Microsoft Business Solutions

Manual de Consolidação da Segurança do Navision

Publicado em: Outubro de 2004

Microsoft

Conteúdo

Introdução

O Microsoft® Windows® fornece uma sofisticada segurança de rede baseada em padrões. A segurança, no mais amplo sentido, envolve planeamento e análise de compromissos. Por exemplo, um computador pode estar fechado num cofre e ser acessível apenas a um administrador de sistema. Este computador poderá estar seguro, contudo a sua utilidade é limitada, uma vez que não se encontra ligado a nenhum outro computador. É necessário ter em conta a concepção de uma rede que forneça os mais elevados padrões de segurança sem ter de abdicar da facilidade de utilização.

A maioria das organizações toma providências relativamente a ataques externos e instala *firewalls*, mas muitas empresas não concebem uma forma de prevenir falhas de segurança quando um utilizador mal intencionado consegue passar pelo *firewall*. As medidas de segurança no ambiente do seu cliente funcionarão de modo adequado se os utilizadores não tiverem que efectuar procedimentos e passos excessivos para realizarem a sua actividade empresarial com segurança. A implementação de políticas de segurança deve ser efectuada de uma forma simples e acessível aos utilizadores, caso contrário, eles procurarão alternativas menos seguras de realização das suas tarefas.

Dado que o tamanho das instalações do Navision pode variar substancialmente, é importante ponderar cuidadosamente as necessidades de cada cliente e comparar a eficácia da segurança em relação aos custos envolvidos. Enquanto assessor de confiança do seu cliente, utilize o bom senso e recomende uma política que satisfaça as necessidades de segurança sem criar uma sobrecarga que, em última instância, provoque o não cumprimento dessa política por parte do cliente.

Procedimentos Recomendados de Segurança do Navision

As seguintes regras gerais podem ajudar a aumentar a segurança do ambiente do Navision:

- Se pretender executar o Navision Database Server como um serviço ou utilizar o parâmetro de linha de comandos *installasservice* ao iniciar o servidor, deverá certificar-se de que o serviço está a ser executado como conta de Autoridade NT\Serviço de Rede. A conta de Autoridade NT\Serviço de Rede só existe no Windows™ XP e no Windows Server™ 2003. Se tiver instalado o Windows 2000 Server, deverá criar uma conta com os privilégios mínimos para o serviço, caso contrário, ser-lhe-á atribuída uma conta do Sistema Local. Esta conta deve ter, quando muito, os mesmos privilégios que as contas de utilizadores normais ou ser uma conta de domínio sem privilégios de administrador, independente da mesma se encontrar no domínio ou num computador local.

  É necessário atribuir acesso de leitura e escrita dos ficheiros da base de dados à conta de Autoridade NT\Serviço de Rede ou à conta de utilizador sob a qual o servidor se encontra em execução para garantir que os utilizadores conseguem estabelecer ligação à base de dados.

  Para atribuir acesso de leitura e escrita do ficheiro da base de dados no Windows XP à conta de Autoridade NT\Serviço de Rede:

  1. No Explorador do Windows, navegue para a pasta que contém o ficheiro da base de dados.
  2. Seleccione o ficheiro da base de dados, abra o menu de contexto com botão direito do rato e clique em Propriedades.
  3. Na janela ***Propriedades***, clique no separador ***Segurança*** e em Adicionar no campo **Nomes de utilizador ou grupo**.
  4. Na janela ***Seleccionar utilizadores, computadores ou grupos***, introduza *Serviço de Rede* e clique em OK.
  5. É adicionado SERVIÇO DE REDE ao campo **Nomes de utilizador ou grupo** na janela ***Propriedades***.
  6. Seleccione SERVIÇO DE REDE e, no campo **Permissões**, atribua-lhe a permissão *Ler e Escrever*.
- O serviço Navision Application Server é executado, por predefinição, como a conta de Autoridade NT\Serviço de Rede, o que lhe permite ter acesso local ao Navision Database Server. No entanto, numa rede é necessário garantir que o serviço Navision Application Server é executado como uma conta de domínio Windows, reconhecida pelo Navision Database Server, se pretender que o mesmo tenha acesso ao servidor da base de dados. Esta conta não deverá ter privilégios de administrador no domínio ou num computador local.
- Se estiver a executar a Opção de SQL Server para Navision, o Microsoft SQL Server™ é executado como um serviço. A Opção de SQL Server para Navision necessita que o SQL Server consiga efectuar pesquisas no Active Directory de forma a obter listas de grupos de utilizadores do Windows para efeitos de autenticação. É, assim, necessário garantir que o serviço SQL Server está a ser executado como conta de Autoridade NT\ Serviço de Rede.

Para se certificar de que o serviço está a ser executado como conta de Autoridade NT\ Serviço de Rede:

1. No computador com o SQL Server, localize o serviço MSSQLSERVER, clique com o botão direito do rato no mesmo e, em seguida, clique em Propriedades.
2. Na janela ***Propriedades***, clique no separador ***Iniciar Sessão***.
3. No separador ***Iniciar Sessão***, em Iniciar sessão como, clique em Esta conta, introduza *NT Authority\NetworkService* e clique em OK.

Para obter mais informações sobre segurança do SQL Server, visite o *site*:

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

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

- Se estiver a executar uma solução de E-business do Navision, como o Commerce Gateway, por exemplo, deverá certificar-se de que o Commerce Gateway Request Server foi instalado correctamente com a definição de conta predefinida para os serviços. A definição de conta predefinida é designada por *CGRSUser* e concede ao Commerce Gateway Server, acesso ao conjunto mínimo de outros serviços necessários, incluindo o serviço *MSSQLSERVER* e *BizTalk Service BizTalk Group : BizTalkServerApplication,* e não inclui quaisquer definições de conta global como acontece com a conta do *Sistema Local*.
- Utilize sempre palavras-passe seguras. Para obter mais informações sobre palavras-passe seguras, consulte a secção Palavras-passe Seguras.
- Utilize os Logins Windows (inícios de sessão do Windows). O Navision permite-lhe criar dois tipos de início de sessão: Logins Base Dados e Logins Windows. Recomendamos a utilização dos Logins Windows, uma vez que os mesmos incluem a Autenticação Windows proporcionando, assim, o cumprimento da política de palavras-passe correcta.
- As palavras-passe não devem ser reutilizadas. É geralmente considerada prática comum, a reutilização de palavras-passe em sistemas e domínios. Por exemplo, um administrador responsável por dois domínios poderá criar contas de Administrador de Domínio para cada um deles, utilizar a mesma palavra-passe e até mesmo definir palavras-passe de administrador local em computadores de domínio que sejam idênticas em todo o domínio. Neste caso, se uma conta ou computador estiver comprometido, esse comprometimento poderá ser generalizado para todo o domínio.
- Após a instalação do Navision e a criação ou actualização das bases de dados, deverá criar um Login Windows e atribuir-lhe a função SUPER no Navision. Este super-utilizador irá gerir a administração, segurança, etc. da base de dados. Atribua uma palavra-passe segura a este *login*. A palavra-passe deverá ser mantida confidencial. Deverá ter a mesma protecção que a palavra-passe do administrador do sistema de SQL Server. O acesso à base de dados é gerido pela função SUPER e requer o nível mais elevado de protecção. A palavra-passe de super-utilizador deve ser divulgada apenas aos Administradores do Sistema.
- Todos os outros utilizadores que tenham acesso à base de dados do Navision devem ter as respectivas contas configuradas com privilégios mínimos. Ou seja, devem-lhes ser atribuídas apenas funções no Navision que permitam o acesso às funcionalidades necessárias para a realização das suas tarefas na empresa.
- Certifique-se de que somente os utilizadores cuja função empresarial assim o exija, conseguem importar ficheiros FOB, redesenhar objectos, bem como criar e restaurar cópias de segurança da base de dados.

- Crie regularmente cópias de segurança da base de dados do Navision e teste-as de forma a garantir que as mesmas podem ser restauradas com sucesso.
- Guarde as cópias de segurança num local seguro para limitar o impacto de perigos como incêndios, fumo, pó, temperaturas elevadas, trovoada e catástrofes naturais (por exemplo, um terramoto).
- Embora o Navision possa ser executado em várias versões do Windows, é recomendada a utilização de sistemas operativos recentes, equipados com funcionalidades de segurança actualizadas. Actualmente, estes requisitos são preenchidos pelo Windows XP, o Service Pack 2 e o Windows Server 2003.
- Utilize o serviço Windows Update fornecido com o Windows 2000, Windows XP e Windows Server 2003 para aplicar as mais recentes actualizações de segurança. Utilize a funcionalidade de Actualização Automática do Windows para manter os computadores do seu cliente actualizados com os mais recentes *patches* de segurança, *service pack*s e actualizações.
- Recomendamos a utilização do protocolo de segurança TCPS na comunicação estabelecida entre os clientes do Navision e o Navision Database Server. TCPS consiste numa versão segura do TCP/IP que utiliza a Interface do Fornecedor de Suporte de Segurança (SSPI) com encriptação activada e autenticação Kerberos. O TCPS é o protocolo predefinido para o Navision Database Server.
- O cliente deverá ter um plano de recuperação de desastre que garanta uma rápida prossecução dos serviços após a ocorrência de um desastre. Um plano de recuperação deve contemplar:
  - A aquisição de equipamento novo/provisório.
  - O restauro das cópias de segurança nos novos sistemas.
  - A realização de testes para garantir que o plano de recuperação, na realidade, funciona.

Segurança Física

A segurança física é inquestionavelmente imperativa, uma vez que não existe uma forma de a complementar com a segurança de software. Por exemplo, se uma unidade de disco rígido for roubada, possivelmente os dados armazenados nessa unidade serão perdidos. Discuta as seguintes questões de segurança física durante o desenvolvimento de uma política com o seu cliente:

- Para instalações em grandes proporções com departamentos dedicados de IT, certifique-se de que as salas de servidores e locais de armazenamento de software se encontram fechados à chave.
- As máquinas nesta categoria englobam:
  - O servidor do Microsoft SQL Server 2000
  - O Servidor de Ficheiros onde residem ficheiros executáveis do Navision.
- Mantenha os utilizadores não autorizados afastados dos computadores.
- Certifique-se de que são instalados sistema de alarme anti-roubo, independentemente da sensibilidade dos dados.
- Garanta que as cópias de segurança de dados críticos são armazenadas fora das instalações e que as cópias de segurança são guardadas em cofres à prova de fogo.

Os Empregados

Os direitos administrativos de produtos e funcionalidades devem ser limitados. Por predefinição, os clientes devem atribuir aos seus empregados, apenas acesso de leitura às funções do sistema, a menos que os mesmos necessitem de um acesso superior para a realização das suas tarefas. A Microsoft sugere o seguinte princípio do menor privilégio: conceder aos utilizadores apenas os privilégios mínimos de acesso a dados e funcionalidades.
Ex-funcionários e empregados insatisfeitos constituem uma ameaça para segurança de rede. Quando discutir as questões de segurança com os seus clientes, sugira a seguinte política em relação aos empregados:

- Realizar investigações de antecedentes antes de contratar empregados.
- Prever "represálias" por parte de ex-funcionários e empregados insatisfeitos.
- Certificar-se de que todas as contas e palavras-passe do Windows relativas a um empregado são desactivadas, caso o mesmo saia da empresa. Não apagar utilizadores, por motivos de elaboração de relatórios. Não reutilizar as contas.
- Formar os utilizadores para estarem alerta e comunicarem actividades suspeitas.
- Não conceder privilégios automaticamente. Se os utilizadores não necessitarem de aceder a determinados computadores, salas de computadores ou conjuntos de ficheiros, certificar-se de que não lhes é atribuído esse acesso.
- Formar supervisores de forma a identificarem e reagirem a problemas potenciais dos empregados.
- Certificar-se de que os empregados compreendem as respectivas funções de preservação da segurança de rede.
- Dar uma cópia das políticas da empresa a todos os empregados.
- Não permitir que os utilizadores instalem software não autorizado pela entidade empregadora.

O Administrador

Recomendamos que os administradores de sistema dos seus clientes acompanhem as mais recentes correcções de segurança disponíveis da Microsoft. Os atacantes são peritos na combinação de pequenos erros para permitir intrusões em grande escala numa rede. Os administradores devem, em primeiro lugar, garantir que cada computador individual comporta os mais elevados padrões de segurança e, em seguida, adicionar actualizações de segurança e utilizar software antivírus. Neste guia são fornecidos vários recursos e ligações que o ajudam a encontrar informações preciosas e procedimentos recomendados.

A complexidade constitui outro compromisso na segurança da rede. Quanto mais complexa for a rede, mais difícil se torna a respectiva protecção ou correcção após um intruso ter conseguido obter acesso. O administrador deve documentar minuciosamente a topologia de rede, com o objectivo de a manter o mais simples possível.

A segurança é abordada, em primeiro lugar, na perspectiva da gestão de risco. Dado que a tecnologia individualmente não constitui uma protecção sólida, a segurança requer uma combinação de tecnologia e política. Ou seja, nunca irá existir um produto cuja instalação na rede, forneça instantaneamente uma segurança perfeita. A segurança é o resultado da conjunção de tecnologia e política. É através do modo de utilização da tecnologia que se determina o nível de segurança de uma rede. A Microsoft fornece tecnologia e funcionalidades com base na perspectiva da segurança, mas apenas o administrador, com a sua orientação, pode determinar as políticas adequadas para cada organização. Certifique-se de que a segurança é planeada antecipadamente no processo de implementação e utilização. Identifique com clareza o que o seu cliente pretende proteger e até que ponto está disposto a efectuar essa protecção.

Por fim, desenvolva planos de contingência para situações de emergência antes da ocorrência das mesmas. Um planeamento rigoroso associado a tecnologia de ponta irá proporcionar elevados padrões de segurança ao seu cliente.

Para obter mais informações gerais sobre segurança, consulte "The Ten Immutable Laws of Security Administration," em:
http://www.microsoft.com/technet/archive/community/columns/security/essays/10salaws.mspx.

e os artigos sobre gestão de segurança em:
http://www.microsoft.com/technet/community/columns/secmgmt/smarch.mspx

Proteger o Sistema Operativo do Servidor

Embora possam existir casos de pequenas empresas que não possuam um sistema operativo de servidor, é importante que compreenda e consiga comunicar os procedimentos recomendados de segurança a grandes empresas com ambientes de rede mais complexos. Deve também ter consciência de que muitos dos procedimentos e políticas descritos neste documento podem ser facilmente aplicados a essas empresas que possuem apenas sistemas operativos de cliente.

Os conceitos apresentados nesta secção aplicam-se aos produtos do Microsoft Windows 2000 Server e do Microsoft Windows Server 2003, embora a maioria destas informações tenha sido extraída da Ajuda Online do Windows Server 2003. O Windows Server 2003 fornece um robusto conjunto de funcionalidades de segurança. A Ajuda Online do Windows Server 2003 contém informações completas sobre todos os procedimentos e funcionalidades de segurança.

Para obter informações adicionais sobre o Windows 2000 Server, visite o Windows 2000 Server Security Center, em
http://www.microsoft.com/technet/security/prodtech/win2000/default.mspx.

e leia o Windows 2000 Security Hardening Guide em:
http://www.microsoft.com/technet/security/prodtech/win2000/win2khg/default.mspx

Para obter informações adicionais sobre o Windows Server 2003, consulte o *Windows Server 2003 Security Guide*, em
http://www.microsoft.com/technet/security/prodtech/win2003/w2003hg/sgch00.mspx

As funcionalidades principais do modelo de segurança do servidor Windows consistem na autenticação, controlo de acesso e início de sessão único:

- A autenticação é o processo utilizado pelo sistema para validar a identidade de um utilizador através das respectivas credenciais de início de sessão. O nome e a palavra-passe de um utilizador são identificados numa lista de utilizadores autorizados. Se o sistema detectar uma correspondência, é-lhe concedida autorização de acesso de acordo com as especificações na lista de permissões para esse utilizador.
- O controlo de acesso limita o acesso a informações ou recursos informáticos com base na identidade do utilizador e na respectiva associação a vários grupos predefinidos. O controlo de acesso é normalmente utilizado pelos administradores de sistema para controlar o acesso dos utilizadores a recursos de rede, como servidores, directórios e ficheiros. A implementação desta funcionalidade é normalmente efectuada através da concessão, a utilizadores e grupos, de permissões de acesso a objectos específicos.
- O início de sessão único permite a um utilizador iniciar uma sessão no domínio Windows, utilizando uma única palavra-passe e ser autenticado em qualquer computador no domínio. O início de sessão único permite aos administradores implementar a autenticação de palavras-passe em toda a rede Windows, proporcionando aos utilizadores, facilidade de acesso.

As seguintes secções contêm descrições mais detalhadas destas três funcionalidades chave.

Autenticação

A autenticação constitui uma parte fundamental da segurança do sistema e é utilizada para confirmar a identidade de qualquer utilizador que tente iniciar sessão num domínio ou aceder a recursos de rede. O elemento mais falível na maioria dos sistemas de autenticação é a palavra-passe do utilizador.

As palavras-passe constituem a primeira linha de defesa contra o acesso não autorizado ao domínio e aos computadores locais. Recomende os seguintes procedimentos relativamente à utilização de palavras-passe:

- Utilizar sempre palavras-passe seguras.
- Se as palavras-passe tiverem de ser anotadas num papel, o mesmo deverá ser guardado num local seguro e destruído quando já não for necessário.
- Nunca divulgar palavras-passe.
- Utilizar palavras-passe diferentes para todas as contas de utilizador.
- Alterar periodicamente as palavras-passe.
- Ser cuidadoso relativamente ao local onde as palavras-passe são guardadas nos computadores.

Palavras-passe Seguras

A função das palavras-passe na protecção da rede de uma organização é frequentemente subestimada e ignorada. Tal como foi mencionado anteriormente, as palavras-passe constituem a primeira linha de defesa contra o acesso não autorizado à rede. Deve, portanto, certificar-se de que os seus clientes instruem os empregados no sentido de utilizarem palavras-passe seguras.

No entanto, as ferramentas de descodificação de palavras-passe estão em constante aperfeiçoamento e os computadores utilizados para esse fim são cada vez mais eficazes. Após o período de tempo necessário, a ferramenta de descodificação de palavras-passe consegue descodificar qualquer palavra-passe. No entanto, as palavras-passe seguras são muito mais difíceis de descodificar que as palavras-passe simples.

Para consultar directrizes de criação de palavras-passe seguras de fácil memorização, visite

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

e

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

Definir a Política de Palavras-passe

Quando auxiliar o seu cliente na definição da política de palavras-passe, certifique-se de que a mesma exige que todas as contas de utilizadores tenham palavras-passe seguras. Na maioria dos sistemas, o seguimento das recomendações no Windows Server 2003 Security Guide é suficiente:

- Configure a definição da política **Aplicar histórico de palavras-passe** para que várias palavras-passe anteriores sejam memorizadas. Com esta definição da política, quando a palavra-passe expirar, os utilizadores ficam impedidos de a utilizar novamente.

  Definição recomendada: 24

- Configure a definição da política **Duração máxima da palavra-passe** para que as palavras-passe expirem com a frequência necessária no ambiente do cliente.

  Definição recomendada: entre 42 (predefinido) e 90.

- Configure a definição da política **Duração mínima da palavra-passe** para que as palavras-passe não possam ser alteradas até que atinjam um determinado período de dias. Esta definição da política funciona em conjunto com a definição da política **Aplicar histórico de palavras-passe**. Se for definida uma duração mínima da palavra-passe, os utilizadores ficam impedidos de alterar repetidamente as respectivas palavras-passe de forma a contornar a definição da política **Aplicar histórico de palavras-passe** e, em seguida, utilizar as palavras-passe originais. Os utilizadores têm de aguardar durante o número de dias especificado para alterar as palavras-passe.

  Definição recomendada: 2.

- Configure a definição da política **Tamanho mínimo da palavra-passe** para que as palavras-passe sejam compostas por um número mínimo especificado de caracteres. As palavras-passe extensas, com sete ou mais caracteres, são geralmente mais seguras do que as palavras-passe curtas. Com esta definição da política, os utilizadores ficam impedidos de utilizar palavras-passe em branco e têm de as criar com um determinado número mínimo de caracteres.

  Definição recomendada: 8.

- Active a definição da política **A palavra-passe tem de satisfazer requisitos de complexidade**. Esta definição da política verifica todas as novas palavras-passe para garantir que as mesmas satisfazem os requisitos básicos de palavras-passe seguras. Esta definição serve para garantir que as palavras-passe contêm, pelo menos, três símbolos das quatro categorias (maiúsculas, minúsculas, números e símbolos não alfanuméricos) e que não contêm qualquer parte do nome do utilizador, incluindo o nome próprio e o apelido.

  Nota
  As palavras-passe que satisfaçam estes requisitos não são necessariamente consideradas muito seguras. Por exemplo, a palavra-passe “Senha1” preenche estes requisitos.

  Definição recomendada: Sim

- Para obter uma lista completa destes requisitos, consulte "A palavra-passe tem de satisfazer requisitos de complexidade" na Ajuda Online do Windows Server.

- Armazenar palavras-passe utilizando a encriptação reversível – A encriptação reversível é utilizada nos sistemas em que uma aplicação necessita de aceder a palavras-passe de texto simples. Não é necessário na maioria das implementações.

  Definição recomendada: Não.

Para obter mais informações, consulte o Windows Server 2003 Security Guide:

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

Definir uma Política de Bloqueio de Conta

Seja prudente na definição de uma política de bloqueio de conta. A política de bloqueio de conta nunca deve ser definida numa pequena empresa, uma vez que existem fortes possibilidades de bloquear utilizadores autorizados e tal situação poderá ser bastante dispendiosa para o seu cliente.

Se o cliente decidir aplicar a política de bloqueio de conta, configure a definição da **Política de limite de bloqueio de conta** com um número suficientemente elevado, que permita que as contas dos utilizadores autorizados não sejam bloqueadas apenas porque os mesmos escreveram várias vezes a palavra-passe incorrectamente.

Para obter mais informações sobre a política de bloqueio de conta, consulte "Account Lockout Policy Overview" na Ajuda Online do Windows Server.

Para obter informações sobre o modo de aplicação ou modificação da política de bloqueio de conta, consulte "To Apply or Modify Account Lockout Policy" na Ajuda Online do Windows Server.

Controlo de Acesso

Uma rede Windows e os respectivos recursos (incluindo o Navision) podem ser protegidos ponderando os direitos que os utilizadores, grupos de utilizadores e outros computadores possuem na rede. Pode proteger um computador ou vários computadores, concedendo direitos de utilizador específicos a utilizadores ou grupos. Pode proteger um objecto, por exemplo, um ficheiro ou uma pasta, atribuindo permissões que autorizem os utilizadores ou grupos a efectuar acções específicas nesse objecto. Os conceitos chave que constituem o controlo de acesso incluem:

- Permissões
- Propriedade de objectos
- Herança de permissões
- Direitos de utilizadores
- Auditoria de objectos

Permissões

As permissões definem o tipo de acesso a um objecto ou a uma propriedade de objecto, como ficheiros, pastas e objectos de registo, concedido a um utilizador ou grupo. As permissões são aplicadas a quaisquer objectos protegidos, como ficheiros ou objectos de registo. As permissões podem ser concedidas a qualquer utilizador, grupo ou computador. A atribuição de permissões a grupos é um bom procedimento.

Propriedade de Objectos

Quando um objecto é criado, é-lhe atribuído um proprietário. Por predefinição, no Windows 2000 Server, o proprietário é considerado o criador do objecto. Esta predefinição foi alterada no Windows Server 2003 para objectos criados por membros do grupo Administradores.

Sempre que um membro do grupo Administradores cria um objecto no Windows Server 2003, o grupo Administradores torna-se o respectivo proprietário, em vez da conta individual que criou o objecto. Este comportamento pode ser alterado através do *snap-in* da Consola de Gestão da Microsoft (MMC) de Definições de Segurança Locais, utilizando a definição **Objectos de sistema: Proprietário predefinido para objectos criados por membros do grupo Administradores**. Independentemente das permissões definidas num objecto, o proprietário do objecto poderá sempre alterá-las.

Para obter mais informações, consulte "Propriedade" na Ajuda Online do Windows Server.

Herança de Permissões

A herança permite aos utilizadores, uma fácil atribuição e gestão de permissões. Esta funcionalidade permite que os objectos no interior de um contentor herdem automaticamente as permissões herdáveis desse contentor. Por exemplo, quando criar ficheiros numa pasta, os mesmos herdam as permissões da pasta. Só são herdadas as permissões marcadas para esse fim.

Direitos de Utilizadores

Os direitos de utilizadores concedem privilégios específicos e direitos de início de sessão a utilizadores e grupos no ambiente informático.

Para obter informações sobre direitos de utilizadores, consulte "Direitos de utilizador" na Ajuda Online do Windows Server.

Auditoria de Objectos

Pode auditar o acesso dos utilizadores a objectos. Em seguida, pode ver estes eventos relativos a segurança no registo de segurança, através do Visualizador de Eventos.

Para obter mais informações, consulte "Auditoria" na Ajuda Online do Windows Server.

Procedimentos Recomendados de Controlo de Acesso

- Atribuir permissões a grupos em vez de utilizadores. Uma vez que é ineficiente gerir contas de utilizadores directamente, a atribuição de permissões com base no utilizador deve ser a excepção.
- Utilizar Permissões negadas para certos casos especiais. Por exemplo, pode utilizar Permissões negadas para excluir o subconjunto de um grupo que tenha Permissões permitidas.
- Nunca recusar o acesso do grupo Todos a um objecto. Se recusar a permissão de todos os utilizadores para um objecto, essa acção irá também incluir os administradores. Uma solução mais adequada seria remover o grupo Todos, desde que atribua permissões a outros utilizadores, grupos ou computadores para esse objecto. Lembre-se de que se não forem definidas permissões, o acesso não será permitido.
- Atribuir permissões a um objecto numa posição elevada da árvore e, em seguida, aplicar a herança para propagar as definições de segurança por toda a árvore. Pode aplicar, de modo rápido e eficaz, definições de controlo de acesso a todos os subordinados ou a uma subárvore de um objecto principal. Através desta acção, conseguirá uma aplicação em grande escala, empregando um esforço mínimo. As definições de permissões que estabelecer devem ser adequadas à maioria dos utilizadores, grupos e computadores.

- As permissões explícitas podem, por vezes, substituir permissões herdadas. As Permissões negadas herdadas não impedem o acesso a um objecto se o mesmo tiver uma entrada de Permissão permitida explícita. As permissões explícitas têm prioridade sobre as permissões herdadas e até mesmo sobre as Permissões negadas herdadas.
- Para permissões de objectos do Active Directory®, certifique-se de que compreende os procedimentos recomendados específicos aos objectos do Active Directory.

Para obter mais informações, consulte "Best Practices for Assigning Permissions on Active Directory Objects" na Ajuda Online do Windows Server 2003.

Firewall de Segurança Externa

Um *firewall* consiste num elemento de *hardware* ou *software* que impede a entrada ou saída de pacotes de dados de uma rede específica. Para controlar o fluxo de tráfego, as portas no *firewall* encontram-se abertas ou fechadas para pacotes informativos. O *firewall* observa várias informações em cada pacote de dados: o protocolo através do qual o pacote está a ser entregue, o destino ou remetente do pacote, o tipo de conteúdo do pacote e o número da porta para a qual o envio está a ser efectuado. Se o *firewall* for configurado para aceitar o protocolo especificado através da porta de destino, a entrada do pacote é permitida. O Microsoft Windows Small Business Server 2003 Premium Edition efectua envios com o Microsoft Internet Security and Acceleration (ISA) Server 2000 como solução de firewall. O Small Business Server Standard Edition também inclui um firewall.

ISA Server 2004

O Internet Security and Acceleration (ISA) Server 2000 encaminha com segurança pedidos e respostas entre a Internet e os computadores do cliente na rede interna.

O ISA Server funciona como o *gateway* seguro de Internet para clientes na rede local. O computador do ISA Server é transparente para as outras entidades no caminho de comunicação. O utilizador da Internet não deverá conseguir distinguir se está presente um servidor de *firewall*, a menos que tente aceder a um serviço ou visitar um site a que o computador do ISA Server tenha negado o acesso. O servidor de Internet que está a ser acedido, interpreta os pedidos do computador do ISA Server como se os mesmos tivessem sido originados a partir da aplicação do cliente.

Quando opta pela filtragem de fragmentos do Protocolo Internet (IP), os serviços do Proxy Web e do Firewall são activados para filtrar fragmentos de pacotes. Através da filtragem de fragmentos de pacotes, todos os pacotes IP fragmentados são ignorados. Um dos "ataques" populares consiste no envio de pacotes fragmentados, seguido da remontagem dos mesmos, de forma a torná-los prejudiciais para o sistema.

O ISA Server inclui um mecanismo de detecção de intrusões que identifica a hora de uma tentativa de ataque a uma rede e efectua um conjunto de acções configuradas (ou alertas) no caso de ocorrência de um ataque.

Se os Serviços de Informação Internet (IIS) estiverem instalados no computador do ISA Server, terá de os configurar de modo a não utilizarem as portas que o ISA Server utiliza para pedidos Web enviados (por predefinição, 8080) e para pedidos Web recebidos (por predefinição, 80). Por exemplo, pode alterar os IIS para monitorizarem a porta 81 e, em seguida, configurar o computador do ISA Server para direccionar os pedidos Web recebidos para a porta 81 no computador local com os IIS em execução.

Se existir um conflito entre as portas que o ISA Server e os IIS utilizam, o programa de configuração interrompe o serviço de publicação dos IIS. Em seguida, poderá alterar os IIS para monitorizarem uma porta diferente e reiniciar o respectivo serviço de publicação.

Políticas do ISA Server

Pode definir uma política no ISA Server que determine o acesso de entrada e de saída. As regras de *sites* e de conteúdo especificam os *sites* e o conteúdo a que é possível aceder. As regras de protocolos indicam se um determinado protocolo está acessível para comunicações de entrada e de saída.

Pode criar regras de *sites* e de conteúdo, regras de protocolos, regras de publicação na Web e filtros de pacotes IP. Estas políticas determinam o modo como os clientes do ISA Server comunicam com a Internet e o tipo de comunicação permitida.

Protecção de Vírus

Um vírus informático consiste num ficheiro executável concebido para se replicar e apagar ou danificar ficheiros de dados ou programas, evitando a sua detecção. Na realidade, os vírus são frequentemente corrigidos e ajustados de forma a ser impossível detectá-los. Os vírus são normalmente enviados como anexos de correio electrónico. Os programas antivírus têm de ser constantemente actualizados para procurarem vírus novos e modificados. Os vírus constituem o método principal de vandalismo informático.

O software antivírus é especificamente concebido para detecção e prevenção de programas de vírus. Dado que existe uma constante criação de novos programas de vírus, vários fabricantes de produtos antivírus disponibilizam actualizações periódicas do *software* aos clientes. A Microsoft recomenda a implementação de software antivírus no ambiente do seu cliente.

O software antivírus é normalmente instalado em cada um destes três locais: estações de trabalho de utilizadores, servidores e na rede onde é efectuada a recepção de correio electrónico (e o envio, em alguns casos) para a organização.

Tipos de Vírus

Existem três tipos principais de vírus que infectam os sistemas informáticos: vírus do sector de arranque, vírus de programa e programas "Cavalo de Tróia".

Vírus do Sector de Arranque

Quando o computador é ligado, o vírus pesquisa o sector de arranque do disco rígido antes do sistema operativo ou outros ficheiros de arranque serem carregados. Os vírus do sector de arranque são concebidos para substituir as informações nos sectores de arranque do disco rígido pelo seu próprio código. Quando um computador é infectado por um vírus do sector de arranque, o código do vírus é o primeiro elemento a ser lido pela memória. Depois do vírus se infiltrar na memória, é replicado para outros discos em utilização no computador infectado.

Vírus de Programa

O vírus de programa é o tipo de vírus mais vulgar. Instala-se no ficheiro executável de um programa, adicionando o seu próprio código ao ficheiro executável. O código do vírus é normalmente adicionado de forma a ser imune à detecção. Quando o ficheiro infectado é executado, permite que o vírus se instale em outros ficheiros executáveis. Os ficheiros infectados por este tipo de vírus têm geralmente as extensões de nome de ficheiro .com, .exe ou .sys.

Alguns vírus de programa são concebidos para programas específicos. Os tipos de programas alvo consistem regularmente em ficheiros de sobreposição (.ovl) e em ficheiros de biblioteca de ligações dinâmicas (.dll). Embora estes ficheiros não sejam executados, são utilizados pelos ficheiros executáveis. O vírus é transmitido durante essa utilização.

A danificação de dados ocorre quando o vírus é despoletado. Um vírus pode ser despoletado ao executar um ficheiro infectado ou quando existe uma determinada definição no ambiente (como uma data de sistema específica).

Programas "Cavalo de Tróia"

Um programa "cavalo de Tróia" não consiste realmente num vírus. O ponto fulcral que distingue um vírus de um programa "cavalo de Tróia" assenta no facto do programa não se replicar, destruindo apenas informações no disco rígido. Um programa "cavalo de Tróia" simula um programa legítimo, como um jogo ou utilitário, mas ao ser executado, destrói ou codifica os dados.

Procedimentos Recomendados de Protecção de Vírus

A propagação de um vírus em forma de macro pode ser evitada. Eis algumas sugestões que deve partilhar com os seus clientes de forma a impedir eventuais infecções:

- Instalar uma solução de protecção de vírus que verifique a existência de vírus em mensagens recebidas da Internet antes que as mesmas passem para o *router*. Isto irá garantir que é verificada a existência de vírus conhecidos nas mensagens de correio electrónico.
- Saber a origem dos documentos que são recebidos. Os documentos não deverão ser abertos, a menos que o respectivo remetente seja considerado fidedigno.
- Falar com a pessoa que criou o documento. Se os utilizadores tiverem dúvidas relativamente à segurança do documento, devem contactar a pessoa que o criou.
- Utilizar a protecção contra vírus em forma de macro do Microsoft Office. No Office, as aplicações alertam o utilizador se um documento contiver macros. Esta funcionalidade permite ao utilizador, activar ou desactivar as macros durante a abertura do documento.
- Utilizar software antivírus para detectar e remover vírus de macro. O software antivírus detecta e geralmente remove os vírus de macro dos documentos. A Microsoft recomenda a utilização de programas de software antivírus certificados pela International Computer Security Association (ICSA).

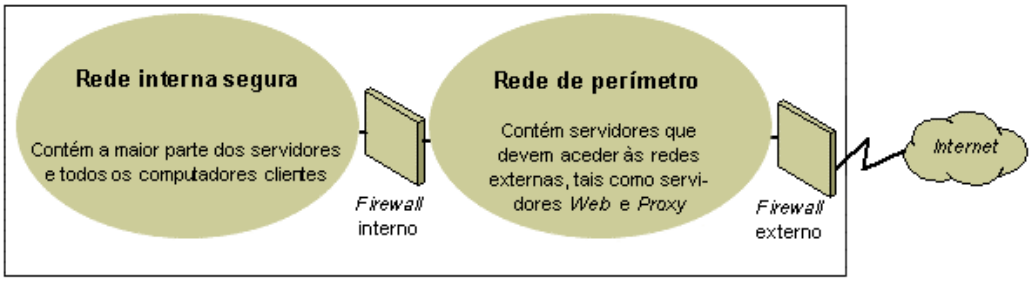
Para obter mais informações sobre vírus e segurança em geral, visite os seguintes Web *sites* da Microsoft Security:

- Microsoft Security em http://www.microsoft.com/security/default.asp.
- Documentação sobre segurança na Microsoft TechNet http://www.microsoft.com/technet/security/Default.mspx.

Estratégias de Segurança de Redes

Dado que a concepção e implementação de um ambiente inter-redes IP requer um equilíbrio das características da rede pública e privada, o *firewall* tornou-se um elemento de extrema importância na protecção da integridade de redes. Um *firewall* não consiste num único componente. A National Computer Security Association (NCSA) define um *firewall* como "um sistema ou combinação de sistemas que impõe um limite entre duas ou mais redes." Embora sejam utilizados vários termos, esse limite é geralmente conhecido como rede de perímetro. A rede de perímetro protege a intranet ou a rede local (LAN) da empresa contra intrusões, controlando o acesso a partir da Internet ou de outras redes de grandes proporções.

O seguinte diagrama mostra uma rede de perímetro limitada por *firewalls* e colocada entre uma rede privada e a Internet no intuito de proteger a rede privada:



Rede de Perímetro Básica

As organizações diferem na abordagem à utilização de *firewalls* para fornecer segurança. A filtragem de pacotes IP oferece condições mínimas de segurança, é difícil de gerir e fácil de subjugar. Os *gateways* de aplicações são mais seguros que os filtros de pacotes e mais fáceis de gerir devido ao facto de estarem relacionados apenas com algumas aplicações específicas, como, por exemplo, um sistema de correio electrónico particular. Os *gateways* de circuitos são mais eficazes para situações em que o utilizador de uma aplicação de rede seja motivo de maior preocupação do que os dados transmitidos por essa aplicação. O servidor proxy consiste numa ferramenta completa de segurança que inclui um gateway de aplicação, acesso seguro para utilizadores anónimos e outros serviços. Eis algumas informações sobre estas diferentes opções:

- **Filtragem de Pacotes IP**
  A filtragem de pacotes IP constituiu a primeira implementação da tecnologia de *firewall*. Os cabeçalhos de pacotes são examinados de forma a verificar os endereços de origem e de destino, o Protocolo de Controlo de Transmissão (TCP), os números das portas do Protocolo de Datagrama de Utilizador (UDP) e outras informações. A filtragem de pacotes é uma tecnologia limitada que apresenta um óptimo funcionamento em ambientes de segurança simples onde, por exemplo, todos os elementos exteriores à rede de perímetro não são considerados fidedignos. Recentemente, vários fabricantes aperfeiçoaram o método de filtragem de pacotes, adicionando-lhe funcionalidades inteligentes de tomada de decisões que permitiram a criação de uma nova forma de filtragem de pacotes, intitulada de *stateful protocol inspection*. Pode configurar a filtragem de pacotes para aceitar tipos de pacotes específicos e recusar todos os outros ou para recusar tipos de pacotes específicos e aceitar todos os outros.
- ***Gateways* de Aplicações**
  Os *gateways* de aplicações são utilizados sempre que o conteúdo actual de uma aplicação constitua um motivo de preocupação. O facto de serem específicos a determinadas aplicações representa uma vantagem e uma limitação, uma vez que não comportam uma capacidade de adaptação fácil às alterações na tecnologia.

- ***Gateways* de Circuitos**
  Os *gateways* de circuitos são caracterizados como túneis construídos no *firewall* que estabelecem uma ligação entre sistemas ou processos específicos. A utilização mais adequada dos *gateways* de circuitos é para situações em que o utilizador de uma aplicação constitua potencialmente um risco mais elevado do que as informações processadas pela aplicação. O *gateway* de circuitos distingue-se de um filtro de pacotes pela sua capacidade de estabelecer uma ligação a um esquema de aplicação fora-de-banda que permite obter informações adicionais.
- **Servidores Proxy**
  Os servidores proxy são ferramentas completas de segurança, que incluem a funcionalidade de *firewall* e de *gateway* de aplicação para gestão do tráfego entre a Internet e a rede local. Os servidores proxy também permitem a colocação de documentos em *cache* e o controlo de acesso. Um servidor proxy pode melhorar o desempenho através da colocação em *cache* e do fornecimento directo de dados solicitados com frequência, como uma página da Web popular. Tem também a capacidade de filtrar e rejeitar pedidos que o proprietário não considere adequados, como pedidos de acesso não autorizado a ficheiros proprietários.

Certifique-se de que o cliente tira partido dessas funcionalidades de segurança do *firewall* que representam uma ajuda significante. Coloque uma rede de perímetro num ponto da topologia de rede para que todo o tráfego de entrada na rede empresarial tenha que passar pelo perímetro controlado pelo *firewall* externo. Pode ajustar o controlo de acesso do *firewall* de forma a corresponder às necessidades do cliente e configurar os *firewalls* para comunicarem todas as tentativas de acesso não autorizado.

Para minimizar o número portas que é necessário abrir no *firewall* interno, pode utilizar um *firewall* de camada de aplicação, como o ISA Server 2000.

Para obter mais informações gerais sobre TCP/IP, consulte "Designing a TCP/IP Network" em http://www.microsoft.com/resources/documentation/WindowsServ/2003/all/deployguide/en-us/dnsbb_tcp_overview.asp.

Redes Sem Fios

Por predefinição, as redes sem fios são normalmente configuradas de forma a permitir a visualização de dados confidenciais transmitidos. Podem ser vulneráveis a um acesso externo prejudicial devido às configurações predefinidas de alguns componentes de hardware sem fios, à acessibilidade que as mesmas proporcionam e aos métodos actuais de encriptação. Existem ferramentas e opções de configuração que podem proteger contra a visualização de dados confidenciais, mas tenha em mente que as mesmas não servem para proteger os computadores contra piratas informáticos e vírus transmitidos através da ligação à Internet. Desta forma, é extremamente importante que inclua um *firewall* para protecção dos computadores contra intrusos indesejados na Internet.

Para obter mais informações sobre a protecção de uma rede sem fios, consulte "How to Make Your 802.11b Wireless Home Network More Secure" em http://support.microsoft.com/default.aspx?scid=kb;en-us;309369.

Cenários de Segurança de Redes

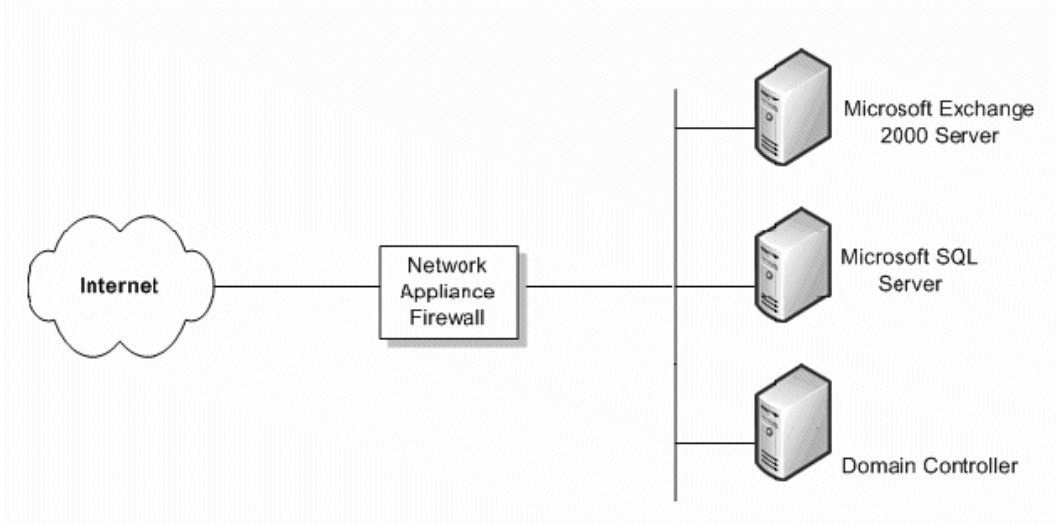
O nível de segurança de rede que a organização do cliente necessita depende de vários factores. Normalmente, resume-se a um compromisso entre o orçamento e a necessidade manter os dados empresariais seguros. É possível que uma pequena empresa tenha uma estrutura de segurança bastante complexa que forneça o mais alto nível de segurança de rede, porém, uma pequena empresa poderá não conseguir disponibilizar os recursos financeiros necessários para esse nível de segurança. Nesta secção, são observados quatro cenários e dadas recomendações, para cada um deles, que fornecem vários níveis de segurança.

Sem *Firewall*

Se o cliente tiver uma ligação à Internet, mas não tiver um *firewall*, existe a necessidade de implementar uma medida de segurança de rede. Existem aplicações simples de *firewall* de redes que fornecem uma segurança suficiente para desencorajar a maioria dos pretensos piratas informáticos.

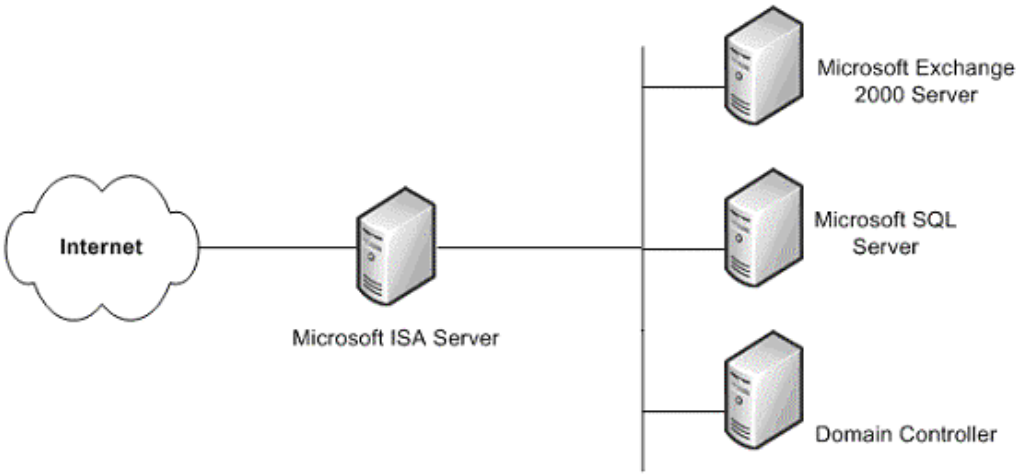
Um *Firewall* Simples

O nível mínimo recomendado de segurança consiste num único *firewall* entre a Internet e os dados do seu cliente. Este *firewall* poderá não fornecer um nível avançado de segurança e não deverá ser considerado muito seguro. Mas é melhor que nada.



***Firewall* Simples**

Com alguma sorte, o orçamento do cliente permitirá uma solução mais segura que proteja os dados empresariais. Essa solução é o ISA Server. O custo acrescido deste servidor adicional fornece muito mais segurança do que os *firewalls* vulgares, dado que fornecem apenas tradução de endereços de rede (NAT) e filtragem de pacotes.



***Firewall* do ISA Server**

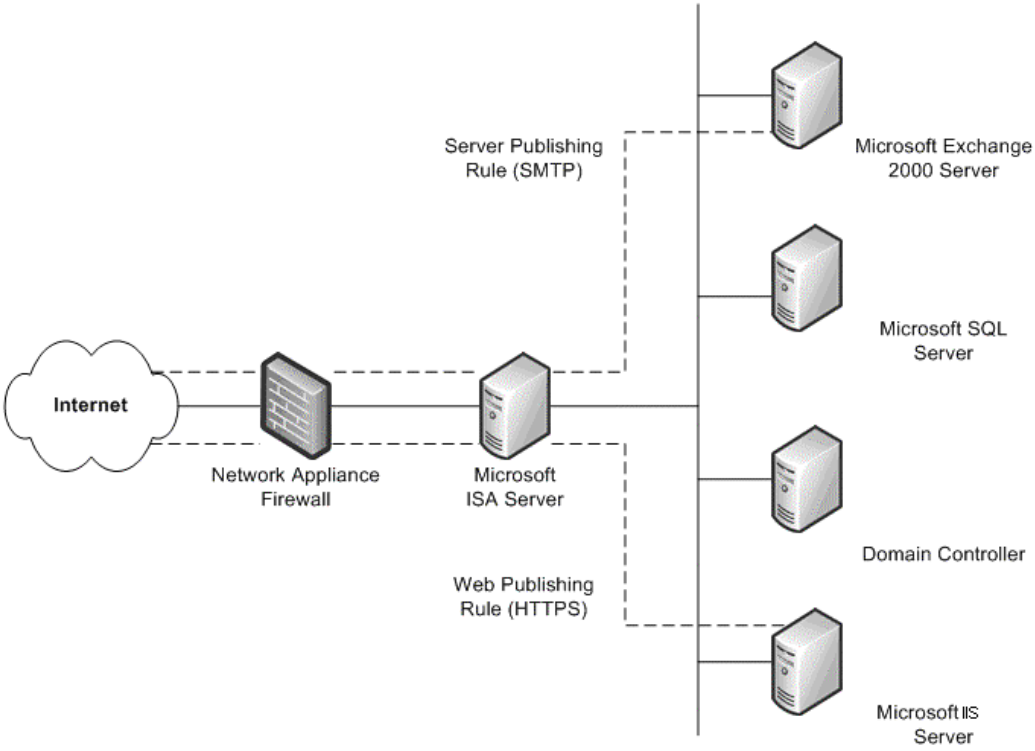
Esta solução de *firewall* único é mais segura que uma aplicação básica de *firewall* e fornece serviços de segurança específicos do Windows.

Um *Firewall* Existente

Se o cliente tiver um *firewall* que separe a intranet da Internet, poderá considerar a aquisição de um *firewall* adicional que forneça várias formas de configurar os recursos internos à Internet.

Um método possível é a publicação na Web. Este método é efectuado implementando um ISA Server antes do servidor da Web que está a fornecer acesso aos utilizadores da Internet. Através dos pedidos Web recebidos, o ISA Server pode representar um servidor da Web para o mundo exterior, respondendo aos pedidos efectuados pelo cliente, de conteúdo da Web a partir da *cache*. O ISA Server só reencaminha pedidos para o servidor da Web quando os mesmos não podem ser respondidos a partir da *cache*.

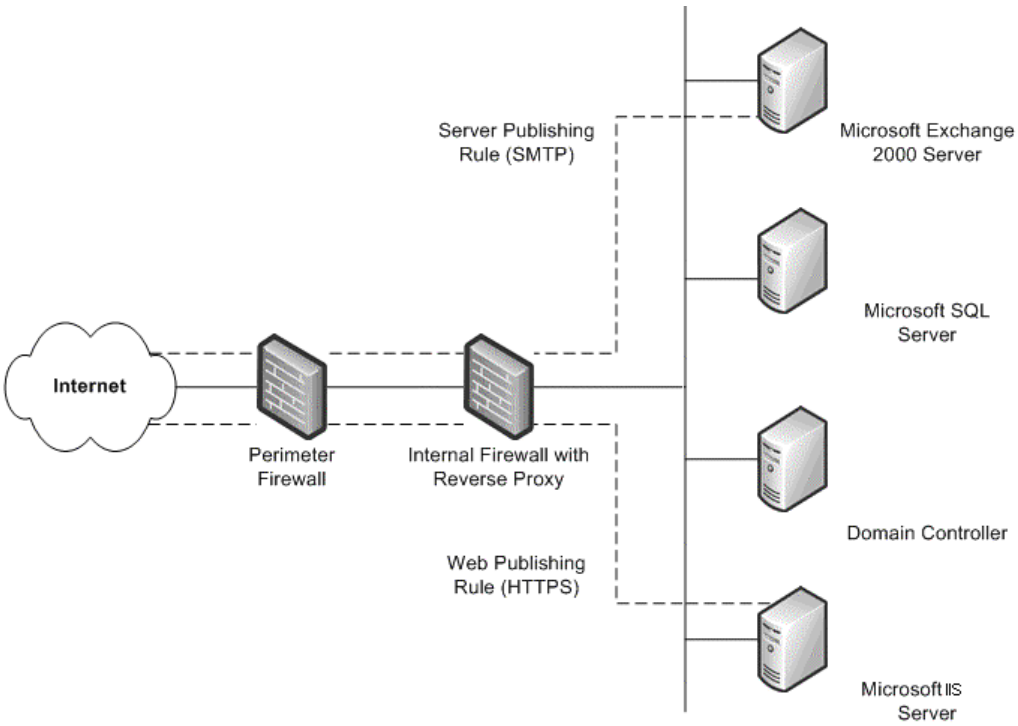
Outro método é a publicação no servidor. O ISA Server permite a publicação de servidores internos na Internet sem comprometer a segurança da rede interna. É possível configurar as regras de publicação na Web e de publicação no servidor que determinam os pedidos a enviar para um servidor na rede local, fornecendo uma camada adicionada de segurança para os servidores internos.



***Firewall* Existente com ISA Server**

Dois *Firewalls* Existentes

O quarto cenário é quando a organização tem dois *firewalls* instalados com uma rede de perímetro estabelecida (DMZ). Um ou mais destes servidores fornece serviços de proxy invertido para que os clientes da Internet não acedam directamente aos servidores na intranet. Em alternativa, um dos *firewalls*, de preferência o *firewall* interno, intercepta os pedidos da rede para os servidores internos, inspeccionando os pacotes e reencaminhando-os em nome do anfitrião da Internet.



Dois *Firewalls* Existentes

Este cenário fica semelhante ao anterior após a adição de um segundo *firewall*. A única diferença assenta no facto do *firewall* interno que suporta proxy invertido não ser um ISA Server. Neste cenário, deve trabalhar em conjunto com os gestores de cada *firewall* para definir as regras de publicação no servidor associadas à política de segurança.

Gestão de *Patches* de Segurança

Os sistemas operativos e aplicações são frequentemente bastante complexos. Podem consistir em milhões de linhas de códigos, escritas por vários programadores. É essencial que o *software* funcione fiavelmente e não comprometa a segurança do ambiente de IT. Para minimizar a ocorrência de problemas, os programas são rigorosamente testados antes de serem lançados no mercado. No entanto, os piratas informáticos empenham-se constantemente em encontrar pontos fracos no *software*, de tal forma que torna impossível a antecipação de todos os futuros ataques.

Para muitas organizações, a gestão de *patches* integra uma parte da estratégia de gestão de configurações e alterações globais. Todavia, independentemente da natureza e do tamanho da organização, é imperativo possuir uma boa estratégia de gestão de *patches*, mesmo que a gestão de configurações e alterações ainda não tenha sido aplicada efectivamente. A esmagadora maioria dos ataques bem sucedidos a sistemas informáticos ocorre em sistemas sem *patches* de segurança instalados.

Os *patches* de segurança apresentam um desafio específico para a maioria das organizações. Uma vez exposta uma fraqueza no *software*, ela é rapidamente divulgada pelos atacantes para toda a comunidade de piratas

informáticos. Quando ocorre uma fraqueza no seu *software*, a Microsoft empenha-se no lançamento de um *patch* de segurança com a maior brevidade possível. Até o *patch* ser implementado, a segurança poderá ficar severamente diminuída.

No ambiente do Navision, é necessário garantir que os seus clientes têm os mais recentes *patches* de segurança instalados em todo o sistema. Certifique-se de que o cliente utiliza uma das tecnologias disponibilizadas pela Microsoft. Estas incluem:

- **Microsoft Security Notification Service**
  O Security Notification Service consiste numa lista de endereços de correio electrónico para a qual são distribuídos avisos sempre que uma actualização estiver disponível. Estes avisos constituem um elemento precioso para uma estratégia dinâmica de segurança. Encontram-se também disponíveis no Web site TechNet Product Security Notification: http://www.microsoft.com/technet/security/bulletin/notify.mspx.
- **Actualizações Automáticas do Windows**
  O Windows pode aplicar automaticamente as actualizações de segurança nos computadores.
- **Microsoft Security Bulletin Search Tool**
  A ferramenta de pesquisa Security Bulletin está disponível no Web site Security Bulletin Service: http://www.microsoft.com/technet/security/current.aspx. O cliente pode determinar as actualizações necessárias com base no sistema operativo, aplicações e *service pack*s actualmente em execução.
- **Microsoft Baseline Security Analyzer (MBSA)**
  Esta ferramenta gráfica está disponível no Web site Microsoft Baseline Security Analyzer: http://www.microsoft.com/technet/security/tools/mbsahome.mspx. O funcionamento desta ferramenta consiste na comparação do estado actual de um computador com uma lista de actualizações gerida pela Microsoft. O MBSA também efectua algumas verificações básicas de segurança e definições de expiração de palavras-passe, de políticas de contas de convidados e de outras áreas. O MBSA irá também procurar vulnerabilidades nos Serviços de Informação Internet (IIS) da Microsoft, SQL Server™ 2000, Exchange 5.5, Exchange 2000 e Exchange Server 2003.
- **Serviços de Actualização de Software da Microsoft (SUS)**
  Conhecida anteriormente como Windows Update Corporate Edition, esta ferramenta permite que as empresas reúnam nos computadores locais todas as actualizações críticas e pacotes de segurança SRP (security rollup packages) disponíveis no site público do Windows Update. Esta ferramenta funciona com uma nova edição dos clientes de actualização automática (AU) no intuito de estabelecer a base para uma poderosa estratégia de instalações e transferências automáticas. O novo conjunto de clientes AU inclui um cliente para os sistemas operativos Windows 2000 e Windows Server 2003 e tem a capacidade de instalar automaticamente as actualizações transferidas. Para obter mais informações sobre os Serviços de Actualização de Software da Microsoft, consulte http://www.microsoft.com/windows2000/windowsupdate/sus/default.asp.
- **Microsoft Systems Management Server (SMS) Software Update Services Feature Pack**
  O SMS Software Update Services Feature Pack contém uma variedade de ferramentas destinadas a facilitar o processo de emissão de actualizações de software por toda a empresa. Inclui as ferramentas Security Update Inventory Tool, Microsoft Office Inventory Tool para Actualizações, Distribute Software Updates Wizard e uma SMS Web Reporting Tool com suplemento de Web Reports para Actualizações de Software. Para obter mais informações sobre cada ferramenta, consulte http://www.microsoft.com/smserver/downloads/20/featurepacks/suspack/.

Fale com os seus clientes sobre cada uma destas ferramentas e incentive a utilização das mesmas. É extremamente importante que as questões de segurança sejam abordadas com a maior brevidade possível, mantendo, no entanto, a estabilidade do ambiente.

Definições de Segurança do SQL Server 2000

Dado que o Navision também pode ser executado no SQL Server 2000, é importante que tome medidas para aumentar a segurança da instalação do SQL Server 2000 do cliente. Os seguintes passos irão ajudá-lo a aumentar a segurança do SQL Server:

- Certifique-se de que tem instalado o sistema operativo, actualizações e service packs do SQL Server 2000 mais recentes. Para obter os detalhes mais recentes, consulte o Web site Microsoft Security http://www.microsoft.com/security/default.asp.
- Para segurança de ficheiros ao nível do sistema, certifique-se de que todos os dados e ficheiros de sistema do SQL Server 2000 estão instalados nas partições NTFS. Deve tornar os ficheiros acessíveis apenas para utilizadores administrativos ou ao nível do sistema através da atribuição de permissões NTFS. Esta acção irá salvaguardar o acesso a esses ficheiros quando o serviço MSSQLSERVER não estiver em execução.
- Utilize uma conta de domínio com privilégios limitados, como a conta de Autoridade NT\ Serviço de Rede ou de LocalSystem (recomendado) para o serviço SQL Server 2000 (MSSQLSERVER). Esta conta deve ter direitos mínimos no domínio e ajuda a evitar (mas não a impedir) um ataque ao servidor. Ou seja, esta conta deve ter apenas permissões ao nível do utilizador local no domínio. Se o SQL Server 2000 estiver a utilizar uma conta de Administrador de Domínio para executar os serviços, uma exposição do servidor irá originar um comprometimento de todo o domínio. Utilize o Gestor de Empresas do SQL Server para alterar esta definição. As listas de controlo de acesso (ACLs) de ficheiros, do registo e de direitos de utilizadores serão alteradas automaticamente.
- A maioria das edições do SQL Server 2000 é instalada com duas bases de dados predefinidas, **Northwind** e **pubs**. Ambas consistem em bases de dados de demonstração que são utilizadas para testar, praticar e dar exemplos gerais. Não devem ser implementadas num sistema de produção. O conhecimento da existência destas bases de dados pode incentivar um atacante a tentar tirar partido das configurações predefinidas. Se a **Northwind** e **pubs** estiveram presentes no computador do SQL Server 2000 de produção, deverão ser removidas.
- A auditoria do sistema do SQL Server 2000 encontra-se desactivada por predefinição, o que implica que as condições não sejam auditadas. Isto dificulta a detecção de intrusões e ajuda os atacantes a encobrir o respectivo rasto. No mínimo, deve activar a auditoria de tentativas falhadas de inícios de sessão.

Para obter as mais actualizadas informações de segurança do SQL Server 2000, consulte http://www.microsoft.com/sql/techinfo/administration/2000/security/default.asp.

Acerca da Microsoft Business Solutions

A Microsoft Business Solutions, subsidiária da Microsoft, oferece uma vasta gama de aplicações empresariais concebidas para ajudar as empresas de pequena e média dimensão a estarem mais interligadas com clientes, colaboradores, parceiros e fornecedores. As aplicações da Microsoft Business Solutions optimizam os processos empresariais estratégicos nas áreas de gestão financeira, análise, gestão de recursos humanos, gestão de projectos, gestão de relações com clientes, gestão de serviços, gestão da cadeia de valor, e-commerce, gestão de produção e vendas. As aplicações são concebidas para fornecerem aos clientes, capacidades para atingirem o sucesso empresarial. Para obter mais informações sobre a Microsoft Business Solutions, visite o site http://www.microsoft.com/BusinessSolutions/