Microsoft Business Solutions

Navision Security Hardening Guide

Fecha de publicación: octubre de 2004

Microsoft

Contenido

Introducción

Microsoft® Windows® proporciona sofisticada seguridad de red basada en estándares. En el sentido más amplio, la seguridad incluye planeamiento y consideración de ventajas e inconvenientes. Por ejemplo, un equipo se puede encerrar en una cámara acorazada a la que sólo tiene acceso un administrador de sistemas. Puede que este equipo tenga la máxima seguridad, pero no es útil porque no está conectado a ningún otro equipo. Debe considerar cómo proporcionar seguridad a la red sin sacrificar la capacidad de uso.

La mayoría de las organizaciones se preparan para ataques externos y establecen barreras de seguridad, pero muchas empresas no tienen en cuenta cómo mitigar una infracción de seguridad cuando un usuario malintencionado consigue traspasar el servidor de seguridad. Las medidas de seguridad del entorno del cliente funcionarán correctamente si los usuarios no tienen que llevar a cabo muchos procedimientos y pasos para hacer su trabajo de manera segura. La implementación de directivas de seguridad debe ser lo más sencilla posible para los usuarios. De lo contrario, tenderán a buscar formas menos seguras de hacer las cosas.

Puesto que el tamaño de las instalaciones de Navision puede variar enormemente, es importante considerar detenidamente las necesidades de cada cliente y sopesar la eficacia de la seguridad con los costos en los que se puede incurrir. Como asesor de confianza del cliente, debe utilizar su mejor criterio y recomendar una directiva que cubra sus necesidades de seguridad sin crear una carga que acabe por causar que el cliente deje de aplicar la directiva.

Prácticas recomendadas de seguridad de Navision

Las siguientes reglas generales pueden ayudar a aumentar la seguridad del entorno de Navision:

- Si desea ejecutar Navision Database Server como un servicio o utilizar el parámetro de línea de comandos *installasservice* al iniciar el servidor, debe asegurarse de que el servicio se ejecuta como la cuenta NT Authority\Servicio de red. La cuenta NT Authority\Servicio de red sólo existe en Windows™ XP y Windows Server™ 2003. Si utiliza Windows 2000 Server, debe crear una cuenta con privilegios mínimos para el servicio; de lo contrario, se asignará al servicio una cuenta Sistema local. Como máximo, esta cuenta debe tener los mismos privilegios que la cuenta Usuarios normal o ser una cuenta de dominio que no sea un administrador del dominio ni de ningún equipo local.

  Debe recordar que tiene que otorgar a la cuenta NT Authority\Servicio de red, o la cuenta de usuario con la que se ejecuta el servidor, acceso de lectura y escritura a los archivos de base de datos para asegurar que los usuarios pueden conectar a la base de datos.

  Para conceder a la cuenta NT Authority\Servicio de red acceso de lectura y escritura a un archivo de base de datos en Windows XP:

  1. En el Explorador de Windows, vaya a la carpeta que contiene el archivo de base de datos.
  2. Seleccione el archivo, haga clic en él con el botón secundario del *mouse* (ratón) y haga clic en Propiedades.
  3. En la ventana ***Propiedades***, haga clic en la ficha ***Seguridad*** y, en el campo **Nombres de usuario y grupo**, haga clic en Agregar.
  4. En la ventana ***Seleccionar usuarios, equipos o grupos***, escriba *Servicio de red* y haga clic en Aceptar.
  5. SERVICIO DE RED se ha agregado al campo **Nombres de usuario y grupo** de la ventana ***Propiedades***.
  6. Seleccione SERVICIO DE RED y, en el campo **Permisos**, asígnele los permisos *Leer* y *Escribir*.
- El servicio Navision Application Server se ejecuta como la cuenta NT Authority\Servicio de red de forma predeterminada y esto le permite tener acceso al servidor de base de datos de Navision de forma local. Sin embargo, en una red debe asegurarse de que el servicio Navision Application Server se ejecuta como una cuenta de dominio de Windows reconocida por el servidor de base de datos de Navision si desea que tenga acceso al servidor de base de datos. Esta cuenta no debe ser un administrador del dominio ni de ningún equipo local.
- Si ejecuta la opción de SQL Server para Navision, Microsoft SQL Server™ se ejecuta como un servicio. La opción de SQL Server para Navision requiere que SQL Server pueda consultar Active Directory para obtener listas de los grupos de usuarios de Windows con fines de autenticación. Por lo tanto, debe asegurarse de que el servicio SQL Server se ejecuta como la cuenta NT Authority\Servicio de red.

  Para asegurarse de que el servicio se ejecuta como NT Authority\Servicio de red:

  1. En el equipo con SQL Server, busque el servicio MSSQLSERVER, haga clic en él con el botón secundario del *mouse* y, después, haga clic en Propiedades.
  2. En la ventana ***Propiedades***, haga clic en la ficha ***Iniciar sesión***.
  3. En la ficha ***Iniciar sesión***, en Iniciar sesión como, haga clic en Esta cuenta, escriba *NT Authority\ServicioRed* y, finalmente, haga clic en Aceptar.

Para obtener más información acerca de la seguridad de SQL Server, visite las siguientes direcciones:

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

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

- Si ejecuta un producto E-business de Navision como Commerce Gateway, debe asegurarse de que Commerce Gateway Request Server se ha instalado correctamente con la configuración de cuenta predeterminada para los servicios. La configuración de cuenta predeterminada se denomina *CGRSUser* y concede a Commerce Gateway Server acceso al conjunto mínimo de otros servicios que requiere, lo que incluye el servicio *MSSQLSERVER* y *BizTalk Service BizTalk Group : BizTalkServerApplication*, y no incluye configuración de cuenta global como en el caso de la cuenta *Sistema local*.
- Utilice siempre contraseñas seguras. Para obtener más información acerca de las contraseñas seguras, consulte la sección Cambie las contraseñas periódicamente.
- Utilice inicios de sesión de Windows. Navision le permite crear dos tipos de inicio de sesión: inicios de sesión de base de datos e inicios de sesión de Windows. Se recomienda utilizar los inicios de sesión de Windows porque utilizan la autenticación de Windows y le permiten aplicar una directiva de contraseñas correcta.
- Las contraseñas no se deben reutilizar. Es una práctica habitual reutilizar las contraseñas entre sistemas y dominios. Por ejemplo, un administrador encargado de dos dominios puede crear cuentas de Administrador de dominio en cada uno que utilicen la misma contraseña e incluso establecer contraseñas de administrador local en equipos del dominio que sean iguales en el dominio. En ese caso, si se produce una situación de riesgo con una cuenta o un equipo, puede poner en peligro el dominio entero.
- Una vez instalado Navision y creadas o actualizadas las bases de datos, debe crear un inicio de sesión de Windows y asignarle la función SUPER en Navision. El usuario SUPER se encargará de la administración de bases de datos, la seguridad, etc. Utilice una contraseña segura con este inicio de sesión. La contraseña debe ser confidencial. Debe garantizar la misma protección suministrada a la contraseña SA en SQL Server. La función SUPER administra todo el acceso de base de datos, que requiere el nivel más alto posible de protección. La contraseña del usuario SUPER sólo deben conocerla los administradores del sistema.
- Los demás usuarios que tengan acceso a la base de datos de Navision deben trabajar con privilegios mínimos. Esto significa que sólo se les deben asignar funciones en Navision que les proporcionen acceso únicamente a las características y la funcionalidad que necesiten para realizar sus tareas en la empresa.
- Asegúrese de que sólo los usuarios cuya función en la empresa lo requiera pueden importar archivos FOB y rediseñar objetos así como crear y restaurar copias de seguridad de base de datos.
- Realice copias de seguridad periódicas de la base de datos de Navision y pruébelas para asegurarse de que se pueden restaurar correctamente.
- Almacene las copias de seguridad en un lugar seguro para limitar el impacto de riesgos como el fuego, humo, altas temperaturas, rayos y desastres medioambientales (por ejemplo, un terremoto).
- Aunque Navision se puede ejecutar en varias versiones de Windows, se recomienda utilizar los sistemas operativos más recientes con las características de seguridad más actualizadas. Actualmente son el Service Pack 2 de Windows XP y Windows Server 2003.

- Utilice el servicio Windows Update proporcionado con Windows 2000, Windows XP y Windows Server 2003 para aplicar las actualizaciones de seguridad más recientes. Utilice la característica Actualización automática de Windows para mantener actualizados todos los equipos cliente con las correcciones de seguridad, Service Packs y actualizaciones más recientes.
- Se recomienda utilizar el protocolo seguro TCPS para la comunicación entre los clientes Navision y el servidor de base de datos de Navision. TCPS es una versión segura de TCP/IP que utiliza la Interfaz de proveedor de compatibilidad de seguridad (SSPI, *Security Support Provider Interface*) con cifrado habilitado y autenticación Kerberos. TCPS es el protocolo predeterminado del servidor de base de datos de Navision.
- El cliente debe disponer de un plan de recuperación de desastres que asegure la reanudación rápida de los servicios tras un desastre. Un plan de recuperación debe incluir aspectos como los siguientes:
  - Adquisición de equipamiento nuevo o temporal
  - Restauración de copias de seguridad en los nuevos sistemas
  - Comprobación de que el plan de recuperación funciona realmente

Seguridad física

La seguridad física es absolutamente esencial, ya que no hay ninguna forma de complementarla con seguridad de software. Por ejemplo, si se roba una unidad de disco duro, también se robarán los datos que contiene. Trate las siguientes cuestiones de seguridad física al desarrollar una directiva con el cliente:

- Para grandes instalaciones con departamentos de IT dedicados, asegúrese de que las salas de servidores y los lugares donde se almacena el software están cerrados con llave.
- Entre los equipos de esta categoría se incluyen:
  - El servidor con Microsoft SQL Server 2000
  - El servidor de archivos donde residen los ejecutables de Navision
- Mantenga los equipos fuera del alcance de los usuarios no autorizados.
- Asegúrese de instalar alarmas antirrobo, con independencia del nivel de confidencialidad de los datos.
- Asegúrese de que las copias de seguridad de los datos cruciales se almacenan fuera del sitio y que las copias de seguridad se guardan en contenedores ignífugos.

Empleados

Es conveniente limitar los derechos administrativos en todos los productos y características. De forma predeterminada, los clientes sólo deben conceder a los empleados acceso de lectura a las funciones del sistema, salvo que requieran otros privilegios para realizar su trabajo. Microsoft recomienda seguir el principio de privilegios mínimos: conceder a los usuarios sólo los privilegios necesarios para tener acceso a los datos y la funcionalidad.

Los empleados descontentos y los que ya no trabajan en la empresa son una amenaza para la seguridad de la red. Al tratar acerca de la seguridad con los clientes, recomiende la siguiente directiva en relación con los empleados:

- Lleve a cabo investigaciones de antecedentes laborales.
- Prevea "venganzas" de los empleados descontentos y los que ya no trabajan en la empresa.
- Asegúrese de que se deshabilitan todas las cuentas de Windows y contraseñas asociadas cuando un empleado abandona la empresa. A efectos de informes, no elimine los usuarios. No reutilice las cuentas.
- Proporcione entrenamiento a los usuarios para que estén alerta ante actividades sospechosas e informen de ellas.
- No conceda privilegios de forma automática. Si los usuarios no necesitan tener acceso a determinados equipos, salas de equipos o conjuntos de archivos, asegúrese de que no lo tengan.
- Proporcione entrenamiento a los supervisores para identificar y responder ante posibles problemas con los empleados.
- Asegúrese de que los empleados conocen su función en el mantenimiento de la seguridad de la red.
- Dé una copia de las directivas de la compañía a todos los empleados.
- No permita que los usuarios instalen software que no esté autorizado por los responsables.

Administrador

Se recomienda que los administradores del sistema de los clientes se mantengan informados de las correcciones de seguridad más recientes disponibles en Microsoft. Los atacantes son muy hábiles en la combinación de pequeños errores para realizar intrusiones a gran escala en una red. En primer lugar, los administradores deben asegurarse de que cada equipo es lo más seguro posible y, después, deben agregar las actualizaciones de seguridad y utilizar software antivirus. En esta guía se ofrecen multitud de vínculos y recursos para ayudarle a buscar información valiosa y prácticas recomendadas.

La complejidad es otro de los inconvenientes para proteger la red. Cuanto más compleja sea la red, más difícil será protegerla o solucionar los problemas después de que un intruso haya conseguido obtener acceso. El administrador debe crear documentos de la topografía completa de la red, con el objetivo de mantener la máxima sencillez posible.

La seguridad está principalmente relacionada con la administración del riesgo. Como la tecnología no es la solución a todos los problemas, la seguridad exige una combinación de tecnología y directivas. Dicho de otra forma, nunca habrá un producto que simplemente pueda desempaquetar e instalar en la red, y que proporcione al instante una seguridad perfecta. La seguridad es el resultado de la tecnología y las directivas: lo que en última instancia determina el nivel de seguridad de una red es la forma de utilizar la tecnología. Microsoft proporciona tecnología y características que tienen en cuenta la seguridad, pero sólo el administrador, con la orientación adecuada, puede determinar las

directivas correctas para cada organización. Asegúrese de planear la seguridad al principio del proceso de implementación. Debe conocer qué desea proteger el cliente y qué está dispuesto a hacer para protegerlo.

Por último, desarrolle planes de contingencias para posibles emergencias antes de que sucedan. Combine planes exhaustivos con tecnología sólida para que el cliente disfrute de la máxima seguridad.

Para obtener más información acerca de la seguridad en general, consulte el documento "The Ten Immutable Laws of Security Administration" (Decálogo de la administración de la seguridad) en la dirección:
http://www.microsoft.com/technet/archive/community/columns/security/essays/10salaws.mspx

y los artículos acerca de la administración de la seguridad en la dirección:
http://www.microsoft.com/technet/community/columns/secmgmt/smarch.mspx

Protección del sistema operativo de servidor

Aunque es posible que muchos pequeños clientes no tengan un sistema operativo de servidor, es importante que conozca las prácticas recomendadas de seguridad y pueda comunicarlas a los grandes clientes que tienen entornos de red más complejos. Asimismo, debe saber que muchas de las directivas y prácticas que se describen en este documento se pueden aplicar de forma sencilla en empresas que sólo utilizan sistemas operativos de cliente.

Los conceptos de esta sección son aplicables a los productos Microsoft Windows 2000 Server y Microsoft Windows Server 2003, aunque la información se ha extraído principalmente de la Ayuda en pantalla de Windows Server 2003. Windows Server 2003 ofrece un eficaz conjunto de características de seguridad. La Ayuda en pantalla de Windows Server 2003 contiene información completa acerca de todas las características y procedimientos de seguridad.

Para obtener información adicional acerca de Windows 2000 Server, visite el centro de seguridad de Windows 2000 Server, en la dirección
http://www.microsoft.com/technet/security/prodtech/win2000/default.mspx

y lea la guía Windows 2000 Security Hardening Guide en la dirección:
http://www.microsoft.com/technet/security/prodtech/win2000/win2khg/default.mspx

Para obtener información adicional acerca de Windows Server 2003, consulte la *Guía de seguridad de Windows Server 2003*, en la dirección
http://www.microsoft.com/technet/security/prodtech/win2003/w2003hg/sgch00.mspx

Las características principales del modelo de seguridad de servidor de Windows son la autenticación, el control de acceso y el inicio de sesión único:

- La autenticación es el proceso mediante el cual el sistema valida la identidad de un usuario utilizando sus credenciales de inicio de sesión. El nombre y la contraseña del usuario se comparan con los datos de una lista autorizada. Si el sistema detecta una coincidencia, la autorización concede acceso al usuario en la medida especificada en la lista de permisos para dicho usuario.

- El control de acceso limita el acceso del usuario a información o recursos informáticos en función de su identidad y su pertenencia a varios grupos predefinidos. En general, el control de acceso lo utilizan los administradores de sistemas para controlar el acceso de los usuarios a los recursos de la red, como servidores, directorios y archivos. Generalmente se implementa mediante la concesión de permiso a usuarios y grupos para tener acceso a objetos específicos.
- El inicio de sesión único permite que un usuario inicie sesión en el dominio de Windows una vez, con una sola contraseña, y se autentique en cualquier equipo del dominio de Windows. El inicio de sesión único permite a los administradores implementar la autenticación mediante contraseña en toda la red Windows, al tiempo que proporciona a los usuarios finales facilidad de acceso.

En las siguientes secciones se ofrece una descripción más detallada de estas tres características clave.

Autenticación

La autenticación es un aspecto fundamental de la seguridad del sistema y se utiliza para confirmar la identidad de cualquier usuario que intenta iniciar sesión en un dominio o tener acceso a los recursos de la red. El punto débil de la mayoría de los sistemas de autenticación es la contraseña del usuario.

Las contraseñas proporcionan la primera línea de defensa contra el acceso no autorizado al dominio y los equipos locales. Sugiera las siguientes prácticas recomendadas:

- Utilice siempre contraseñas seguras.
- Si las contraseñas deben escribirse en un papel, guarde el papel en un lugar seguro y destrúyalo cuando ya no sea necesario.
- No revele nunca las contraseñas a nadie.
- Utilice diferentes contraseñas para todas las cuentas de usuario.
- Cambie las contraseñas periódicamente.
- Tenga cuidado de dónde se guardan las contraseñas en los equipos.

Contraseñas seguras

La función que desempeñan las contraseñas en la protección de la red de una organización suele subestimarse y pasarse por alto. Como se mencionó anteriormente, las contraseñas proporcionan la primera línea de defensa contra el acceso no autorizado a la red. Por lo tanto, debe asegurarse de que los clientes indican a sus empleados que utilicen contraseñas seguras.

Sin embargo, las herramientas para descubrir contraseñas son cada vez mejores y los equipos que se utilizan para ello son más eficaces que nunca. Si se le da tiempo suficiente, una herramienta automatizada puede descubrir cualquier contraseña. No obstante, las contraseñas seguras son mucho más difíciles de descubrir que las no seguras.

Si desea más información acerca de cómo crear contraseñas seguras que los usuarios pueden recordar, consulte las direcciones

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

y

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

Definición de la directiva de contraseñas

Al ayudar al cliente a definir su directiva de contraseñas, asegúrese de crear una directiva que exija que todas las cuentas de usuario tengan contraseñas seguras. En la mayoría de los sistemas, es suficiente con seguir las recomendaciones de la Guía de seguridad de Windows Server 2003:

- Defina la configuración de directiva **Forzar el historial de contraseñas** para que se recuerden varias contraseñas anteriores. Con esta configuración de directiva, los usuarios no pueden utilizar la misma contraseña cuando ésta caduca.

  Configuración recomendada: 24

- Defina la configuración de directiva **Vigencia máxima de la contraseña** para que las contraseñas caduquen con la frecuencia necesaria en el entorno del cliente.

  Configuración recomendada: entre 42 (predeterminado) y 90.

- Defina la configuración de directiva **Vigencia mínima de la contraseña** para que las contraseñas no se puedan cambiar hasta que transcurra un determinado número de días. Esta configuración de directiva funciona en combinación con la configuración de directiva **Forzar el historial de contraseñas**. Si se define una vigencia mínima de la contraseña, los usuarios no pueden cambiar repetidamente sus contraseñas para eludir la configuración de directiva **Forzar el historial de contraseñas** y, después, utilizar sus contraseñas originales. Los usuarios deben esperar el número de días especificado para cambiar su contraseña.

  Configuración recomendada: 2.

- Defina una configuración de directiva **Longitud mínima de la contraseña** de forma que las contraseñas deban estar formadas por un número mínimo de caracteres especificado. Las contraseñas largas, de siete caracteres o más, suelen ser más seguras que las cortas. Con esta configuración de directiva, los usuarios no pueden utilizar contraseñas en blanco y deben crear contraseñas que tengan al menos un determinado número de caracteres de longitud.

  Configuración recomendada: 8.

- Habilite la configuración de directiva **Las contraseñas deben cumplir los requerimientos de complejidad**. Esta configuración de directiva comprueba todas las contraseñas nuevas para asegurar que se cumplen los requisitos básicos de seguridad de las contraseñas. Esta configuración asegura que las contraseñas constan de al menos tres caracteres de las cuatro categorías (mayúsculas, minúsculas, números y símbolos no alfanuméricos) y que no contienen ninguna parte del nombre de usuario ni el nombre o apellidos del usuario.

  Nota
  Las contraseñas que cumplen estos requisitos no son necesariamente muy seguras. Por ejemplo, la contraseña “Contraseña1” cumple estos requisitos.

  Configuración recomendada: Sí

- Para ver una lista de estos requisitos, consulte "Las contraseñas deben cumplir los requerimientos de complejidad" en la Ayuda en pantalla de Windows Server.
- Almacene las contraseñas con cifrado reversible. El cifrado reversible se utiliza en sistemas en los que una aplicación necesita acceso a contraseñas de texto sin formato. En la mayoría de las implementaciones no es necesario.

  Configuración recomendada: No.

Para obtener más información, consulte la Guía de seguridad de Windows Server 2003:

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

Definición de una directiva de bloqueo de cuentas

Tenga cuidado al definir la directiva de bloqueo de cuentas. Esta directiva no debe establecerse nunca en una pequeña empresa, ya que es bastante probable que bloquee a los usuarios autorizados, lo que puede resultar muy costoso para el cliente.

Si el cliente decide aplicar la directiva de bloqueo de cuentas, establezca la configuración **Umbral de bloqueos de la cuenta** en un número suficientemente alto para que las cuentas de los usuarios autorizados no se queden bloqueadas simplemente por escribir incorrectamente su contraseña varias veces.

Para obtener más información acerca de la directiva de bloqueo de cuentas, consulte "Introducción a la directiva de bloqueo de cuentas" en la Ayuda en pantalla de Windows Server.

Para obtener información acerca de cómo aplicar o modificar la directiva de bloqueo de cuentas, consulte "Para aplicar o modificar la directiva de bloqueo de cuentas" en la Ayuda en pantalla de Windows Server.

Control de acceso

Una red Windows y sus recursos (incluido Navision) se pueden proteger si se considera qué derechos tienen los usuarios, grupos de usuarios y demás equipos en la red. Puede proteger un equipo o varios concediendo derechos de usuario específicos a los usuarios o grupos. Puede proteger un objeto, como un archivo o una carpeta, mediante la asignación de permisos con los que los usuarios o grupos puedan realizar acciones específicas en dicho objeto. Los conceptos clave que componen el control de acceso incluyen:

- Permisos
- Propiedad de los objetos
- Herencia de permisos
- Derechos de usuario
- Auditoría de objetos

Permisos

Los permisos definen el tipo de acceso que se concede a un usuario o grupo para un objeto o propiedad de objeto, como archivos, carpetas y objetos del Registro. Los permisos se aplican a cualquier objeto protegido, como los archivos y los objetos del Registro. Los permisos se pueden conceder a cualquier usuario, grupo o equipo. Es conveniente asignar permisos a los grupos.

Propiedad de los objetos

Cuando se crea un objeto se le asigna un propietario. De forma predeterminada en Windows 2000 Server, el propietario es el creador del objeto. Esto ha cambiado en Windows Server 2003 para los objetos creados por los miembros del grupo Administradores.

Cuando un miembro del grupo Administradores crea un objeto en Windows Server 2003, el propietario es el grupo Administradores en lugar de la cuenta individual que ha creado el objeto. Este comportamiento se puede modificar mediante el complemento MMC (Microsoft Management Console) Configuración de seguridad local, utilizando la configuración **Objetos de sistema: propietario predeterminado para objetos creados por miembros del grupo de administradores**. Con independencia de qué permisos se establezcan en un objeto, su propietario siempre puede cambiarlos.

Para obtener más información, consulte "Posesión" en la Ayuda en pantalla de Windows Server.

Herencia de permisos

La herencia permite que los administradores asignen y administren de forma sencilla los permisos. Esta característica causa automáticamente que los objetos de un contenedor hereden todos los permisos posibles de ese contenedor. Por ejemplo, al crear archivos en una carpeta, heredan los permisos de la carpeta. Sólo se heredan los permisos marcados para herencia.

Derechos de usuario

Los derechos de usuario conceden privilegios y derechos de inicio de sesión específicos a usuarios y grupos del entorno informático.

Para obtener información acerca de los derechos de usuario, consulte "Derechos de usuario" en la Ayuda en pantalla de Windows Server.

Auditoría de objetos

El acceso de los usuarios a los objetos se puede auditar. Después, puede ver los sucesos relacionados con la seguridad en el registro de seguridad mediante el Visor de sucesos.

Para obtener más información, consulte "Auditoría" en la Ayuda en pantalla de Windows Server.

Prácticas recomendadas de control de acceso

- Asigne permisos a los grupos en lugar de a los usuarios. Puesto que no es eficaz mantener directamente las cuentas de usuario, la asignación de permisos por usuario debe llevarse a cabo excepcionalmente.
- Utilice permisos Denegar en casos especiales. Por ejemplo, puede utilizarlos para excluir un subconjunto de un grupo que tiene permisos Permitir.
- Nunca deniegue al grupo Todos el acceso a un objeto. Si deniega a todos el permiso para un objeto, incluirá también a los administradores. Una solución mejor sería quitar el grupo Todos, a condición de que conceda a otros usuarios, grupos o equipos los permisos para ese objeto. Recuerde que si no hay definidos permisos, no se permite el acceso.
- Asigne los permisos para un objeto en la parte más alta posible del árbol y, después, aplique la herencia para propagar la configuración de seguridad por el árbol. Puede aplicar de forma rápida y eficaz la configuración de control de acceso a todos los elementos secundarios o a un subárbol de un objeto principal. De esa manera, obtendrá el máximo efecto con el mínimo esfuerzo. La configuración de permisos que establezca debe ser adecuada para la mayoría de los usuarios, grupos y equipos.
- En ocasiones, los permisos explícitos pueden reemplazar a los permisos heredados. Los permisos Denegar heredados no impiden el acceso a un objeto si éste tiene una entrada de permiso explícito Permitir. Los permisos explícitos tienen preferencia sobre los permisos heredados, incluidos los permisos Denegar heredados.
- En el caso de los permisos en objetos de Active Directory®, asegúrese de conocer las prácticas recomendadas específicas para ellos.

Para obtener más información, consulte "Prácticas recomendadas para asignar permisos a objetos de Active Directory" en la Ayuda en pantalla de Windows Server 2003.

Servidor de seguridad externo

Un servidor de seguridad es hardware o software que impide que los paquetes de datos entren o salgan de una red determinada. Para controlar el flujo de tráfico, los puertos del servidor de seguridad están abiertos o cerrados para los paquetes de información. El servidor de seguridad examina diversas partes de información en cada paquete de datos: el protocolo mediante el que el paquete se va a entregar, el destino o el remitente del paquete, el tipo de contenido del paquete y el número de puerto al que se envía. Si el servidor de seguridad está configurado para aceptar el protocolo especificado a través del puerto de destino, se permite el paso del paquete. Microsoft Windows Small Business Server 2003 Premium Edition incluye Microsoft Internet Security and Acceleration (ISA) Server 2000 como solución de servidor de seguridad. Small Business Server Standard Edition también incluye un servidor de seguridad.

ISA Server 2004

Internet Security and Acceleration (ISA) Server 2000 enruta de forma segura las solicitudes y respuestas entre Internet y los equipos cliente de la red interna.

ISA Server actúa como una puerta de enlace de seguridad con Internet para los clientes de la red local. El equipo con ISA Server es transparente para las otras partes de la ruta de comunicación. El usuario de Internet no debería saber si hay un servidor de seguridad presente, salvo que intente tener acceso a un servicio o ir a un sitio al que el equipo con ISA Server le deniega el acceso. El servidor de Internet al que se tiene acceso interpreta las solicitudes del equipo ISA Server como si éstas tuvieran origen en la aplicación cliente.

Al elegir el filtrado de fragmentos de Protocolo Internet (IP) se permite que los servicios Proxy Web y Servidor de seguridad filtren fragmentos de paquetes. Mediante el filtrado de fragmentos de paquetes, todos los paquetes IP fragmentados se descartan. Un "ataque" muy conocido utiliza el envío de paquetes fragmentados que luego se ensamblan de nuevo de forma que pueden causar daños en el sistema.

ISA Server incluye un mecanismo de detección de intrusiones que identifica la hora en que se intenta un ataque contra una red y lleva a cabo un conjunto de acciones (o alertas) configuradas por si se produce un ataque.

Si Servicios de Internet Information Server (IIS) está instalado en el equipo con ISA Server, debe configurarlo para que no use los puertos que ISA Server utiliza para las solicitudes Web salientes (de forma predeterminada, 8080) y entrantes (de forma predeterminada, 80). Por ejemplo, puede modificar IIS para que supervise el puerto 81 y, después, configurar el equipo con ISA Server para dirigir las solicitudes Web entrantes al puerto 81 del equipo local en el que se ejecuta IIS.

Si se produce un conflicto entre los puertos que ISA Server e IIS utilizan, el programa de configuración detiene el servicio de publicación de IIS. Después, puede modificar IIS para que supervise un puerto diferente y reiniciar el servicio de publicación de IIS.

Directivas de ISA Server

Puede definir una directiva de ISA Server que determine el acceso de entrada y salida. Las reglas de sitio y contenido especifican a qué sitios y a qué contenido se puede tener acceso. Las reglas de protocolo indican si se puede tener acceso a un protocolo determinado para la comunicación entrante y saliente.

Puede crear reglas de sitio y contenido, reglas de protocolo, reglas de publicación en Web y filtros de paquetes IP. Estas directivas determinan cómo se comunican los clientes de ISA Server con Internet y qué comunicación se permite.

Protección antivirus

Un virus informático es un archivo ejecutable diseñado para replicarse a sí mismo, borrar o dañar archivos de datos y programas, y evitar su detección. De hecho, los virus suelen reescribirse y ajustarse para que no se puedan detectar. Es frecuente que los virus se envíen como datos adjuntos de correo electrónico. Los programas antivirus deben actualizarse constantemente para poder buscar virus nuevos y modificados. Los virus son el principal método de vandalismo informático.

El software antivirus está especialmente diseñado para la detección y prevención de los programas de virus. Como se crean continuamente nuevos programas de virus, muchos fabricantes de productos antivirus ofrecen a los clientes actualizaciones periódicas de su software. Microsoft recomienda encarecidamente la implementación de software antivirus en el entorno del cliente.

El software antivirus suele instalarse en estos tres lugares: las estaciones de trabajo de los usuarios, los servidores y la red donde el correo electrónico entra (y, en algunos casos, sale) en la organización.

Tipos de virus

Existen tres tipos principales de virus que infectan los equipos: virus del sector de inicio, virus de infección de archivos y programas troyanos.

Virus del sector de inicio

Al iniciar un equipo, se analiza el sector de inicio del disco duro antes de cargar el sistema operativo o los archivos de inicio. Los virus del sector de inicio están diseñados para reemplazar la información del sector de inicio de los discos duros por su propio código. Cuando un equipo se infecta con este tipo de virus, el código del virus se lee en la memoria antes que todo lo demás. Una vez que el virus está en la memoria, puede replicarse en cualquier otro disco que esté en uso en el equipo infectado.

Virus de infección de archivos

El tipo más común de virus, el virus de infección de archivos, se adjunta a un archivo de programa ejecutable agregando su propio código. El código del virus suele agregarse de forma que evita la detección. Cuando se ejecuta el archivo infectado, el virus puede adjuntarse a otros archivos ejecutables. Los archivos que se infectan con este tipo de virus suelen tener la extensión .com, .exe o .sys.

Algunos virus de infección de archivos están diseñados para programas específicos. Los tipos de programas que suelen ser objeto de ataques son los archivos de superposición (.ovl) y los archivos de biblioteca de vínculos dinámicos (.dll). Aunque estos archivos no se ejecutan, los ejecutables los llaman. El virus se transmite cuando se realiza la llamada.

Los daños en los datos tienen lugar cuando se activa el virus. Un virus puede activarse al ejecutar un archivo infectado o cuando se cumple una condición determinada en el entorno (por ejemplo, una fecha específica del sistema).

Programas troyanos

En realidad, un programa troyano no es un virus. La distinción fundamental entre un virus y un programa troyano es que el troyano no se replica a sí mismo, sólo destruye información en el disco duro. El troyano se disfraza como un programa legítimo, por ejemplo un juego o una utilidad. Sin embargo, al ejecutarse puede destruir o estropear datos.

Prácticas recomendadas de protección antivirus

La difusión de un virus de macro se puede impedir. A continuación se ofrecen algunas sugerencias para evitar las infecciones que debe comentar a sus clientes:

- Instale una solución de protección antivirus que busque virus en los mensajes entrantes de Internet antes de que éstos pasen por el enrutador. De esta forma se asegura que se han analizado los mensajes de correo electrónico en busca de virus conocidos.
- Observe el origen de los documentos que se reciben. Los documentos no deben abrirse salvo que procedan de un remitente que el cliente considere de confianza.
- Hable con la persona que ha creado el documento. Si los usuarios no están totalmente convencidos de que el documento sea seguro, deben ponerse en contacto con la persona que ha creado el documento.
- Utilice la protección contra virus de macro de Microsoft Office. En Office, las aplicaciones alertan al usuario si un documento contiene macros. Esta característica permite que el usuario habilite o deshabilite las macros al abrir el documento.
- Utilice software de detección de virus para detectar y eliminar los virus de macro. El software de detección de virus puede detectar y generalmente eliminar los virus de macro de los documentos. Microsoft recomienda el uso de software antivirus que esté certificado por ICSA (*International Computer Security Association*).

Para obtener más información acerca de los virus y la seguridad informática en general, visite los siguientes sitios Web de seguridad de Microsoft:

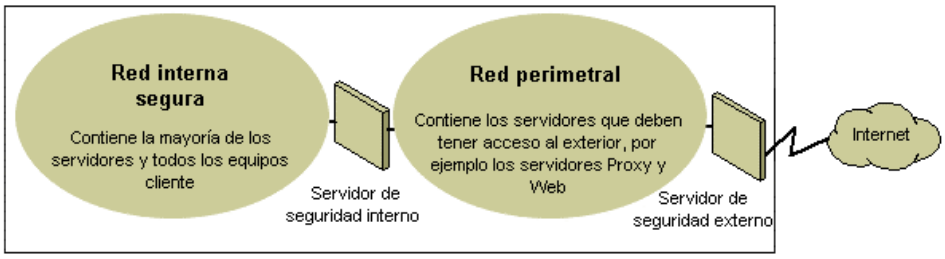
- Seguridad de Microsoft, en la dirección http://www.microsoft.com/security/default.asp.
- Documentación de seguridad en Microsoft TechNet, en la dirección http://www.microsoft.com/technet/security/Default.mspx.

Estrategias de seguridad de red

Como el diseño y la implementación de un entorno de trabajo en redes IP requieren un equilibrio entre posibles problemas de redes públicas y privadas, el servidor de seguridad se ha convertido en un componente clave para salvaguardar la integridad de la red. Un servidor de seguridad no es un solo componente. La definición de servidor de seguridad de NCSA (*National Computer Security Association*) es "un sistema o combinación de sistemas que impone un límite entre dos o más redes". Aunque se utilizan diferentes

términos, dicho límite se conoce habitualmente como "red perimetral". La red perimetral protege la intranet o la red de área local (LAN) contra intrusiones mediante el control del acceso desde Internet u otras redes de gran tamaño.

En el siguiente diagrama se muestra una red perimetral flanqueada por servidores de seguridad y situada entre una red privada e Internet con el fin de proteger la red privada:



Red perimetral básica

El enfoque del uso de servidores de seguridad como medida de protección varía según la organización. El filtrado de paquetes IP ofrece una seguridad deficiente, es complicado de administrar y se puede vencer con facilidad. Las puertas de enlace de aplicación son más seguras que los filtros de paquetes y más sencillas de administrar porque sólo pertenecen a unas pocas aplicaciones específicas, por ejemplo un sistema determinado de correo electrónico. Las puertas de enlace de circuitos son muy eficaces cuando el usuario de una aplicación de red es una preocupación mayor que los datos que transfiere dicha aplicación. El servidor proxy es una herramienta de seguridad completa que incluye una puerta de enlace de aplicación y acceso seguro para los usuarios anónimos, entre otros servicios. A continuación se ofrece información sobre las diferentes opciones:

- **Filtrado de paquetes IP**
  El filtrado de paquetes IP fue la primera implementación de la tecnología de servidor de seguridad. Los encabezados de los paquetes se examinan en busca de las direcciones de origen y destino, y los puertos de Protocolo de control de transporte (TCP) y de Protocolo de datagramas de usuario (UDP) así como otro tipo de información. El filtrado de paquetes es una tecnología limitada que funciona correctamente en entornos de seguridad clara en los que, por ejemplo, todo lo que está fuera de la red perimetral no es de confianza y todo lo que está dentro sí. En los últimos años, diversos proveedores han mejorado el método de filtrado de paquetes al agregar características inteligentes de toma de decisiones a la base del filtrado de paquetes y han creado una nueva forma de filtrado de paquetes llamada *control de protocolo activo*. Puede configurar el filtrado de paquetes para aceptar tipos específicos de paquetes a la vez que se rechazan todos los demás o para rechazar tipos específicos de paquetes y aceptar todos los demás.
- **Puertas de enlace de aplicación**
  Las puertas de enlace de aplicación se utilizan cuando la mayor preocupación es el contenido real de una aplicación. El hecho de que son específicas de aplicaciones es a la vez una ventaja y un inconveniente, ya que no se adaptan fácilmente a los cambios en la tecnología.

- **Puertas de enlace de circuitos**
  Las puertas de enlace de circuitos son túneles creados en un servidor de seguridad que conectan procesos o sistemas específicos en un lado con procesos o sistemas específicos en el otro. Las puertas de enlace de circuitos son muy útiles en situaciones en las que la persona que utiliza una aplicación es un riesgo potencialmente mayor que la información que transporta la aplicación. La puerta de enlace de circuitos se distingue del filtro de paquetes por su capacidad para conectar a un esquema de aplicación fuera de banda que puede agregar información.
- **Servidores proxy**
  Los servidores proxy son herramientas de seguridad completas que incluyen funciones de servidor de seguridad y de puerta de enlace de aplicación, y que administran el tráfico entre Internet y una red LAN. Los servidores proxy también proporcionan almacenamiento en caché de documentos y control de acceso. Un servidor proxy puede mejorar el rendimiento mediante el almacenamiento en caché y el suministro directo de datos solicitados con frecuencia, por ejemplo una página Web popular. El servidor proxy también puede filtrar y descartar solicitudes que el propietario no considera apropiadas, como las solicitudes de acceso no autorizado a los archivos de propiedad exclusiva.

Asegúrese de que el cliente aprovecha las características de protección del servidor de seguridad que pueden ayudarle. Coloque una red perimetral en un punto de la topología de la red donde todo el tráfico de fuera de la red empresarial deba pasar a través del perímetro mantenido por el servidor de seguridad externo. Puede ajustar el control de acceso del servidor de seguridad para cubrir las necesidades del cliente y puede configurar los servidores de seguridad para que informen de todos los intentos de acceso no autorizado.

Para minimizar el número de puertos que deben abrirse en el servidor de seguridad interno, puede utilizar un servidor de seguridad de nivel de aplicación, como ISA Server 2000.

Para obtener más información acerca de TCP/IP, consulte el documento "Designing a TCP/IP Network" (Diseño de una red TCP/IP) en la dirección http://www.microsoft.com/resources/documentation/WindowsServ/2003/all/deployguide/en-us/dnsbb_tcp_overview.asp.

Redes inalámbricas

De forma predeterminada, las redes inalámbricas están en general configuradas de manera que se pueden escuchar las señales inalámbricas. Pueden ser vulnerables a un intruso malintencionado que obtenga acceso gracias la configuración predeterminada de algunos dispositivos de hardware inalámbrico, la accesibilidad que ofrecen las redes inalámbricas y los actuales métodos de cifrado. Hay opciones y herramientas de configuración que pueden proteger de la escucha, pero debe tenerse en cuenta que no sirven para proteger los equipos contra los intrusos y los virus que entran a través de la conexión de Internet. Por lo tanto, es extremadamente importante incluir un servidor de seguridad para proteger los equipos de intrusos no deseados en Internet.

Para obtener más información acerca de cómo proteger una red inalámbrica, consulte el artículo "How to Make Your 802.11b Wireless Home Network More Secure" (Cómo hacer más segura su red doméstica inalámbrica 802.11b) en la dirección http://support.microsoft.com/default.aspx?scid=kb;en-us;309369.

Escenarios de seguridad de red

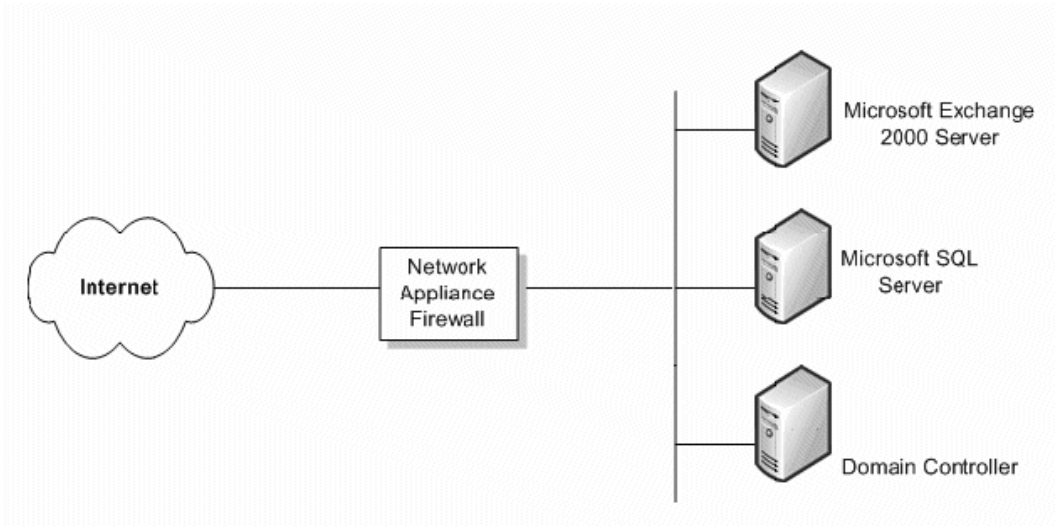
El nivel de seguridad de red que requiere la organización del cliente depende de varios factores. Suele reducirse a un equilibrio entre el presupuesto y la necesidad de mantener la seguridad de los datos de la empresa. Una pequeña empresa puede tener una estructura de seguridad muy compleja que proporcione el nivel más alto posible de seguridad de red, pero es probable que no se lo pueda permitir. En esta sección, se examinan cuatro escenarios y se ofrecen recomendaciones en cada uno que proporcionan diferentes niveles de seguridad.

Sin servidor de seguridad

Si el cliente tiene una conexión a Internet pero no tiene un servidor de seguridad, debe implementarse alguna medida de seguridad de red. Hay dispositivos sencillos de servidor de seguridad de red que proporcionan suficiente seguridad para disuadir a la mayoría de los aspirantes a intrusos.

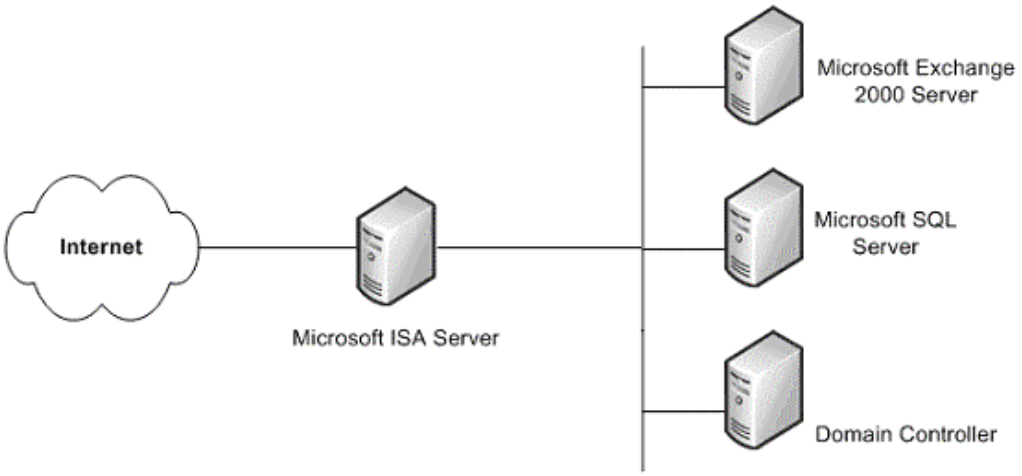
Un servidor de seguridad sencillo

El nivel mínimo de seguridad recomendado es un solo servidor de seguridad entre Internet y los datos del cliente. Este servidor de seguridad no proporciona seguridad avanzada y no debe considerarse muy seguro. Pero es mejor que nada.



Servidor de seguridad sencillo

Es deseable que el presupuesto del cliente permita una solución más segura para proteger los datos empresariales. Una de esas soluciones es ISA Server. El costo adicional de este servidor proporciona mucha más seguridad que el servidor de seguridad medio, que en general sólo proporciona traducción de direcciones de red (NAT) y filtrado de paquetes.



Servidor de seguridad ISA Server

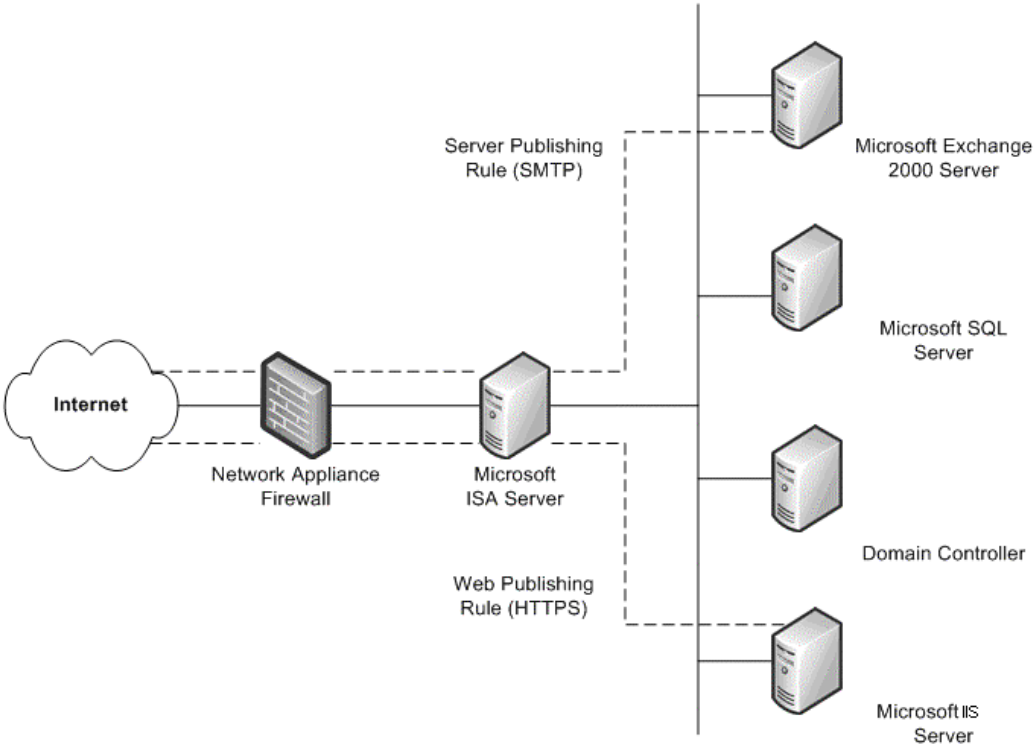
Esta solución de servidor de seguridad es más segura que un dispositivo de servidor de seguridad básico y proporciona servicios de seguridad específicos para Windows.

Servidor de seguridad existente

Si el cliente dispone de un servidor de seguridad que separa su intranet de Internet, puede ser conveniente considerar la posibilidad de utilizar un servidor de seguridad adicional que proporcione varias maneras de configurar los recursos internos para Internet.

Uno de esos métodos es la publicación en Web. En este caso, ISA Server se implementa delante del servidor Web de una organización que proporciona acceso a los usuarios de Internet. En el caso de las solicitudes Web entrantes, ISA Server puede suplantar a un servidor Web en el exterior para atender desde la caché las solicitudes cliente de contenido Web. ISA Server reenvía las solicitudes al servidor Web únicamente cuando éstas no se pueden atender desde la caché.

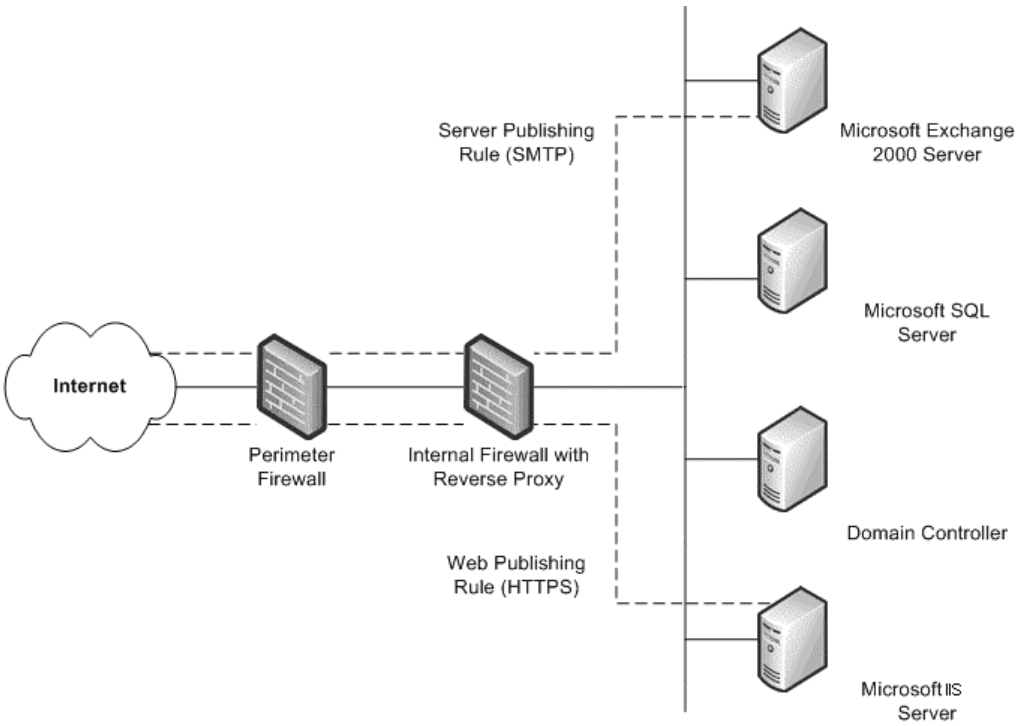
Otro método es la publicación de servidor. ISA Server permite la publicación de servidores internos en Internet sin arriesgar la seguridad de la red interna. Puede configurar reglas de publicación en Web y publicación de servidor que determinen qué solicitudes se deben enviar a un servidor de la red local, lo que proporciona un nivel mayor de seguridad para los servidores internos.



Servidor de seguridad existente con ISA Server agregado

Dos servidores de seguridad existentes

El cuarto escenario es aquel en el que la organización cuenta con dos servidores de seguridad y una red perimetral establecida (DMZ). Uno o varios de estos servidores proporcionan servicios de proxy inverso de forma que los clientes de Internet no tienen acceso directamente a los servidores de la intranet. En su lugar, uno de los servidores de seguridad, preferentemente el servidor interno, intercepta las solicitudes de red para los servidores internos, comprueba los paquetes y, después, los reenvía en nombre del host de Internet.



Dos servidores de seguridad existentes

Este escenario es similar al anterior tras agregar el segundo servidor de seguridad. La única diferencia es que el servidor de seguridad interno que admite el proxy inverso no es un servidor ISA Server. En este escenario, debe trabajar estrechamente con los responsables de cada servidor de seguridad para definir las reglas de publicación en servidor que se ajusten a la directiva de seguridad.

Administración de revisiones de seguridad

Los sistemas operativos y las aplicaciones suelen ser enormemente complejos. Pueden constar de millones de líneas de código escritas por muchos programadores diferentes. Es fundamental que el software funcione de manera confiable y no ponga en riesgo la seguridad o estabilidad del entorno de IT. Para minimizar los problemas, los programas se prueban exhaustivamente antes de su lanzamiento. Sin embargo, los atacantes no cesan en su empeño de buscar vulnerabilidades en el software, por lo que no es posible prever todos los ataques futuros.

En muchas organizaciones, la administración de revisiones forma parte de su estrategia general de administración de los cambios y la configuración. Sin embargo, con independencia de la naturaleza y el tamaño de la organización, es crucial contar con una estrategia correcta de administración de revisiones, incluso si la organización aún no dispone de administración eficaz de los cambios y la configuración. La inmensa mayoría de los ataques que tienen éxito contra los equipos informáticos se producen en aquellos sistemas en los que no se han instalado revisiones de seguridad.

Las revisiones de seguridad suponen un reto específico para la mayoría de las organizaciones. Una vez expuesta una vulnerabilidad en el software, los atacantes difundirán en general información acerca de ella rápidamente entre la comunidad de intrusos. Cuando se detecta una vulnerabilidad en el software, Microsoft se esfuerza por ofrecer una revisión de seguridad lo antes posible. Hasta que se implementa la revisión, la seguridad que el cliente espera y de la que depende puede verse gravemente afectada.

En el entorno de Navision, debe asegurarse de que los clientes tienen instaladas las revisiones de seguridad más recientes en todo el sistema. Asegúrese de que el cliente utiliza una de las tecnologías de Microsoft que están disponibles. Entre ellas se incluyen:

- **Servicio de notificación de seguridad de Microsoft**
  El Servicio de notificación de seguridad es una lista de correo electrónico que distribuye avisos cuando hay una actualización disponible. Estos avisos son un componente valioso de una estrategia de seguridad activa. También están disponibles en el sitio Web de TechNet de notificación de seguridad de productos: http://www.microsoft.com/technet/security/bulletin/notify.mspx.
- **Actualizaciones automáticas de Microsoft**
  Windows puede aplicar automáticamente actualizaciones de seguridad en los equipos.
- **Herramienta de búsqueda de boletines de seguridad de Microsoft**
  Esta herramienta está disponible en el sitio Web del Servicio de boletines de seguridad: http://www.microsoft.com/technet/security/current.aspx. El cliente puede determinar qué actualizaciones necesita en función del sistema operativo, aplicaciones y Service Packs que ejecute.
- **Microsoft Baseline Security Analyzer (MBSA)**
  Esta herramienta gráfica está disponible en el sitio Web de Microsoft Baseline Security Analyzer: http://www.microsoft.com/technet/security/tools/mbsahome.mspx. La herramienta compara el estado actual de un equipo con una lista de actualizaciones mantenida por Microsoft. Además, MBSA lleva a cabo comprobaciones básicas de seguridad de contraseñas y configuración de caducidad, directivas de cuentas de invitado y varias otras áreas. MBSA también busca vulnerabilidades en Servicios de Microsoft Internet Information Server (IIS), SQL Server™ 2000, Exchange 5.5, Exchange 2000 y Exchange Server 2003.
- **Microsoft Software Update Services (SUS)**
  Denominada anteriormente Windows Update Corporate Edition, esta herramienta permite a las empresas alojar en los equipos locales todas las actualizaciones críticas y paquetes de seguridad acumulados (SRP) disponibles en el sitio público de Windows Update. La herramienta funciona con una nueva versión de clientes de actualización automática (AU) para formar la base de una estrategia eficaz de descarga e instalación automáticas. El nuevo conjunto de clientes AU incluye un cliente para los sistemas operativos Windows 2000 y Windows Server 2003, y ofrece la posibilidad de instalar automáticamente las actualizaciones descargadas. Para obtener más información acerca de Microsoft SUS, visite la dirección http://www.microsoft.com/windows2000/windowsupdate/sus/default.asp.

- **Software Update Services Feature Pack de Microsoft Systems Management Server (SMS)**
  Software Update Services Feature Pack de SMS contiene varias herramientas orientadas a facilitar el proceso de emisión de actualizaciones de seguridad en toda la empresa. Entre ellas se incluyen una herramienta de inventario de actualizaciones de seguridad, una herramienta de inventario de actualizaciones para Microsoft Office, un asistente para la distribución de actualizaciones de software y una herramienta de informes Web de SMS con un complemento de informes Web para actualizaciones de software. Para obtener más información acerca de estas herramientas, visite la dirección http://www.microsoft.com/smserver/downloads/20/featurepacks/suspack/.

Hable con los clientes acerca de cada una de estas herramientas y recomiende su uso. Es muy importante que los problemas de seguridad se traten lo más rápidamente posible, sin que se resienta la estabilidad del entorno.

Configuración de seguridad de SQL Server 2000

Puesto que Navision también se ejecuta en SQL Server 2000, es importante que tome medidas para aumentar la seguridad de la instalación de SQL Server 2000 del cliente. Los siguientes pasos ayudarán a mejorar la seguridad de SQL Server:

- Asegúrese de que están instalados los Service Packs y actualizaciones del sistema operativo y de SQL Server 2000 más recientes. Para ver la información más reciente, consulte el sitio Web de seguridad de Microsoft en la dirección http://www.microsoft.com/security/default.asp.
- En cuanto a la seguridad del sistema de archivos, asegúrese de que todos los datos y archivos de sistema de SQL Server 2000 están instalados en particiones NTFS. Los archivos sólo deben ser accesibles para los usuarios administrativos o de nivel del sistema mediante permisos NTFS. De esta forma, los archivos estarán protegidos del acceso de los usuarios cuando el Servicio MSSQLSERVER no esté en ejecución.
- Utilice una cuenta de dominio con privilegios mínimos, como NT Authority\Servicio de red o la cuenta LocalSystem (recomendado), para el servicio SQL Server 2000 (MSSQLSERVER). Esta cuenta debe tener derechos mínimos en el dominio y contribuirá a resistir (pero no detener) un ataque al servidor en caso de riesgo. Dicho de otra forma, esta cuenta sólo debe tener permisos de usuario locales en el dominio. Si SQL Server 2000 utiliza una cuenta de Administrador de dominio para ejecutar los servicios, cualquier riesgo del servidor generará un riesgo para todo el dominio. Para cambiar esta configuración, utilice el Administrador corporativo de SQL Server. Las listas de control de acceso (ACL) de los archivos, el Registro y los derechos de usuario se modificarán automáticamente.
- La mayoría de las ediciones de SQL Server 2000 se instalan con dos bases de datos predeterminadas, **Northwind** y **pubs**. Ambas son bases de datos que se utilizan con fines de prueba y aprendizaje, y como ejemplos generales. No deben implementarse en un sistema de producción. El conocimiento de la presencia de estas bases de datos puede originar que un intruso intente llevar a cabo un ataque que afecte a la configuración predeterminada. Si las bases de datos **Northwind** y **pubs** están presentes en el equipo SQL Server 2000 de producción, deben quitarse.
- La auditoría del sistema SQL Server 2000 está deshabilitada de forma predeterminada, por lo que no se audita ninguna condición. Esto dificulta la detección de intrusiones y ayuda a los atacantes a pasar inadvertidos. Como mínimo, debe habilitarse la auditoría de inicios de sesión erróneos.

Para ver la información de seguridad más actualizada de SQL Server 2000, visite la dirección
http://www.microsoft.com/sql/techinfo/administration/2000/security/default.asp.

Acerca de Microsoft Business Solutions

Microsoft Business Solutions es una división de Microsoft que ofrece una amplia gama de aplicaciones y servicios empresariales integrados de extremo a extremo que se han diseñado para ayudar a las pequeñas, medianas y grandes empresas a estar más conectados con clientes, empleados, socios y proveedores. Las aplicaciones de Microsoft Business Solutions optimizan los procesos empresariales estratégicos relativos a administración financiera, análisis, administración de recursos humanos, administración de proyectos, administración de relaciones con los clientes, administración de servicios de campo, administración de la cadena de suministro, comercio electrónico, fabricación y administración minorista. Las aplicaciones están diseñadas para proporcionar una visión que ayude a los clientes a lograr el éxito empresarial. Encontrará más información acerca de Microsoft Business Solutions en la dirección http://www.microsoft.com/BusinessSolutions/