik at passord ikke kan endres før de er et visst antall dager gamle. Denne policyinnstillingen fungerer sammen med policyinnstillingen **Tving passordlogg**. Hvis en minimal passordalder er definert, kan ikke brukerne endre passordene gjentatte ganger for å omgå policyinnstillingen **Tving passordlogg** og deretter bruke de opprinnelige passordene. Brukerne må vente i det angitte antallet dager før de kan endre passordene.

  Anbefalt innstilling: 2.

- Definer policyinnstillingen **Minimal passordlengde** slik at passord må bestå av minst et angitt antall tegn. Lange passord, på sju eller flere tegn, er vanligvis sterkere enn korte passord. Med denne policyinnstillingen kan ikke brukerne bruke tomme passord, og de må opprette passord som består av minst et visst antall tegn.

  Anbefalt innstilling: 8.

- Aktiver policyinnstillingen **Passord må møte kravene**. Denne policyinnstillingen kontrollerer alle nye passord for å sikre at de oppfyller de grunnleggende kravene til sterke passord. Denne innstillingen sikrer at passord har minst tre symboler fra de fire kategoriene (store bokstaver, små bokstaver, tall, ikke-alfanumeriske symboler), og at et passord ikke inneholder noen deler av brukernavnet og brukerens for- eller etternavn.

  Obs!
  Passord som oppfyller disse kravene, trenger ikke å være spesielt sterke. Passordet "Passord1" oppfyller for eksempel disse kravene.

  Anbefalt innstilling: Ja

- Hvis du vil se en fullstendig liste over disse kravene, se Password Must Meet Complexity Requirements i den elektroniske hjelpen for Windows Server.

- Lagre passord ved hjelp av reverserbar kryptering. Reverserbar kryptering brukes i systemer der et program trenger tilgang til klartekstpassord. Det er ikke nødvendig i de fleste typer distribusjoner.

  Anbefalt innstilling: Nei.

Hvis du vil ha mer informasjon, se sikkerhetsveiledningen for Windows Server 2003 på følgende webområde:

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

Definere regler for låsing av konto

Vær forsiktig når du definerer regler for låsing av konto. Regler for låsing av konto skal aldri angis i et lite selskap, ettersom det er stor sjanse for at autoriserte brukere også låses ute, og det kan være svært kostbart for kunden.

Hvis kunden bestemmer seg for å bruke regler for låsing av konto, setter du policyinnstillingen **Terskelverdi for låsing av konto** til et høyt nok tall slik at autoriserte brukere ikke låses ute av brukerkontoene sine bare fordi de skriver passordene feil flere ganger.

Hvis du vil ha mer informasjon om regler for låsing av konto, se Account Lockout Policy Overview i den elektroniske hjelpen for Windows Server.

Hvis du vil ha informasjon om hvordan du bruker eller endrer regler for låsing av konto, se To Apply or Modify Account Lockout Policy i den elektroniske hjelpen for Windows Server.

Tilgangskontroll

Et Windows-nettverk og tilhørende ressurser (inkludert Navision) kan sikres ved å vurdere hvilke rettigheter brukere, grupper av brukere og andre datamaskiner skal ha i nettverket. Du kan sikre en datamaskin eller flere datamaskiner ved å innvilge brukere eller grupper bestemte brukerrettigheter. Du kan sikre et objekt, for eksempel en fil eller mappe, ved å tilordne tillatelser som gjør det mulig for brukere eller grupper å utføre bestemte handlinger på det aktuelle objektet. Følgende konsepter er hovedkonsepter i tilgangskontroll:

- Tillatelser
- Eierskap over objekter
- Arv av tillatelser
- Brukerrettigheter
- Objektovervåking

Tillatelser

Tillatelser definerer tilgangstypen som en bruker eller gruppe innvilges for et objekt eller en objektegenskap, for eksempel filer, mapper og registerobjekter. Tillatelser brukes på alle sikrede objekter, for eksempel filer eller registerobjekter. Tillatelser kan gis til alle brukere, grupper eller datamaskiner. Det er lurt å tilordne tillatelser til grupper.

Eierskap over objekter

En eier tilordnes et objekt når objektet opprettes. I Windows 2000 Server er eieren som standard opphavsmannen til objektet. Dette er blitt endret i Windows Server 2003 for objekter som opprettes av medlemmer av Administratorer-gruppen.

Når et medlem av Administratorer-gruppen oppretter et objekt i Windows Server 2003, blir Administratorer-gruppen eieren i stedet for kontoen som opprettet objektet. Denne virkemåten kan endres via MMC-snapin-modulen Lokale sikkerhetsinnstillinger, ved hjelp av innstillingen **Systemobjekter: Standardeier for objekter opprettet av medlemmer av gruppen Administratorer**. Uansett hvilke tillatelser som er angitt for et objekt, kan eieren av objektet alltid endre tillatelsene for et objekt.

Hvis du vil ha mer informasjon, se Ownership i den elektroniske hjelpen for Windows Server.

Arv av tillatelser

Med arv kan administratorer enkelt tilordne og håndtere tillatelser. Denne funksjonen forårsaker at objekter i en beholder automatisk arver alle arvbare tillatelser i den aktuelle beholderen. Når du for eksempel oppretter filer i en mappe, arver de tillatelsene i mappen. Bare tillatelsene som er merket for å skulle arves, blir arvet.

Brukerrettigheter

Brukerrettigheter gir brukere og grupper i databehandlingsmiljøet spesielle rettigheter og påloggingsrettigheter.

Hvis du vil ha informasjon om brukerrettigheter, se User Rights i den elektroniske hjelpen for Windows Server.

Objektovervåking

Du kan overvåke brukernes tilgang til objekter. Du kan deretter vise disse sikkerhetsrelaterte hendelsene i sikkerhetsloggen ved hjelp av Hendelsesliste.

Hvis du vil ha mer informasjon, se Auditing i den elektroniske hjelpen for Windows Server.

Gode fremgangsmåter for tilgangskontroll

- Tilordne tillatelser til grupper i stedet for til brukere. Da det er lite effektivt å vedlikeholde brukerkontoer direkte, bør du bare unntaksvis tilordne tillatelser til brukere.
- Merk av for tillatelser under Avslå for visse spesialtilfeller. Du kan for eksempel merke av for tillatelser under Avslå for å ekskludere et delsett av en gruppe som det er merket av for tillatelser under Tillat for.
- Ikke nekt Alle-gruppen tilgang til et objekt. Hvis du nekter Alle-gruppen tillatelser til et objekt, omfatter det også administratorene. En bedre løsning vil være å fjerne Alle-gruppen, dersom du gir andre brukere, grupper eller datamaskiner tillatelser til det aktuelle objektet. Husk at hvis ingen tillatelser er definert, er ingen tilgang tillatt.
- Tilordne tillatelser til et objekt så høyt på treet som mulig, og bruk deretter arv for å overføre sikkerhetsinnstillingene til hele treet. Du kan raskt og effektivt bruke innstillinger for tilgangskontroll på alle underordnede objekter eller et undertre for et overordnet objekt. Ved å gjøre dette får du størst mulig effekt med minst mulig innsats. Tillatelsesinnstillingene du velger, bør passe for de fleste brukere, grupper og datamaskiner.
- Eksplisitte tillatelser kan noen ganger overstyre arvede tillatelser. Arvede avslåtte tillatelser hindrer ikke tilgang til et objekt hvis objektet har en eksplisitt tillatende tillatelsesoppføring. Eksplisitte tillatelser har forrang over arvede tillatelser, selv arvede avslåtte tillatelser.
- For tillatelser for Active Directory®-objekter må du være sikker på at du forstår de gode fremgangsmåtene for Active Directory-objekter.

Hvis du vil ha mer informasjon, se Best Practices for Assigning Permissions on Active Directory Objects i den elektroniske hjelpen for Windows Server 2003.

Ekstern sikkerhetsbrannmur

En brannmur er maskinvare eller programvare som hindrer at datapakker kommer inn i eller forlater et bestemt nettverk. Porter i brannmuren er enten åpne eller lukket for informasjonspakker for å kontrollere trafikkflyten. Brannmuren ser på flere typer informasjon i hver datapakke: protokollen som pakken leveres gjennom, målet for eller avsenderen av pakken, hvilken type

innhold pakken har, og portnummeret den sendes til. Hvis brannmuren er konfigurert til å godta den angitte protokollen gjennom målporten, får pakken passere. Microsoft Windows Small Business Server 2003 Premium Edition leveres med Microsoft Internet Security and Acceleration (ISA) Server 2000 som brannmurløsning. Small Business Server Standard Edition inneholder også en brannmur.

ISA Server 2004

Internet Security and Acceleration (ISA) Server 2000 dirigerer forespørsler og svar sikkert mellom Internett og klientdatamaskinene i det interne nettverket.

ISA Server fungerer som sikker gateway til Internett for klienter i det lokale nettverket. ISA Server-datamaskinen er gjennomsiktig for de andre partene i kommunikasjonsbanen. Internett-brukeren vil ikke kunne se at det finnes en brannmurserver, med mindre brukeren forsøker å få tilgang til en tjeneste eller gå til et område som ISA Server-datamaskinen nekter brukeren tilgang til. Internett-serveren som noen prøver å få tilgang til, tolker forespørslene fra ISA Server-datamaskinen som om forespørslene kom fra klientprogrammet.

Når du velger fragmentfiltrering i Internett-protokollen, gjør du nettproxy- og brannmurtjenestene i stand til å filtrere pakkefragmenter. Ved å filtrere pakkefragmenter forkastes alle fragmenterte IP-pakker. Et kjent angrep går ut på å sende fragmenterte pakker og deretter sette dem sammen igjen på en måte som kan skade systemet.

ISA Server har en mekanisme som oppdager forsøk på inntrenging, og som identifiserer tidspunktet for et angrepsforsøk mot et nettverk og utfører en rekke konfigurerte handlinger (eller varsler) ved angrepsforsøk.

Hvis Internet Information Services (IIS) er installert på ISA Server-datamaskinen, må du konfigurere den slik at den ikke bruker portene som ISA Server bruker for utgående nettforespørsler (som standard 8080) og innkommende nettforespørsler (som standard 80). Du kan for eksempel endre IIS til å overvåke port 81, og deretter kan du konfigurere ISA Server-datamaskinen til å dirigere innkommende nettforespørsler til port 81 på den lokale datamaskinen som kjører IIS.

Hvis det oppstår en konflikt mellom porter som ISA Server og IIS bruker, stopper installasjonsprogrammet IIS-publiseringstjenesten. Du kan deretter endre IIS til å overvåke en annen port og starte IIS-publiseringstjenesten på nytt.

Regler for ISA Server

Du kan definere regler for ISA Server som styrer inngående og utgående tilgang. Regler for område og innhold angir hvilke områder og hvilket innhold det skal være mulig å få tilgang til. Protokollregler angir om en bestemt protokoll skal være tilgjengelig for inngående og utgående kommunikasjon.

Du kan opprette regler for område og innhold, protokollregler, nettpubliseringsregler og IP-pakkefiltre. Disse reglene bestemmer hvordan ISA Server-klientene kommuniserer med Internett og hvilken kommunikasjon som er tillatt.

Beskyttelse mot virus

Et datavirus er en kjørbar fil som er utformet for å replikere seg selv, slette eller skade datafiler og -programmer, og unngå å bli oppdaget. Virus skrives ofte om og justeres slik at de ikke kan bli oppdaget. Virus sendes ofte som e-postvedlegg. Antivirusprogrammer må oppdateres kontinuerlig for at de skal kunne se etter nye og endrede virus. Virus er den vanligste metoden for å skade datamaskiner.

Antivirusprogramvare er spesielt utformet for å oppdage og forhindre virusprogrammer. Ettersom det opprettes nye virusprogrammer hele tiden, tilbyr mange produsenter av antivirusprodukter kundene sine periodiske oppdateringer av programvaren. Microsoft anbefaler på det sterkeste å implementere antivirusprogramvare i kundens miljø.

Virusprogramvare installeres vanligvis på følgende tre steder: arbeidsstasjoner for brukere, servere og nettverket der e-postmeldinger kommer inn til (og i noen tilfeller forlater) organisasjonen.

Virustyper

Det finnes tre hovedtyper virus som infiserer datasystemer: oppstartssektorvirus, filinfiserende virus og trojanske hester.

Oppstartssektorvirus

Når en datamaskin starter, skanner den oppstartssektoren på harddisken før operativsystemet eller andre oppstartsfiler lastes inn. Et oppstartssektorvirus er utformet for å erstatte informasjonen i oppstartssektorene på harddisken med egen kode. Når en datamaskin infiseres med et oppstartssektorvirus, leses koden til viruset inn i minnet før noe annet. Når viruset er i minnet, kan det replikere seg selv på andre disker som er i bruk på den infiserte datamaskinen.

Filinfiserende virus

Den vanligste virustypen, et filinfiserende virus, kobler seg til en kjørbar programfil ved å legge til sin egen kode i den kjørbare filen. Viruskoden legges vanligvis til på en måte som gjør at den ikke blir oppdaget. Når den infiserte filen kjøres, kan viruset koble seg til andre kjørbare filer. Filer som blir infisert av denne typen virus, er vanligvis av typene COM, EXE eller SYS.

Noen filinfiserende virus er utformet for bestemte programmer. Programtyper som ofte er mål for virus, er OVL- og DDL-filer. Selv om disse filene ikke kjøres, kaller kjørbare filer dem. Viruset overføres når kallet utføres.

Skade på data oppstår når viruset utløses. Et virus kan utløses når en infisert fil kjøres, eller når en bestemt miljøinnstilling oppfylles (for eksempel en bestemt systemdato).

Trojanske hester

En trojansk hest er ikke egentlig et virus. Den viktigste forskjellen mellom et virus og en trojansk hest er at en trojansk hest ikke replikerer seg selv. Den bare ødelegger informasjon på harddisken. En trojansk hest forkler seg som et legitimt program, for eksempel et spill eller et verktøy. Når den kjøres, kan den imidlertid ødelegge eller skade data.

Gode fremgangsmåter for beskyttelse mot virus

Spredning av et makrovirus kan forhindres. Her er noen tips for å unngå infisering, som du bør dele med kundene:

- Installer en løsning for virusbeskyttelse som skanner innkommende meldinger fra Internett for virus før meldingene passerer ruteren. Da sikrer du at e-postmeldinger skannes for kjente virus.
- Kjenn til kilden for dokumentene som mottas. Dokumenter bør ikke åpnes med mindre de er fra noen kunden stoler på.
- Snakk med personen som opprettet dokumentet. Hvis brukerne er det minste i tvil om dokumentet er trygt, bør de kontakte personen som opprettet dokumentet.
- Bruk beskyttelsesprogrammet mot makrovirus i Microsoft Office. I Office varsles brukerne dersom et dokument inneholder makroer. Denne funksjonen gjør brukeren i stand til å aktivere eller deaktivere makroene når dokumentet åpnes.
- Bruk programvare for virusskanning til å oppdage og fjerne makrovirus. Programvare for virusskanning kan oppdage og ofte fjerne makrovirus fra dokumenter. Microsoft anbefaler bruk av antivirusprogramvare som er sertifisert av International Computer Security Association (ICSA).

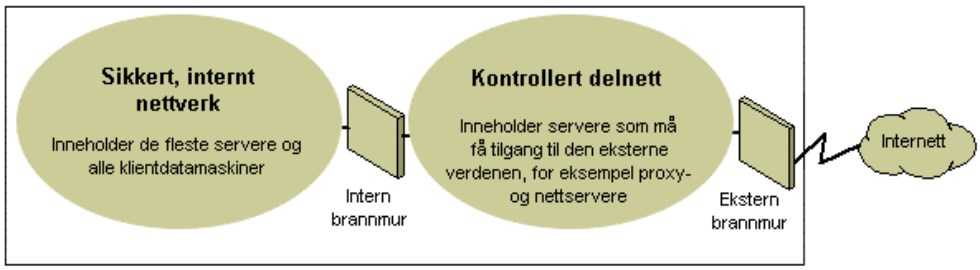
Hvis du vil ha mer informasjon om virus og datamaskinsikkerhet generelt, kan du besøke følgende webområder for Microsoft-sikkerhet:

- Microsoft-sikkerhet på http://www.microsoft.com/security/default.asp.
- Sikkerhetsdokumentasjon på Microsoft TechNet http://www.microsoft.com/technet/security/Default.mspx.

Strategier for nettverkssikkerhet

Ettersom utformingen og distribusjonen av et IP/IPX-miljø krever at private og offentlige nettverksanliggender balanseres, er brannmuren blitt en hovedingrediens i beskyttelsen av nettverksintegritet. En brannmur er ikke én komponent. National Computer Security Association (NCSA) definerer en brannmur som "et system eller en kombinasjon av systemer som etablerer en grense mellom to eller flere nettverk". Selv om forskjellige ord brukes, er denne grensen ofte kjent som et kontrollert delnett. Det kontrollerte delnettet beskytter intranettet eller lokalnettet for bedriften mot inntrenging ved å kontrollere tilgangen fra Internett eller andre store nettverk.

Diagrammet nedenfor viser et kontrollert delnett som er omkranset av brannmurer og plassert mellom et privat nettverk og Internett for å sikre det private nettverket:



Grunnleggende kontrollert delnett

Organisasjoner bruker brannmurer på svært forskjellige måter for å beskytte seg. IP-pakkefiltrering gir dårlig sikkerhet, er tungvint å håndtere, og er enkelt å bryte gjennom. Program-gatewayer er sikrere enn pakkefiltre og enklere å håndtere ettersom de bare gjelder for noen få bestemte programmer, for eksempel et bestemt e-postsystem. Krets-gatewayer er mest effektive når brukeren av et nettverksprogram er viktigere enn dataene som sendes av det aktuelle programmet. Proxy-serveren er et omfattende sikkerhetsverktøy som inkluderer en program-gateway, sikker tilgang for anonyme brukere og andre tjenester. Her er litt informasjon om disse forskjellige alternativene:

- **IP-pakkefiltrering**
  IP-pakkefiltrering var den første implementeringen av brannmurteknologi. Pakkehoder undersøkes for kilde- og måladresser, TCP- (Transmission Control Protocol) og UDP-portnumre (User Datagram Protocol) og annen informasjon. Pakkefiltrering er en begrenset teknologi som fungerer best i klare sikkerhetsmiljøer der for eksempel alt utenfor det kontrollerte delnettet ikke er klarert, og alt innenfor er klarert. De siste årene har en rekke leverandører forbedret sine pakkefiltreringsmetoder ved å legge til intelligente funksjoner for beslutningstaking i pakkefiltreringskjernene, og dermed er en ny form for pakkefiltrering opprettet, kalt *tilstandsfull protokollinspeksjon.* Du kan konfigurere pakkefiltrering til enten å godta bestemte typer pakker mens alle andre typer nektes, eller å nekte bestemte typer pakker og godta alle andre.
- **Program-gatewayer**
  Program-gatewayer brukes når innholdet i et program er viktigst. At de er programspesifikke er både en styrke og begrensning, for de tilpasses ikke så enkelt til endringer i teknologi.
- **Krets-gatewayer**
  Krets-gatewayer er tunneler som bygges via en brannmur som kobler bestemte prosesser eller systemer på den ene siden til bestemte prosesser eller systemer på den andre siden. Krets-gatewayer er aller best å bruke i situasjoner der personen som bruker et program, potensielt er en større risiko enn informasjonen som sendes av programmet. Krets-gatewayen skiller seg fra et pakkefilter ved at den kan koble til et utenforliggende program som kan legge til ytterligere informasjon.
- **Proxy-servere**
  Proxy-servere er omfattende sikkerhetsverktøy som inkluderer gateway-funksjonalitet for brannmurer og programmer, som håndterer Internett-trafikk til og fra et lokalt nettverk. Proxy-servere tilbyr også dokumentbufring og tilgangskontroll. En proxy-server kan forbedre ytelsen ved at den bufrer og leverer data som forespørres ofte, direkte, for eksempel en populær nettside. En proxy-server kan også filtrere og forkaste forespørsler som eieren ikke synes er passende, for eksempel forespørsler om uautorisert tilgang til proprietære filer.

Pass på at kundene utnytter sikkerhetsfunksjonene i brannmuren som kan være nyttige for dem. Plasser et kontrollert delnett på et sted i nettverkstopologien der all trafikk som kommer fra utenfor bedriftsnettverket, må passere gjennom delnettet som den eksterne brannmuren vedlikeholder. Du kan finjustere tilgangskontrollen for brannmuren slik at den dekker kundens behov, og konfigurere brannmurer til å rapportere alle forsøk på uautorisert tilgang.

Hvis du vil minimere antallet porter du trenger for å åpne den interne brannmuren, kan du bruke en brannmur for programlag, for eksempel ISA Server 2000.

Hvis du vil ha mer informasjon om TCP/IP, se Designing a TCP/IP Network på http://www.microsoft.com/resources/documentation/WindowsServ/2003/all/deployguide/en-us/dnsbb_tcp_overview.asp.

Trådløse nettverk

Trådløse nettverk konfigureres som standard på en måte som gjør det mulig å tyvlytte på de trådløse signalene. De kan være sårbare for ondsinnede utenforstående som får tilgang på grunn av standardinnstillingene på noe trådløs maskinvare, tilgjengeligheten til trådløse nettverk og gjeldende krypteringsmetoder. Det finnes konfigurasjonsalternativer og -verktøy som kan beskytte mot tyvlytting, men husk på at de ikke gjør noe for å beskytte datamaskinene mot hackere og virus som kommer inn gjennom Internett-tilkoblingen. Av den grunn er det svært viktig å bruke en brannmur for å beskytte datamaskinene mot uønskede inntrengere på Internett.

Hvis du vil ha mer informasjon om hvordan du beskytter et trådløst nettverk, se How to Make Your 802.11b Wireless Home Network More Secure på http://support.microsoft.com/default.aspx?scid=kb;en-us;309369.

Scenarier for nettverkssikkerhet

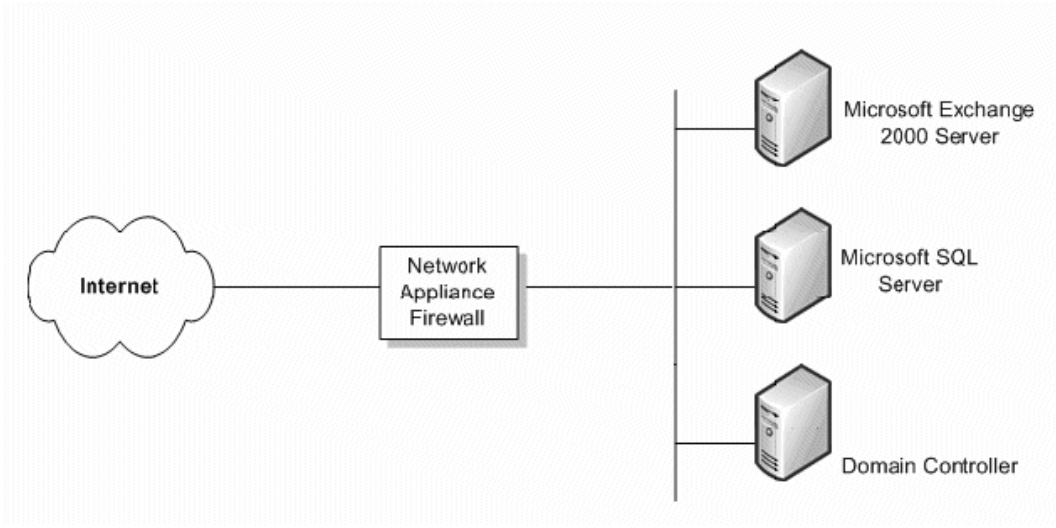
Hvilket nivå av nettverkssikkerhet kundens organisasjon trenger, er avhengig av flere faktorer. Det er vanlig å måtte få til et kompromiss mellom budsjett og behovet for å holde bedriftsdataene sikre. Det er mulig for en liten bedrift å ha en svært sammensatt sikkerhetsstruktur som gir det høyeste nivået av nettverkssikkerhet som er mulig, men en liten bedrift vil kanskje ikke ha råd til et slikt sikkerhetsnivå. I denne delen ser vi på fire scenarier og gir anbefalinger i hvert scenario som gir varierende sikkerhetsnivåer.

Ingen brannmur

Hvis kunden har en tilkobling til Internett, men ingen brannmur, må én eller annen form for nettverkssikkerhet implementeres. Det finnes enkle nettverksbrannmurer som gir nok sikkerhet til å stoppe de fleste potensielle hackere.

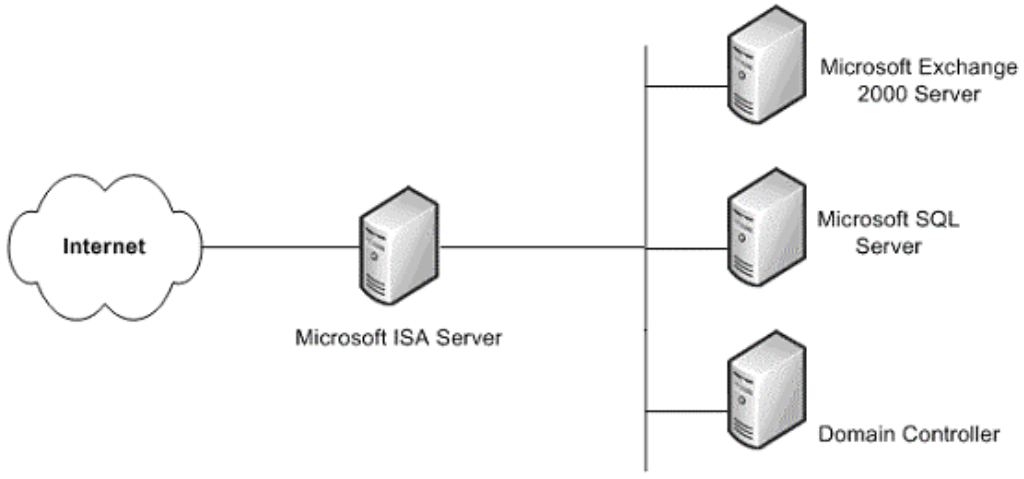
Én enkel brannmur

Det laveste sikkerhetsnivået som anbefales, er én brannmur mellom Internett og kundens data. Denne brannmuren gir kanskje ikke noe avansert sikkerhetsnivå, og bør ikke anses som særlig sikker. Den er imidlertid bedre enn ingen brannmur.



Enkel brannmur

Forhåpentligvis tillater kundens budsjett en sikrere løsning som beskytter bedriftsdataene. Én slik løsning er ISA Server. Den økte kostnaden ved denne tilleggsserveren gir mye større sikkerhet enn gjennomsnittlige forbrukerbrannmurer, ettersom de vanligvis bare utfører nettverksadresseoversetting (NAT) og pakkefiltrering.



ISA Server-brannmur

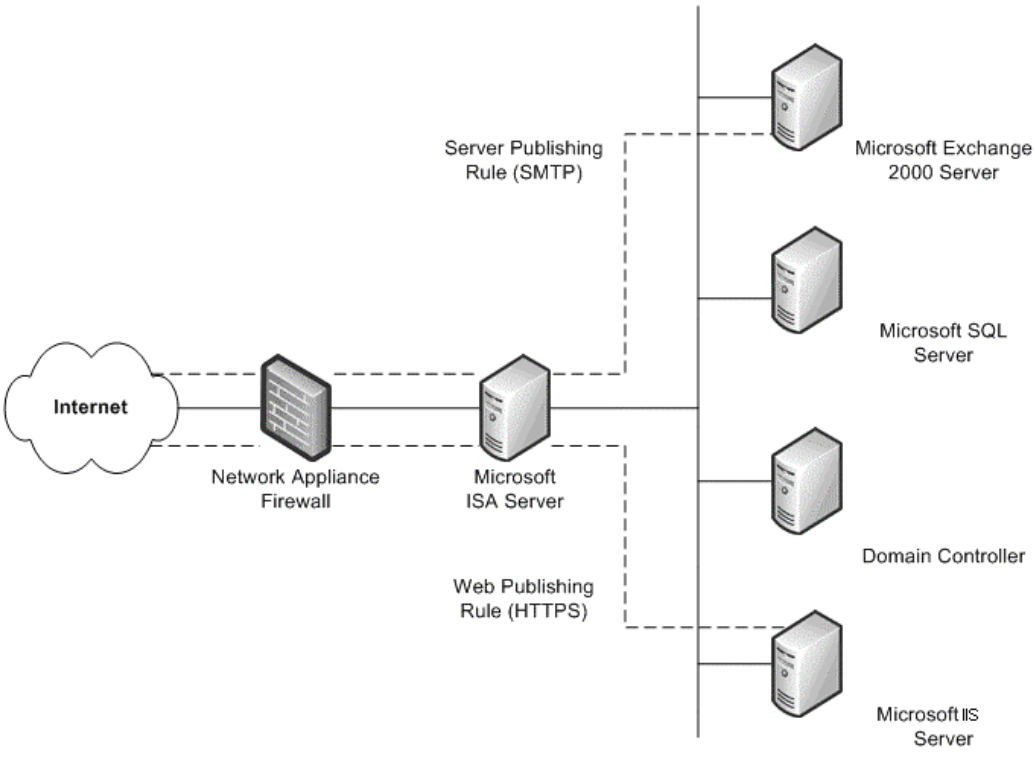
Denne enkle brannmurløsningen er sikrere enn en brannmur på inngangsnivå og tilbyr Windows-spesifikke sikkerhetstjenester.

Én eksisterende brannmur

Hvis kunden har en eksisterende brannmur som skiller intranettet fra Internett, kan du vurdere å supplere med en ekstra brannmur som tilbyr flere måter å konfigurere interne ressurser på til Internett.

Én slik metode er nettpublisering. Det er når en ISA-server brukes foran nettserveren i en organisasjon, som gir Internett-brukere tilgang. Med innkommende nettforespørsler kan ISA-serveren utgi seg for å være en nettserver overfor verden utenfor, og oppfylle klientforespørsler etter nettinnhold fra bufferen. ISA Server videresender forespørsler til nettserveren bare når forespørslene ikke kan betjenes fra bufferen.

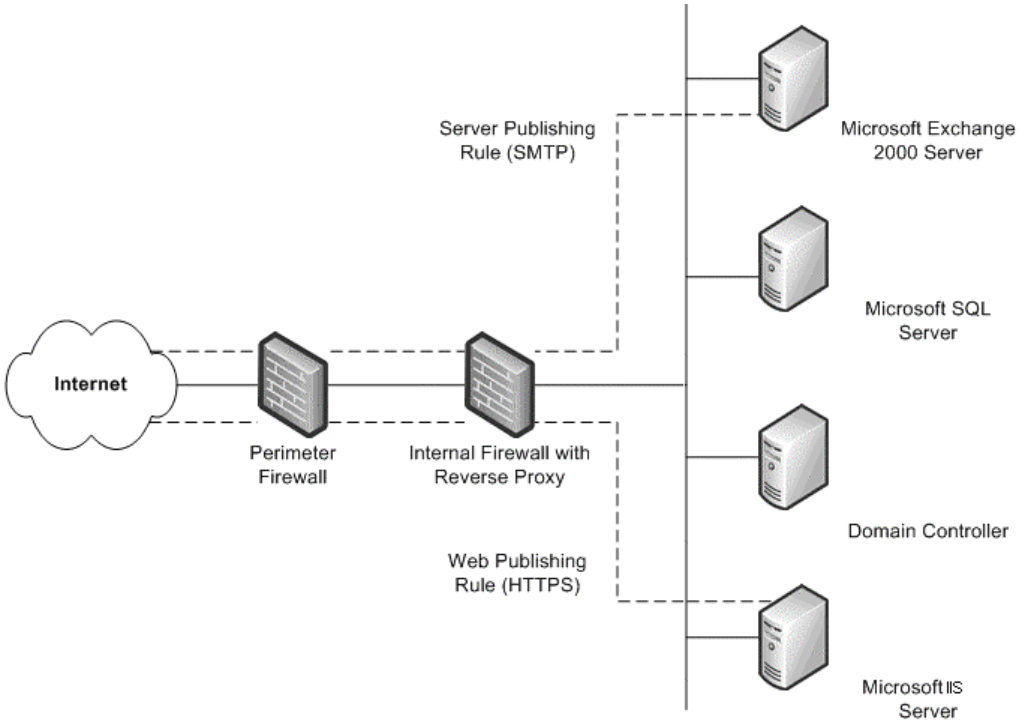
En annen metode er serverpublisering. ISA Server tillater at interne servere publiseres til Internett uten at det går på bekostning av sikkerheten for det interne nettverket. Du kan konfigurere regler for nettpublisering og serverpublisering som bestemmer hvilke forespørsler som skal sendes til en server på det lokale nettverket, noe som gir økt sikkerhet for de interne serverne.



Eksisterende brannmur med ekstra ISA Server

To eksisterende brannmurer

Det fjerde scenariet er når organisasjonen har to brannmurer med et kontrollert delnett etablert. Én eller flere av disse serverne inneholder omvendte proxy-tjenester, slik at Internett-klienter ikke får direkte tilgang til servere på intranettet. I stedet fanger én av brannmurene, helst den interne brannmuren, opp nettverksforespørsler for interne servere, inspiserer disse pakkene, og videresender dem deretter på vegne av Internett-verten.



To eksisterende brannmurer

Dette scenariet ligner på det forrige scenariet når den andre brannmuren er lagt til. Den eneste forskjellen er at den interne brannmuren som støtter omvendt proxy, ikke er en ISA-server. I dette scenariet bør du arbeide tett opp mot administratorene for hver av brannmurene for å definere regler for serverpublisering som er i overensstemmelse med sikkerhetsreglene.

Administrasjon av sikkerhetsoppdateringer

Operativsystemer og programmer er ofte svært sammensatte. De kan bestå av millioner av linjer med kode som er skrevet av mange forskjellige programmerere. Det er viktig at programvaren fungerer som den skal, og at den ikke setter sikkerheten eller stabiliteten til IT-miljøet i fare. Programmer testes grundig før de gis ut for å minimere eventuelle problemer. Ondsinnede brukere prøver imidlertid stadig å finne svakheter i programvare, så det er ikke mulig å forutse alle fremtidige angrep.

For mange organisasjoner er administrasjon av oppdateringer en del av den generelle strategien for administrasjon av endringer og konfigurasjon. Samme hvilken type organisasjon det er og hvor stor den er er det likevel viktig å ha en god strategi for administrasjon av oppdateringer, selv om organisasjonen ikke ennå har effektiv administrasjon av endringer og konfigurasjon. De aller fleste vellykkede angrep mot datasystemer skjer på systemer som ikke har sikkerhetsoppdateringer installert.

Sikkerhetsoppdateringer er en spesifikk utfordring for de fleste organisasjoner. Når en svakhet først er eksponert i programvare, sprer ondsinnede brukere vanligvis informasjon om den raskt i hackermiljøet. Når en svakhet oppstår i Microsoft-programvare, prøver Microsoft å gi ut en sikkerhetsoppdatering så raskt som mulig. Før oppdateringen er distribuert, kan sikkerheten som kunden er avhengig av og forventer, være alvorlig svekket.

I Navision-miljøet må du sikre at kundene har de nyeste sikkerhetsoppdateringene installert i hele systemet. Kontroller at kunden bruker én av teknologiene som Microsoft har gjort tilgjengelig. De er:

- **Microsofts sikkerhetsvarslingstjeneste**
  Sikkerhetsvarslingstjenesten er en e-postliste som distribuerer varsler når en oppdatering blir tilgjengelig. Disse varslene er en verdifull del av en proaktiv sikkerhetsstrategi. De er også tilgjengelige på TechNets webområde for produktsikkerhetsvarsling: http://www.microsoft.com/technet/security/bulletin/notify.mspx.
- **Microsofts automatiske oppdateringer**
  Windows kan bruke sikkerhetsoppdateringer på maskinene automatisk.
- **Microsofts sikkerhetsbulletinsøkeverktøy**
  Sikkerhetsbulletinsøkeverktøyet er tilgjengelig på webområdet for sikkerhetsbulletintjenesten: http://www.microsoft.com/technet/security/current.aspx. Kunden kan bestemme hvilke oppdateringer vedkommende trenger basert på operativsystemet, programmene og serviceoppgraderingene de kjører for øyeblikket.
- **Microsoft Baseline Security Analyzer (MBSA)**
  Dette grafiske verktøyet er tilgjengelig på webområdet for Microsoft Baseline Security Analyzer: http://www.microsoft.com/technet/security/tools/mbsahome.mspx. Dette verktøyet sammenligner gjeldende status for en datamaskin med en liste over oppdateringer som vedlikeholdes av Microsoft. MBSA utfører også noen grunnleggende sikkerhetskontroller for passordstyrke og utløpsinnstillinger, regler for gjestekontoer og en rekke andre områder. MBSA ser også etter sårbarheter i Microsoft Internet Information Services (IIS), SQL Server™ 2000, Exchange 5.5, Exchange 2000 og Exchange Server 2003.
- **Microsofts tjenester for programvareoppdatering (SUS - Software Update Services)**
  Dette verktøyet, som tidligere var kjent som Windows Update Corporate Edition, gjør selskaper i stand til å være vert for alle kritiske oppdateringer og SRPer (Security Rollup Packages) som er tilgjengelige på det offentlige Windows Update-webområdet, på lokale datamaskiner. Dette verktøyet fungerer sammen med en ny versjon av Automatiske oppdateringer-klienter og danner grunnlaget for en kraftig automatisk nedlastings- og installasjonsstrategi. Det nye klientsettet for automatiske oppdateringer inneholder en klient for Windows 2000- og Windows Server 2003-operativsystemer og kan installere nedlastede oppdateringer automatisk. Hvis du vil ha mer informasjon om Microsofts tjenester for programvareoppdatering (SUS), se http://www.microsoft.com/windows2000/windowsupdate/sus/default.asp.

- **Microsofts funksjonalitetspakke for tjenester for programvareoppdatering, Systems Management Server (SMS)**
  Funksjonalitetspakken for tjenester for programvareoppdatering, SMS, inneholder en rekke verktøy som skal lette prosessen med å utstede programvareoppdateringer i selskapet. Verktøyene inneholder et innholdsverktøy for sikkerhetsoppdateringer, et innholdsverktøy for Microsoft Office-oppdateringer, veiviseren for distribusjon av programvareoppdateringer og et nettrapporteringsverktøy for SMS med tilleggsprogram for nettrapporter for programvareoppdateringer. Hvis du vil ha mer informasjon om hvert verktøy, se http://www.microsoft.com/smserver/downloads/20/featurepacks/suspack/.

Snakk med kundene om hvert av disse verktøyene, og oppmuntre dem til å bruke verktøyene. Det er svært viktig at sikkerhetstemaer tas opp så raskt som mulig, samtidig som stabiliteten i miljøet opprettholdes.

Sikkerhetsinnstillinger for SQL Server 2000

Ettersom Navision også kjører på SQL Server 2000, er det viktig at du iverksetter tiltak for å øke sikkerheten for kundens SQL Server 2000-installasjon. Trinnene nedenfor bidrar til å øke sikkerheten for SQL Server:

- Kontroller at det nyeste operativsystemet og de nyeste serviceoppgraderingene og oppdateringene for SQL Server 2000 er installert. Hvis du vil ha de nyeste opplysningene, går du til webområdet for Microsoft-sikkerhet http://www.microsoft.com/security/default.asp.
- Når du skal sjekke at sikkerheten på systemnivå er god, må du kontrollere at alle SQL Server 2000-data og -systemfiler er installert på NTFS-partisjoner. Du må gjøre filene tilgjengelige bare for brukere på administrator- eller systemnivå via NTFS-tillatelser. Da beskytter du mot at brukere får tilgang til disse filene når tjenesten MSSQLSERVER ikke kjører.
- Bruk en domenekonto med få rettigheter, for eksempel NT-myndighet\nettverkstjeneste eller kontoen LocalSystem (anbefales) for SQL Server 2000-tjenesten (MSSQLSERVER). Denne kontoen bør ha minimale rettigheter i domenet og bør bidra til å begrense (men ikke stoppe) angrep på serveren hvis sikkerheten reduseres. Med andre ord bør denne kontoen bare ha tillatelser på lokalt brukernivå i domenet. Hvis SQL Server 2000 bruker en domeneadministratorkonto til å kjøre tjenestene, vil en reduksjon i sikkerheten for serveren føre til reduksjon i sikkerheten for hele domenet. Hvis du vil endre denne innstillingen, bruker du SQL Server Enterprise Manager til å gjøre endringen. Tilgangskontrollistene (ACLene - Access Control Lists) til filer, registeret og brukerrettighetene endres automatisk.
- De fleste versjoner av SQL Server 2000 installeres med to standarddatabaser, **Gastronor** og **Pubs**. Begge databasene er eksempeldatabaser som brukes til testing, opplæring og generelle eksempler. De må ikke brukes i et produksjonssystem. Hvis ondsinnede brukere får kjennskap til at disse databasene er i bruk, kan de bli oppmuntret til å forsøke å utnytte standardinnstillinger og -konfigurasjon. Hvis **Gastronor** og **Pubs** finnes på produksjonsdatamaskinen for SQL Server 2000, må de fjernes.
- Overvåking av SQL Server 2000-systemet er som standard deaktivert, slik at ingen betingelser overvåkes. Dette gjør det vanskelig å oppdage inntrengere, og det er lettere for ondsinnede brukere å dekke sine spor. Du bør i det minste aktivere overvåking av mislykkede pålogginger.

Hvis du vil se den nyeste sikkerhetsinformasjonen for SQL Server 2000, se http://www.microsoft.com/sql/techinfo/administration/2000/security/default.asp.

Microsoft Business Solutions

Microsoft Business Solutions er en avdeling i Microsoft som tilbyr et stort utvalg integrerte, komplette bransjeprogrammer og tjenester som er utformet for å hjelpe mindre og større selskaper til å få et nærere forhold til sine kunder, ansatte, partnere og leverandører. Programmene til Microsoft Business Solutions optimaliserer strategiske forretningsprosesser for økonomisk styring, analysering, ressursstyring, prosjektstyring, kunderelasjonsstyring, ettersynsstyring, forsyningskjedestyring, e-handel, produksjons- og detaljsalgstyring. Programmene er utformet for å hjelpe kunder med å lykkes i forretningene. Du finner mer informasjon om Microsoft Business Solutions på http://www.microsoft.com/BusinessSolutions/