Microsoft Business Solutions

Navision Security Hardening Guide

Veröffentlicht: Oktober 2004

Microsoft

Inhalt

Einführung

Microsoft® Windows® bietet ausgereifte Netzwerksicherheit auf der Grundlage von Standards. Im weitesten Sinne beinhaltet Sicherheit die Planung und Berücksichtigung von Kompromissen. Beispielsweise kann ein Computer in einen Tresorraum gesperrt und nur einem Systemadministrator zugänglich gemacht werden. Dieser Computer mag zwar sicher sein, er ist jedoch nicht sehr nützlich, da er nicht mit anderen Computern verbunden ist. Sie müssen daher Überlegungen anstellen, wie das Netzwerk eine möglichst hohe Sicherheit erhalten kann, ohne dass dabei die Nutzungsmöglichkeiten eingeschränkt werden.

Die meisten Organisationen planen externe Angriffe ein und entwerfen Firewalls. Viele Unternehmen vergessen bei ihrer Planung jedoch, Massnahmen zu definieren, wie die Auswirkungen einer Sicherheitslücke verringert werden können, nachdem ein böswilliger Benutzer die Firewall durchbrochen hat. Sicherheitsmassnahmen in der Umgebung des Kunden funktionieren gut, wenn die Benutzer nicht zu viele Verfahren und Schritte durchführen müssen, um Geschäftsvorgänge sicher abzuwickeln. Die Umsetzung von Sicherheitsrichtlinien sollte sich für Benutzer so einfach wie möglich gestalten, sonst entwickeln diese weniger sichere Möglichkeiten zur Durchführung von Aufgaben.

Da die Grösse von Navision-Installationen sehr unterschiedlich ausfallen kann, ist es wichtig, die Anforderungen jedes Kunden sorgfältig zu berücksichtigen und die Effektivität der Sicherheit gegen die anfallenden Kosten abzuwägen. Empfehlen Sie als vertrauter Berater Ihres Kunden eine Richtlinie, die nach bestem Wissen und Gewissen die Sicherheitsanforderungen des Kunden erfüllt, dabei aber keine Belastungen verursacht, die letztendlich das Durchsetzen der Richtlinie wieder verhindern würden.

Bewährte Methoden zum Gewährleisten der Sicherheit in Navision

Die folgenden allgemeinen Regeln helfen beim Erhöhen der Sicherheit für die Navision-Umgebung:

- Wenn Sie Navision Database Server als Dienst ausführen oder beim Start des Servers den Befehlszeilenparameter **installasservice** verwenden möchten, sollten Sie sicherstellen, dass der Dienst unter dem Konto **NT-Autorität\Netzwerkdienst** ausgeführt wird. Das Konto **NT-Autorität\Netzwerkdienst** ist nur unter Windows™ XP und Windows Server™ 2003 vorhanden. Wenn Sie Windows 2000 Server ausführen, sollten Sie für den Dienst ein Konto mit geringen Berechtigungen erstellen, da der Dienst sonst einem lokalen Systemkonto zugewiesen wird. Dieses Konto sollte höchstens über die Berechtigungen des normalen Benutzerkontos verfügen, oder es sollte sich um ein Domänenkonto handeln, das weder in der Domäne noch auf einem lokalen Computer Administrator ist.

  Achten Sie darauf, das Konto **NT-Autorität\Netzwerkdienst** bzw. das Benutzerkonto, unter dem der Server ausgeführt wird, mit Lese- und Schreibberechtigungen für die Datenbankdatei(en) auszustatten. Nur so können Benutzer eine Verbindung mit der Datenbank herstellen.

  So weisen Sie dem Konto **NT-Autorität\Netzwerkdienst** unter Windows XP Lese- und Schreibberechtigungen für eine Datenbankdatei zu:

  1. Navigieren Sie in Windows Explorer zu dem Ordner, der die Datenbankdatei enthält.
  2. Wählen Sie die Datenbankdatei aus, klicken Sie mit der rechten Maustaste darauf, und klicken Sie dann auf **Eigenschaften**.
  3. Klicken Sie im Fenster **Eigenschaften** auf die Registerkarte **Sicherheit**, und klicken Sie dann im Feld **Benutzer- und Gruppennamen** auf **Hinzufügen**.
  4. Geben Sie im Fenster zur Auswahl von Benutzern, Computern oder Gruppen die Zeichenfolge **Netzwerkdienst** ein, und klicken Sie auf **OK**.
  5. Im Fenster **Eigenschaften** wurde dem Feld **Benutzer- und Gruppennamen** der Eintrag **NETZWERKDIENST** hinzugefügt.
  6. Wählen Sie **NETZWERKDIENST** aus, und aktivieren Sie im Feld **Berechtigungen** die Berechtigungen für **Lesen** und **Schreiben**.
- Der Navision Application Server-Dienst wird in der Standardeinstellung unter dem Konto **NT-Autorität\Netzwerkdienst** ausgeführt. Dadurch erhält der Dienst lokalen Zugriff auf Navision Database Server. In einem Netzwerk müssen Sie jedoch sicherstellen, dass der Navision Application Server-Dienst unter einem Windows-Domänenkonto ausgeführt wird, das vom Navision Database Server erkannt wird. Nur so erhält er Zugriff auf den Datenbankserver. Dieses Konto sollte weder in der Domäne noch auf einem lokalen Computer als Administrator fungieren.
- Wenn Sie mit der Navision SQL Server Option arbeiten, wird Microsoft SQL Server™ als Dienst ausgeführt. Für die Navision SQL Server Option muss SQL Server in der Lage sein, über Active Directory Listen von Windows-Benutzergruppen zu Authentifizierungszwecken abzurufen. Daher müssen Sie sicherstellen, dass der SQL Server-Dienst unter dem Konto **NT-Autorität\Netzwerkdienst** ausgeführt wird.

So stellen Sie sicher, dass der Dienst unter **NT-Autorität\Netzwerkdienst** ausgeführt wird:

1. Suchen Sie auf dem Computer mit SQL Server den Dienst **MSSQLSERVER**, klicken Sie mit der rechten Maustaste darauf, und klicken Sie auf **Eigenschaften**.
2. Klicken Sie im Fenster **Eigenschaften** auf die Registerkarte **Anmelden**.
3. Klicken Sie auf der Registerkarte **Anmelden** unter **Anmelden als** auf **Dieses Konto**, geben Sie **NT-Autorität\Netzwerkdienst** ein, und klicken Sie auf **OK**.

Weitere Informationen über Sicherheit mit SQL Server finden Sie unter folgenden Adressen:

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

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

- Wenn ein Navision-E-Business-Produkt wie Commerce Gateway ausgeführt wird, sollten Sie sicherstellen, dass der Commerce Gateway Request Server ordnungsgemäss mit den Standardkontoeinstellungen für die Dienste installiert wurde. Der Standardkontoname für den Commerce Gateway Request Server lautet **CGRSUser** und verfügt über die Mindestzugriffsrechte, um die Interaktion mit MS SQL Server and MS BizTalk Server zu ermöglichen. Es sind keine globalen Kontoeinstellungen wie im Konto **Lokales System** enthalten.
- Verwenden Sie immer sichere Kennwörter. Weitere Informationen über sichere Kennwörter finden Sie im Abschnitt „Sichere Kennwörter“.
- Verwenden Sie Windows-Anmeldungen. Mit Navision können Sie zwei Arten von Anmeldungen erstellen: Datenbankanmeldungen und Windows-Anmeldungen. Es wird die Verwendung von Windows-Anmeldungen empfohlen, da hierbei die Authentifizierung durch Windows erfolgt und somit eine ordnungsgemässe Kennwortrichtlinie durchgesetzt werden kann.
- Kennwörter sollten nicht mehrfach verwendet werden. Es ist häufig gebräuchlich, Kennwörter über verschiedene Systeme und Domänen hinweg mehrfach zu verwenden. Ein Administrator, der für zwei Domänen verantwortlich ist, kann beispielsweise in beiden Domänen Domänenadministratorkonten mit demselben Kennwort erstellen und sogar auf mehreren Computern innerhalb einer Domäne dasselbe Kennwort für lokale Administratoren einrichten. In diesem Fall kann eine Sicherheitsverletzung auf einem einzigen Computer zu Sicherheitsverletzungen in der gesamten Domäne führen.
- Nach dem Installieren von Navision und dem Erstellen oder Aktualisieren der Datenbanken sollten Sie eine Windows-Anmeldung erstellen und dieser in Navision die Rolle **SUPER** zuweisen. Dieser Benutzer **SUPER** ist für die Verwaltung, die Sicherheit usw. der Datenbank verantwortlich. Versehen Sie diese Anmeldung mit einem sicheren Kennwort. Dieses Kennwort sollte vertraulich behandelt werden. Es sollte demselben Schutz unterliegen wie das Systemadministratorkennwort für SQL Server. Sämtliche Zugriffe auf Datenbanken werden durch die Rolle **SUPER** verwaltet, sodass hier der grösstmögliche Schutz notwendig ist. Das Kennwort des Benutzers **SUPER** sollte nur den Systemadministratoren bekannt sein.
- Alle anderen Benutzer, die Zugriff auf die Navision-Datenbank haben, sollten mit geringsten Berechtigungen ausgestattet werden. Dies geschieht durch Zuweisen von Rollen in Navision, mit denen sie nur Zugriff auf die Funktionen erhalten, die zum Durchführen ihrer Aufgaben im Unternehmen erforderlich sind.
- Stellen Sie sicher, dass das Importieren von FOB-Dateien, das Umgestalten von Objekten sowie das Erstellen und Wiederherstellen von Datenbanksicherungen nur Benutzern möglich ist, deren Rolle im Unternehmen dies erfordert.

- Erstellen Sie regelmässig Sicherungskopien Ihrer Navision-Datenbank, und stellen Sie bei den Sicherungskopien unbedingt sicher, dass diese erfolgreich wiederhergestellt werden können.
- Lagern Sie die Sicherungskopien an einem sicheren Ort, um die Auswirkungen von Gefahren wie Feuer, Rauch, hohe Temperaturen, Blitzeinschlag und Umweltkatastrophen (z. B. Erdbeben) gering zu halten.
- Obwohl Navision unter verschiedenen Versionen von Windows ausgeführt werden kann, wird empfohlen, die neuesten Betriebssysteme mit den aktuellsten Sicherheitsfunktionen zu verwenden. Dabei handelt es sich zurzeit um Windows XP mit Service Pack 2 und Windows Server 2003.
- Verwenden Sie den Dienst **Windows Update** von Windows 2000, Windows XP und Windows Server 2003, um die aktuellsten Sicherheitsaktualisierungen anzuwenden. Verwenden Sie die Funktion für automatische Updates von Windows, um alle Clientcomputer mit aktuellen Sicherheitspatches, Service Packs und Aktualisierungen auf dem neuesten Stand zu halten.
- Es wird empfohlen, die Kommunikation zwischen den Navision-Clients und Navision Database Server über das sichere Protokoll TCPS durchzuführen. TCPS ist eine sichere Version von TCP/IP, in der SSPI (Security Support Provider Interface) mit aktivierter Verschlüsselung sowie die Kerberos-Authentifizierung eingesetzt werden. TCPS ist das Standardprotokoll für Navision Database Server.
- Der Kunde sollte über einen Plan für die Wiederherstellung nach Datenverlusten verfügen, mit dessen Hilfe die schnelle Wiederaufnahme der Dienste nach einem Datenverlust sichergestellt werden kann. Ein Plan für die Wiederherstellung nach Datenverlusten sollte Probleme wie die folgenden behandeln:
  - Beschaffung von neuen/vorübergehenden Geräten
  - Wiederherstellung von Sicherungen auf neuen Systemen
  - Gewährleistung der Funktionalität des Plans für die Wiederherstellung

Physische Sicherheit

Die physische Sicherheit ist unabdingbar, da sie nicht durch Softwaresicherheit ersetzt werden kann. Wenn beispielsweise ein Festplattenlaufwerk gestohlen wird, werden die Daten auf diesem Laufwerk letztendlich ebenfalls gestohlen. Diskutieren Sie die folgenden Probleme zur physischen Sicherheit bei der Entwicklung einer Richtlinie mit dem Kunden:

- Stellen Sie für grosse Installationen mit dedizierten IT-Abteilungen sicher, dass Serverräume und Lagerorte für Software abgesperrt sind.
- Zu dieser Kategorie gehören folgende Computer:
  - Der Microsoft SQL Server 2000-Server
  - Der Dateiserver, auf dem die ausführbaren Dateien von Navision gespeichert sind
- Halten Sie nicht autorisierte Benutzer von diesen Computern fern.
- Stellen Sie sicher, dass unabhängig von der Vertraulichkeit der Daten Einbrecheralarme eingebaut werden.
- Stellen Sie sicher, dass Sicherungskopien wichtiger Daten an einem anderen Standort gelagert und in feuergeschützten Behältern aufbewahrt werden.

Die Mitarbeiter

Die administrativen Rechte für sämtliche Produkte und Funktionen sollten eingeschränkt werden. Als Standard sollten die Kunden ihren Mitarbeitern nur Leseberechtigungen auf Systemfunktionen gewähren, sofern zum Durchführen der Aufgaben keine umfassenderen Berechtigungen notwendig sind. Microsoft empfiehlt, dem Prinzip der geringsten Berechtigung zu folgen: Statten Sie Benutzer nur mit den zum Zugreifen auf Daten und Funktionen mindestens erforderlichen Berechtigungen aus. Unzufriedene und ehemalige Angestellte stellen eine Bedrohung für die Netzwerksicherheit dar. Schlagen Sie bei der Erörterung der Sicherheit mit dem Kunden die folgende Richtlinie bezüglich Mitarbeitern vor:

- Stellen Sie vor der Einstellung Nachforschungen über den Werdegang an.
- Rechnen Sie mit „Racheaktionen“ von unzufriedenen und ehemaligen Angestellten.
- Stellen Sie sicher, dass bei der Kündigung eines Mitarbeiters alle zugehörigen Windows-Konten und -Kennwörter deaktiviert werden. Aus Berichterstattungsgründen sollten Benutzer nicht gelöscht werden. Verwenden Sie die Konten nicht mehrmals.
- Schulen Sie Benutzer darin, Wachsamkeit zu üben und verdächtige Aktivitäten zu melden.
- Gewähren Sie Berechtigungen nicht automatisch. Wenn Benutzer den Zugriff auf bestimmte Computer, Computerräume oder Dateien nicht benötigen, stellen Sie sicher, dass sie keinen Zugriff haben.
- Schulen Sie Vorgesetzte im Erkennen und Melden von möglichen Problemen mit Mitarbeitern.
- Stellen Sie sicher, dass die Mitarbeiter ihre Rollen bei der Erhaltung der Netzwerksicherheit verstehen.
- Händigen Sie jedem Mitarbeiter ein Exemplar der Unternehmensrichtlinien aus.
- Geben Sie Benutzern nicht die Möglichkeit, Software zu installieren, die vom Arbeitgeber nicht autorisiert wurde.

Der Administrator

Es wird empfohlen, dass die Systemadministratoren des Kunden jeweils die aktuellen Sicherheitspatches von Microsoft implementieren. Angreifer sind sehr geschickt darin, Kombinationen von mehreren kleinen Programmfehlern für grosse Angriffe in ein Netzwerk zu nutzen. Administratoren sollten zuerst sicherstellen, dass jeder einzelne Computer so sicher wie möglich ist, und dann Sicherheitsaktualisierungen hinzufügen und Antivirussoftware verwenden. Dieses Handbuch enthält viele Verknüpfungen und Ressourcen, über die Sie wertvolle Informationen und bewährte Methoden finden können.

Die Komplexität stellt einen weiteren Kompromiss bei der Absicherung des Netzwerks dar. Je komplexer ein Netzwerk aufgebaut ist, desto schwieriger ist die Absicherung oder die Fehlerbehebung, nachdem ein Eindringling sich Zugriff verschafft hat. Der Administrator sollte die Netzwerktopografie sorgfältig dokumentieren, um sie auf diese Weise so einfach wie möglich zu gestalten.

Das Hauptelement der Sicherheit ist das Risikomanagement. Da nicht jedes Problem durch Technologie behoben werden kann, ist für Sicherheit eine Kombination aus Technologie und Richtlinien erforderlich. Mit anderen Worten: Es gibt kein Produkt, das einfach dekomprimiert und im Netzwerk installiert werden kann und sofort perfekte Sicherheit bietet. Sicherheit kann nur durch Technologie und Richtlinien erzielt werden, d. h., durch die Verwendung der Technologie wird der Grad der Sicherheit in einem Netzwerk bestimmt. Microsoft bietet sicherheitsbewusste Technologie und Funktionen, jedoch kann nur der Administrator unter Ihrer Anleitung die richtigen Richtlinien für jede Organisation festlegen. Planen Sie die Sicherheit unbedingt in einem frühen Stadium des Implementierungs- und Bereitstellungsvorgangs ein. Machen Sie sich klar, was der Kunde schützen möchte und zu welchen Massnahmen er dazu bereit ist.

Entwerfen Sie schliesslich Kontingenzpläne für Notfälle, bevor diese auftreten. Kombinieren Sie ausführliche Planung mit stabiler Technologie, dann erhält der Kunde eine ausgezeichnete Sicherheit.

Weitere Informationen über allgemeine Sicherheit finden Sie in „The Ten Immutable Laws of Security Administration“ unter:
http://www.microsoft.com/technet/archive/community/columns/security/essays/10salaws.mspx

sowie in den Artikeln über Sicherheitsverwaltung unter
http://www.microsoft.com/technet/community/columns/secmgmt/smarch.mspx

Schützen des Serverbetriebssystems

Obwohl viele kleinere Kunden nicht über ein Serverbetriebssystem verfügen, ist es wichtig, bewährte Methoden für die Sicherheit zu verstehen und diese an Kunden mit komplexeren Netzwerkumgebungen weitergeben zu können. Sie sollten sich auch bewusst sein, dass viele der in diesem Dokument beschriebenen Richtlinien und Methoden einfach auf die Kunden übertragen werden können, die nur über Clientbetriebssysteme verfügen.

Die Konzepte in diesem Abschnitt treffen auf Microsoft Windows 2000 Server- und Microsoft Windows Server 2003-Produkte zu. Diese Informationen wurden jedoch überwiegend der Onlinehilfe zu Windows Server 2003 entnommen. Windows Server 2003 bietet stabile Sicherheitsfunktionen. Die Onlinehilfe zu Windows Server 2003 enthält vollständige Informationen über alle Sicherheitsfunktionen und -verfahren.

Weitere Informationen über Windows 2000 Server finden Sie im Windows 2000 Server Security Center unter
http://www.microsoft.com/technet/security/prodtech/win2000/default.mspx.

Lesen Sie ausserdem das Handbuch *Windows 2000 Security Hardening Guide* unter folgender Adresse:
http://www.microsoft.com/technet/security/prodtech/win2000/win2khg/default.mspx

Weitere Informationen über Windows Server 2003 finden Sie im Handbuch *Windows Server 2003 Security Guide* unter
http://www.microsoft.com/technet/security/prodtech/win2003/w2003hg/sgch00.mspx.

Die wichtigsten Funktionen des Windows-Serversicherheitsmodells sind die Authentifizierung, die Zugriffssteuerung und die einmalige Anmeldung:

- Bei der Authentifizierung handelt es sich um den Vorgang, bei dem das System die Identität eines Benutzers über dessen Anmeldeinformationen überprüft. Der Name und das Kennwort des Benutzers werden mit einer autorisierten Liste verglichen. Wenn das System eine Übereinstimmung erkennt, erhält der Benutzer durch die Autorisierung Zugriff in dem Ausmass, das in der Berechtigungsliste für diesen Benutzer angegeben ist.
- Durch Zugriffssteuerungslisten wird der Benutzerzugriff auf Informationen und Verarbeitungsressourcen gemäss der Identität des Benutzers und seiner Mitgliedschaft in verschiedenen vordefinierten Gruppen beschränkt. Die Zugriffssteuerung wird normalerweise von Systemadministratoren zur Steuerung des Zugriffs verwendet, den Benutzer auf Netzwerkressourcen wie Server, Verzeichnisse und Dateien erhalten. Dies wird häufig durch die Vergabe von Berechtigungen zum Zugriff auf bestimmte Objekte an den Benutzer implementiert.
- Mit der einmaligen Anmeldung kann der Benutzer sich einmalig mit einem einzigen Kennwort bei der Windows-Domäne anmelden und sich anschliessend bei jedem Computer in der Windows-Domäne authentifizieren. Durch die einmalige Anmeldung können Administratoren die Kennwortauthentifizierung im Windows-Netzwerk implementieren und gleichzeitig den Benutzern einen einfachen Zugriff zur Verfügung stellen.

Die folgenden Abschnitte enthalten ausführlichere Beschreibungen dieser wichtigen Funktionen.

Authentifizierung

Die Authentifizierung ist ein wesentlicher Aspekt der Systemsicherheit. Sie wird zum Bestätigen der Identität der Benutzer verwendet, die sich bei einer Domäne anmelden oder auf Netzwerkressourcen zugreifen möchten. In den meisten Authentifizierungssystemen stellt das Kennwort des Benutzers das schwächste Glied dar.
Kennwörter stellen die erste Verteidigungsstufe gegen nicht autorisierte Zugriffe auf die Domäne und auf lokale Computer dar. Empfehlen Sie die folgenden bewährten Methoden bezüglich Kennwörtern:

- Verwenden Sie immer sichere Kennwörter.
- Wenn Kennwörter auf Papier notiert werden müssen, lagern Sie das Papier an einem sicheren Ort, und vernichten Sie es, wenn es nicht mehr benötigt wird.
- Teilen Sie Kennwörter niemals mit anderen Personen.
- Verwenden Sie für alle Benutzerkonten unterschiedliche Kennwörter.
- Ändern Sie Kennwörter in regelmässigen Abständen.
- Gehen Sie beim Auswählen eines Speicherortes für Kennwörter auf einem Computer vorsichtig vor.

Sichere Kennwörter

Die Rolle von Kennwörtern beim Absichern des Netzwerks einer Organisation wird häufig unterschätzt und übersehen. Wie bereits erwähnt, bieten Kennwörter die erste Verteidigungsstufe gegen nicht autorisierte Zugriffe auf das Netzwerk. Daher sollten Sie sicherstellen, dass der Kunde von allen Mitarbeitern die Verwendung sicherer Kennwörter verlangt.

Tools zum Entschlüsseln von Kennwörtern werden jedoch fortlaufend verbessert, und die Computer, mit denen Kennwörter entschlüsselt werden, sind leistungsfähiger denn je. Mit genügend Zeit kann über ein automatisiertes Tool zum Entschlüsseln von Kennwörtern jedes Kennwort ermittelt werden. Sichere Kennwörter sind dennoch wesentlich schwieriger zu entschlüsseln als unsichere Kennwörter.

Richtlinien zum Erstellen sicherer Kennwörter, die sich der Benutzer merken kann, finden Sie unter

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

und

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

Festlegen der Kennwortrichtlinie

Wenn Sie dem Kunden beim Festlegen der Kennwortrichtlinie helfen, achten Sie darauf, eine Richtlinie zu erstellen, nach der alle Benutzerkonten sichere Kennwörter aufweisen müssen. Für die meisten Systeme ist es ausreichend, die Empfehlungen im Handbuch *Windows Server 2003 Security Guide* zu befolgen:

- Legen Sie die Richtlinieneinstellung **Kennwortchronik erzwingen** so fest, dass mehrere vorherige Kennwörter gespeichert werden. Mit dieser Richtlinieneinstellung können Benutzer nicht dasselbe Kennwort verwenden, wenn das Kennwort abläuft.

  Empfohlene Einstellung: 24.

- Legen Sie die Richtlinieneinstellung **Maximales Kennwortalter** so fest, dass Kennwörter so häufig ablaufen, wie dies für die Umgebung des Kunden erforderlich ist.

  Empfohlene Einstellung: zwischen 42 (Standard) und 90.

- Legen Sie die Richtlinieneinstellung **Minimales Kennwortalter** so fest, dass Kennwörter nicht geändert werden können, bevor sie eine bestimmte Anzahl von Tagen alt sind. Diese Richtlinieneinstellung funktioniert in Verbindung mit der Richtlinieneinstellung **Kennwortchronik erzwingen**. Wenn ein Mindestalter festgelegt ist, können Benutzer ihre Kennwörter nicht wiederholt ändern, um die Richtlinieneinstellung **Kennwortchronik erzwingen** zu umgehen und dann wieder das alte Kennwort zu verwenden. Benutzer müssen die angegebene Anzahl von Tagen warten, bevor sie das Kennwort ändern können.

  Empfohlene Einstellung: 2.

- Legen Sie die Richtlinieneinstellung **Minimale Kennwortlänge** so fest, dass Kennwörter mindestens aus einer bestimmten Anzahl von Zeichen bestehen müssen. Lange Kennwörter mit sieben oder mehr Zeichen sind normalerweise sicherer als kurze. Mit dieser Richtlinieneinstellung können Benutzer keine leeren Kennwörter verwenden und müssen Kennwörter erstellen, die mindestens eine bestimmte Anzahl von Zeichen lang sind.

  Empfohlene Einstellung: 8.

- Aktivieren Sie die Richtlinieneinstellung **Kennwort muss Komplexitätsvoraussetzungen entsprechen**. Mit dieser Richtlinieneinstellung werden alle neuen Kennwörter geprüft, um sicherzustellen, dass sie grundlegenden Anforderungen für sichere Kennwörter erfüllen. Durch diese Einstellung wird sichergestellt, dass Kennwörter mindestens drei Symbole aus den vier Kategorien (Grossbuchstaben, Kleinbuchstaben, Ziffern, nicht alphanumerische Symbole) enthalten und dass keine Teile des Benutzernamens oder des Vor- oder Nachnamens des Benutzers enthalten sind.

  Hinweis
  Kennwörter, die diese Anforderungen erfüllen, sind nicht notwendigerweise sehr sicher. Beispielsweise erfüllt das Kennwort **Kennwort1** diese Anforderungen.

  Empfohlene Einstellung: Ja.

- Eine vollständige Liste dieser Anforderungen finden Sie in der Onlinehilfe zu Windows Server unter „Kennwort muss Komplexitätsvoraussetzungen entsprechen“.

- **Kennwörter mit umkehrbarer Verschlüsselung speichern** – Umkehrbare Verschlüsselung wird auf Systemen eingesetzt, bei denen Anwendungen Zugriff auf Kennwörter im Klartext benötigen. In den meisten Bereitstellungen ist dies nicht erforderlich.

  Empfohlene Einstellung: Nein.

Weitere Informationen finden Sie im Handbuch *Windows Server 2003 Security Guide*:

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

Festlegen einer Kontosperrungsrichtlinie

Gehen Sie beim Festlegen der Kontosperrungsrichtlinie vorsichtig vor. Die Kontosperrungsrichtlinie sollte niemals in einem kleinen Unternehmen aktiviert werden, da sie auch zum Aussperren autorisierter Benutzer führen und somit hohe Kosten für den Kunden verursachen kann.

Wenn der Kunde sich für die Umsetzung der Kontosperrungsrichtlinie entscheidet, setzen Sie die Richtlinieneinstellung **Kontensperrungsschwelle** auf einen so hohen Wert, dass autorisierte Benutzer nicht aus ihren Benutzerkonten ausgesperrt werden, weil sie ihr Kennwort einige Male falsch eingegeben haben.

Weitere Informationen über die Kontosperrungsrichtlinie finden Sie in der Onlinehilfe zu Windows Server unter „Übersicht über Kontosperrungsrichtlinien“.

Informationen zum Anwenden oder Ändern von Kontosperrungsrichtlinien finden Sie in der Onlinehilfe zu Windows Server unter „So wenden Sie Kontosperrungsrichtlinen an oder ändern sie“.

Zugriffssteuerung

Ein Windows-Netzwerk kann mit seinen Ressourcen (einschliesslich Navision) gesichert werden, indem die Rechte von Benutzern, Benutzergruppen und anderen Computern im Netzwerk berücksichtigt werden. Sie können einen Computer oder mehrere Computer absichern, indem Sie Benutzern oder Gruppen bestimmte Benutzerrechte gewähren. Sie können ein Objekt absichern, z. B. eine Datei oder einen Ordner, indem Sie Berechtigungen zuweisen, mit denen Benutzer oder Gruppen bestimmte Aktionen mit diesem Objekt ausführen können. Zu den wichtigsten Konzepten der Zugriffssteuerung gehören die folgenden:

- Berechtigungen
- Besitz von Objekten
- Vererbung von Berechtigungen
- Benutzerrechte
- Objektüberwachung

Berechtigungen

Durch Berechtigungen werden die Zugriffsarten definiert, die ein Benutzer oder eine Gruppe für ein Objekt oder eine Objekteigenschaft hat, z. B. Dateien, Ordner oder Registrierungsobjekte. Berechtigungen werden auf alle sicheren Objekte angewendet, z. B. Dateien oder Registrierungsobjekte. Berechtigungen können beliebigen Benutzern, Gruppen oder Computern zugewiesen werden. Eine gute Methode ist die Zuweisung von Berechtigungen an Gruppen.

Besitz von Objekten

Einem Objekt wird bei Erstellung ein Besitzer zugewiesen. In der Standardeinstellung in Windows 2000 Server ist der Besitzer die Person, die das Objekt erstellt hat. Dies wurde in Windows Server 2003 für Objekte geändert, die von Mitgliedern der Administratorengruppe erstellt wurden.

Wenn ein Mitglied der Administratorengruppe unter Windows Server 2003 ein Objekt erstellt, wird die Administratorengruppe der Besitzer und nicht das einzelne Konto, mit dem das Objekt erstellt wurde. Dieses Verhalten kann über das MMC-Snap-In (Microsoft Management Console) Lokale Sicherheitseinstellungen über die Einstellung **Systemobjekte: Standardbesitzer für Objekte, die von Mitgliedern der Administratorengruppe erstellt werden** geändert werden. Der Besitzer eines Objekts kann immer die Berechtigungen des Objekts ändern. Dabei ist es gleichgültig, welche Berechtigungen zuvor festgelegt waren.

Weitere Informationen finden Sie in der Onlinehilfe zu Windows Server unter „Besitzrechte“.

Vererbung von Berechtigungen

Mithilfe der Vererbung können Administratoren Berechtigungen einfach zuweisen und verwalten. Durch diese Funktion erben Objekte in einem Container automatisch alle vererbbaren Berechtigungen dieses Containers. Wenn Sie beispielsweise Dateien in einem Ordner erstellen, erben diese die Berechtigungen des Ordners. Es werden nur die Berechtigungen vererbt, die entsprechend markiert sind.

Benutzerrechte

Durch Benutzerrechte werden bestimmte Berechtigungen und Anmelderechte an Benutzer und Gruppen in der Computerumgebung vergeben.

Weitere Informationen über Benutzerrechte finden Sie in der Onlinehilfe zu Windows Server unter „Benutzerrechte“.

Objektüberwachung

Sie können den Zugriff auf Objekte durch Benutzer überwachen. Anschliessend können Sie diese sicherheitsbezogenen Ereignisse mit der Ereignisanzeige im Sicherheitsprotokoll anzeigen.

Weitere Informationen finden Sie in der Onlinehilfe zu Windows Server unter „Überwachungsrichtlinie“.

Bewährte Methoden zur Zugriffssteuerung

- Weisen Sie Berechtigungen an Gruppen und nicht an Benutzer zu. Da die direkte Verwaltung von Benutzerkonten ineffizient ist, sollten Berechtigungen nur in Ausnahmefällen auf Benutzerbasis zugewiesen werden.
- Verwenden Sie in bestimmten Sonderfällen die Ablehnung von Berechtigungen. Beispielsweise können Sie durch Ablehnung von Berechtigungen einen Teil einer Gruppe ausschliessen, die über genehmigte Berechtigungen verfügt.
- Verweigern Sie der Gruppe **Jeder** niemals den Zugriff auf ein Objekt. Wenn der Gruppe **Jeder** Berechtigungen für ein Objekt verweigern, schliesst das auch die Administratoren ein. Eine bessere Lösung besteht im Entfernen der Gruppe **Jeder** und dem anschliessenden Zuweisen von Berechtigungen für dieses Objekt an Benutzer, Gruppen und Computer. Bedenken Sie, dass kein Zugriff zugelassen wird, wenn keine Berechtigungen festgelegt sind.
- Weisen Sie Berechtigungen für ein Objekt so hoch in der Struktur wie möglich zu, und verteilen Sie dann die Sicherheitseinstellungen mithilfe der Vererbung in der Struktur. Sie können Zugriffssteuerungseinstellungen schnell und effektiv für alle untergeordneten Elemente oder eine untergeordnete Struktur eines übergeordneten Objekts übernehmen. Dadurch erhalten Sie die umfassendsten Auswirkungen mit dem geringsten Aufwand. Die eingerichteten Berechtigungseinstellungen sollten für den Grossteil der Benutzer, Gruppen und Computer angemessen sein.

- Ausdrückliche Berechtigungen können mitunter vererbte Berechtigungen ausser Kraft setzen. Mit vererbten abgelehnten Berechtigungen wird der Zugriff auf ein Objekt nicht verhindert, sofern das Objekt über ausdrückliche zugelassene Berechtigungen verfügt. Ausdrückliche Berechtigungen haben vor vererbten Berechtigungen Vorrang, selbst vor vererbten abgelehnten Berechtigungen.
- Bezüglich der Berechtigungen von Active Directory®-Objekten sollten Sie sichergehen, dass Sie mit den bewährten Methoden für Active Directory-Objekte vertraut sind.

Weitere Informationen finden Sie in der Onlinehilfe zu Windows Server 2003 unter „Empfehlungen zum Zuweisen von Berechtigungen für Active Directory-Objekte“.

Externe Sicherheitsfirewall

Eine Firewall ist ein Hardware- oder Softwareelement, das das Eindringen oder Verlassen von Datenpaketen in einem bestimmten Netzwerk verhindert. Zur Steuerung des Datenflusses werden Anschlüsse in der Firewall für Informationspakete geöffnet oder geschlossen. Die Firewall berücksichtigt in jedem Datenpaket mehrere Informationen: das Protokoll, über das das Paket transportiert wird, das Ziel oder der Absender des Pakets, die Art des Inhalts des Pakets sowie die Anschlussnummer, an die es gesendet wird. Wenn die Firewall zum Akzeptieren des angegebenen Protokolls über den Zielanschluss konfiguriert ist, wird das Paket zugelassen. Microsoft Windows Small Business Server 2003 Premium Edition wird mit Microsoft Internet Security and Acceleration (ISA) Server 2000 als Firewalllösung geliefert. Small Business Server Standard Edition enthält ebenfalls eine Firewall.

ISA Server 2004

Internet Security and Acceleration (ISA) Server 2000 leitet Anforderungen und Antworten sicher zwischen dem Internet und Clientcomputern im internen Netzwerk weiter.

ISA Server dient Clients im lokalen Netzwerk als sicheres Gateway zum Internet. Der ISA Server-Computer ist für die anderen Beteiligten im Kommunikationspfad transparent. Der Internetbenutzer sollte einen Firewallserver nicht erkennen können, es sei denn, er versucht auf einen Dienst zuzugreifen oder eine Site zu besuchen und dieser Zugriff wird vom ISA Server-Computer verweigert. Der Internetserver, auf den zugegriffen wird, interpretiert die Anforderungen des ISA Server-Computers, als ob die Anforderungen von der Clientanwendung stammen würden.

Wenn Sie die Filterung von IP-Fragmenten (Internet Protocol) wählen, aktivieren Sie die Filterung von Paketfragmenten durch die Webproxy- und Firewalldienste. Bei der Filterung von Paketfragmenten werden alle fragmentierten IP-Pakete verworfen. Eine bekannte Angriffsmethode besteht im Senden von fragmentierten Paketen und der anschliessenden Zusammensetzung derart, dass das System geschädigt werden kann.

ISA Server bietet einen Eindringversuchserkennungs-Mechanismus, bei dem der Zeitpunkt eines Angriffs auf das Netzwerk erkannt und eine Reihe von konfigurierten Aktionen (oder Alarmen) durchgeführt werden.

Wenn Internetinformationsdienste (IIS) auf dem ISA Server-Computer installiert sind, müssen Sie diese so konfigurieren, dass keine Anschlüsse verwendet werden, die ISA Server für ausgehende Webanforderungen (Standard: 8080) und für eingehende Webanforderungen (Standard 80) verwendet. Beispielsweise können Sie IIS zur Überwachung von Anschluss 81 ändern und dann den ISA Server-Computer so konfigurieren, dass eingehende Webanforderungen an Anschluss 81 des lokalen Computers mit IIS weitergeleitet werden.

Wenn ein Konflikt zwischen Anschlüssen vorliegt, die von ISA Server und IIS verwendet werden, wird der IIS-Publishingdienst unterbrochen. Sie können dann IIS so ändern, dass ein anderer Anschluss überwacht wird, und den IIS-Publishingdienst anschliessend neu starten.

ISA Server-Richtlinien

Sie können eine ISA Server-Richtlinie festlegen, durch die eingehende und ausgehende Zugriffe gesteuert werden. Mit Site- und Inhaltsregeln wird angegeben, auf welche Sites und Inhalte zugegriffen werden kann. Protokollregeln zeigen an, ob ein bestimmtes Protokoll für die eingehende und ausgehende Kommunikation verfügbar ist.

Sie können Site- und Inhaltsregeln, Protokollregeln, Webveröffentlichungsregeln und IP-Paketfilter erstellen. Durch diese Richtlinien wird festgelegt, wie ISA Server-Clients mit dem Internet kommunizieren und welche Kommunikation zulässig ist.

Virenschutz

Ein Computervirus ist eine ausführbare Datei, die so entwickelt wurde, dass sie sich selbst repliziert, Dateien und Programme beschädigt oder löscht und nicht erkannt werden soll. Viren werden tatsächlich häufig neu geschrieben und angepasst, sodass sie nicht erkannt werden können. Viren werden oft als E-Mail-Anlagen gesendet. Antivirusprogramme müssen ständig aktualisiert werden, damit sie nach neuen und geänderten Viren suchen können. Viren sind die am weitesten verbreitete Methode des Computervandalismus.

Antivirussoftware wird speziell für die Erkennung und Unterbindung von Virusprogrammen entwickelt. Da ständig neue Virusprogramme erstellt werden, bieten viele Hersteller von Antivirusprodukten den Kunden regelmässige Aktualisierungen ihrer Software an. Microsoft empfiehlt die Implementierung von Antivirussoftware in der Umgebung des Kunden dringend.

Antivirussoftware wird normalerweise an diesen drei Orten installiert: auf den Arbeitsstationen der Benutzer, auf dem Server und in dem Netzwerk, in dem E-Mail die Organisation erreicht (und in einigen Fällen auch verlässt).

Arten von Viren

Es gibt drei Hauptarten von Viren, die Computersysteme infizieren können: Startsektorviren, Dateien infizierende Viren und Trojaner.

Startsektorviren

Beim Start eines Computers wird der Startsektor der Festplatte untersucht, bevor das Betriebssystem oder andere Startdateien geladen werden. Ein Startsektorvirus wurde so entwickelt, dass die Information im Startsektor der Festplatte durch eigenen Code ersetzt werden. Wenn ein Computer mit einem Startsektorvirus infiziert ist, wird der Code des Virus vor anderen Dateien in den Speicher geladen. Sobald sich der Virus im Speicher befindet, kann er sich auf andere Datenträger replizieren, die am infizierten Computer verwendet werden.

Dateien infizierende Viren

Hierbei handelt es sich um die häufigste Art Virus. Dateien infizierende Viren hängen sich an ausführbare Programmdateien an, indem sie der ausführbaren Datei ihren eigenen Code hinzufügen. Der Viruscode wird normalerweise so hinzugefügt, dass dies nicht erkannt wird. Wenn die infizierte Datei ausgeführt wird, kann der Virus sich an andere ausführbare Dateien anhängen. Mit dieser Art von Virus infizierte Dateien weisen normalerweise eine der Dateierweiterungen COM, EXE oder SYS auf.

Einige Dateien infizierende Viren wurden für bestimmte Programme entwickelt. Häufig angegriffene Programmtypen sind OVL- (Overlay) und DLL-Dateien (Dynamic Link Library). Obwohl diese Dateien nicht ausgeführt werden, können sie von ausführbaren Dateien aufgerufen werden. Der Virus wird beim Durchführen des Aufrufs übertragen.

Datenschäden treten auf, wenn der Virus ausgelöst wird. Ein Virus kann ausgelöst werden, wenn eine infizierte Datei ausgeführt wird oder wenn eine bestimmte Umgebungseinstellung zutrifft (z. B. ein bestimmtes Systemdatum).

Trojaner (Trojanische Pferde)

Ein Trojaner ist eigentlich kein Virus. Das Hauptunterscheidungsmerkmal zwischen einem Virus und einem Trojaner ist, dass ein Trojaner sich nicht repliziert. Er zerstört nur Informationen auf der Festplatte. Ein Trojaner stellt sich als legitimes Programm dar, z. B. als Spiel oder Dienstprogramm. Beim Ausführen kann er Daten zerstören oder unlesbar machen.

Bewährte Methoden zum Virenschutz

Die Verbreitung eines Makrovirus kann verhindert werden. Es folgen einige Tipps zum Vermeiden der Infizierung, die Sie Ihren Kunden mitteilen sollten:

- Installieren Sie eine Virusschutzlösung, die eingehende Nachrichten aus dem Internet auf Viren untersucht, bevor die Nachrichten den Router durchlaufen. Dadurch wird sichergestellt, dass E-Mails auf bekannte Viren untersucht werden.
- Machen Sie sich mit der Quelle empfangener Dokumente vertraut. Dokumente sollten nicht geöffnet werden, sofern sie nicht von einer Person stammen, die der Kunde als vertrauenswürdig einstuft.
- Reden Sie mit der Person, die das Dokument erstellt hat. Wenn die Benutzer nicht vollkommen überzeugt sind, dass das Dokument sicher ist, sollten Sie sich an die Person wenden, die das Dokument erstellt hat.
- Verwenden Sie den Makrovirusschutz von Microsoft Office. In Office geben die Anwendungen eine Warnung aus, wenn ein Dokument Makros enthält. Durch diese Funktion kann der Benutzer Makros beim Öffnen des Dokuments aktivieren oder deaktivieren.
- Verwenden Sie Virenscannersoftware, um Makroviren zu erkennen und zu entfernen. Virenscannersoftware kann Makroviren in Dokumenten erkennen und häufig aus diesen entfernen. Microsoft empfiehlt die Verwendung von Antivirussoftware, die von der International Computer Security Association (ICSA) zertifiziert wurde.

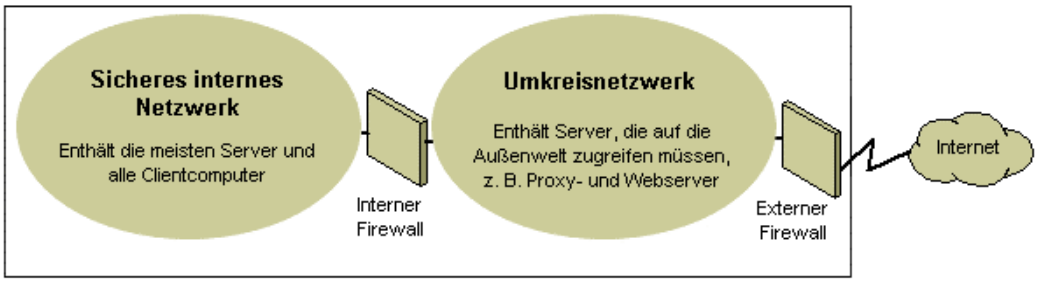
Weitere Informationen über Viren und allgemeine Computersicherheit finden Sie auf den folgenden Microsoft Security-Websites:

- Microsoft Security unter http://www.microsoft.com/security/default.asp.
- Sicherheitsdokumentation bei Microsoft TechNet unter http://www.microsoft.com/technet/security/Default.mspx.

Strategien zur Netzwerksicherheit

Da bei der Entwicklung einer IP-Internetarbeitsumgebung die Balance zwischen privaten und öffentlichen Netzwerkerwägungen hergestellt werden muss, ist die Firewall zu einem wesentlichen Element beim Schutz der Netzwerkintegrität geworden. Eine Firewall ist keine Einzelkomponente. Die National Computer Security Association (NCSA) definiert eine Firewall als „ein System oder eine Kombination aus Systemen, die eine Grenze zwischen zwei oder mehreren Netzwerken erzwingen“. Obwohl verschiedene Begriffe verwendet werden, wird diese Grenze häufig als Umkreisnetzwerk bezeichnet. Das Umkreisnetzwerk schützt Ihr Intranet oder Unternehmens-LAN (Local Area Network) vor Eindringlingen, indem der Zugriff aus dem Internet oder anderen grossen Netzwerken gesteuert wird.

Im folgenden Diagramm ist ein Umkreisnetzwerk dargestellt, das von Firewalls begrenzt und zwischen einem privaten Netzwerk und dem Internet platziert ist, um das private Netzwerk zu schützen.



Einfaches Umkreisnetzwerk

Organisationen unterscheiden sich in ihrer Herangehensweise an die Verwendung von Firewalls und die Bereitstellung von Sicherheit. IP-Paketfilterung bietet eine schwache Sicherheit, ist aufwendig in der Verwaltung und kann einfach umgangen werden. Anwendungsgateways sind sicherer als Paketfilter und einfacher zu verwalten, da sie sich nur auf einige bestimmte Anwendungen beziehen, z. B. ein spezifisches E-Mail-System. Kreisgateways sind am effektivsten, wenn der Benutzer einer Netzwerkanwendung grössere Bedeutung hat als die von dieser Anwendung ausgegebenen Daten. Der Proxyserver ist ein umfassendes Sicherheitstool, das ein Anwendungsgateway, sicheren Zugriff für anonyme Benutzer und weitere Dienste enthält. Es folgen einige Informationen über diese verschiedenen Optionen:

- **IP-Paketfilterung**
  Die IP-Paketfilterung war die erste Implementierung der Firewalltechnologie. Paketkopfzeilen werden auf Quell- und Zieladressen, TCP- (Transmission Control Protocol) und UDP-Anschlussnummern (User Datagram Protocol) und andere Informationen untersucht. Die Paketfilterung ist eine begrenzte Technologie, die am besten in Umgebungen mit klar strukturierter Sicherheit funktioniert, beispielsweise wenn die gesamte Umgebung ausserhalb des Umkreisnetzwerks als nicht vertrauenswürdig und die gesamte Umgebung innerhalb als vertrauenswürdig gilt. In den letzten Jahren wurde die Paketfilterungsmethode von verschiedenen Herstellern verbessert, indem dem Paketfilterungskern intelligente Entscheidungsfunktionen hinzugefügt wurden. Auf diese Weise wurde eine neue Form der Paketfilterung erstellt, die als *zustandsabhängige Protokolluntersuchung* bezeichnet wird. Sie können die Paketfilterung so konfigurieren, dass bestimmte Arten von Paketen akzeptiert und alle anderen abgelehnt werden, oder so, dass bestimmte Arten von Paketen abgelehnt und alle anderen akzeptiert werden.
- **Anwendungsgateways**
  Anwendungsgateways werden eingesetzt, wenn dem Inhalt einer Anwendung die grösste Bedeutung beigemessen wird. Ihre Anwendungsabhängigkeit ist zugleich ihre Stärke und ihre Beschränkung, da sie nicht problemlos an Änderungen in der Technologie angepasst werden können.
- **Kreisgateways**
  Kreisgateways sind Tunnel, die durch eine Firewall führen und bestimmte Prozesse oder Systeme auf der einen Seite mit bestimmten Prozessen oder Systemen auf der anderen verbinden. Kreisgateways werden am besten in Situationen eingesetzt, in denen die Person, die eine Anwendung verwendet, eine potentiell grössere Gefahr darstellt als die durch die Anwendung geführten Informationen. Das Kreisgateway unterscheidet sich von einem Paketfilter in der Möglichkeit, eine Verbindung zu einem Out-of-Band-Anwendungsschema herzustellen, über das weitere Informationen hinzugefügt werden können.

- **Proxyserver**
  Proxyserver sind umfassende Sicherheitstools, die Firewall- und Anwendungsgateway-Funktionen für die Verwaltung des Internet-Datenverkehrs zu und aus einem LAN enthalten. Proxyserver bieten auch Zwischenspeicherung von Dokumenten und Zugriffssteuerung. Mit einem Proxyserver kann die Leistung durch die Zwischenspeicherung und die direkte Weitergabe von häufig angeforderten Daten wie beliebten Webseiten verbessert werden. Ein Proxyserver kann auch Anforderungen filtern und verwerfen, die der Besitzer für nicht angemessen hält, z. B. Anforderungen zum nicht autorisierten Zugriff auf proprietäre Dateien.

Achten Sie darauf, dass der Kunde die Vorzüge aller Firewall-Sicherheitsfunktionen in Anspruch nimmt, die ihm helfen können. Platzieren Sie ein Umkreisnetzwerk in der Netzwerktopologie an einem Punkt, an dem sämtlicher Datenverkehr von ausserhalb des Unternehmensnetzwerks den durch die externe Firewall gebildeten Umkreis durchlaufen muss. Sie können die Zugriffssteuerung für die Firewall auf die Anforderungen des Kunden abstimmen und Firewalls so konfigurieren, dass alle nicht autorisierten Zugriffsversuche gemeldet werden.

Zum Minimieren der Anzahl von Anschlüssen, die in der inneren Firewall geöffnet sein müssen, können Sie eine Firewall auf Anwendungsebene wie ISA Server 2000 verwenden.

Weitere Informationen über TCP/IP finden Sie im Artikel „Designing a TCP/IP Network“ unter http://www.microsoft.com/resources/documentation/WindowsServ/2003/all/deployguide/en-us/dnsbb_tcp_overview.asp.

Drahtlose Netzwerke

In der Standardeinstellung sind drahtlose Netzwerke normalerweise so konfiguriert, dass die drahtlos gesendeten Signale abgefangen werden können. Sie können aufgrund der Standardeinstellungen bestimmter Drahtloshardware, der Zugriffsmöglichkeiten auf drahtlose Netzwerke und aktueller Verschlüsselungsmethoden gegenüber einem böswilligen Aussenstehenden verletzbar sein. Es gibt Konfigurationsoptionen und Tools, mit denen ein Schutz gegen das Abfangen der Daten hergestellt werden kann. Bedenken Sie jedoch, dass dabei kein Schutz vor Hackern und Viren gebildet wird, die über die Internetverbindung eindringen können. Daher ist es ausserordentlich wichtig, die Computer über eine Firewall vor unerwünschten Eindringlingen im Internet zu schützen.

Weitere Informationen finden Sie im Artikel „How to Make Your 802.11b Wireless Home Network More Secure“ unter http://support.microsoft.com/default.aspx?scid=kb;en-us;309369.

Netzwerksicherheitsszenarios

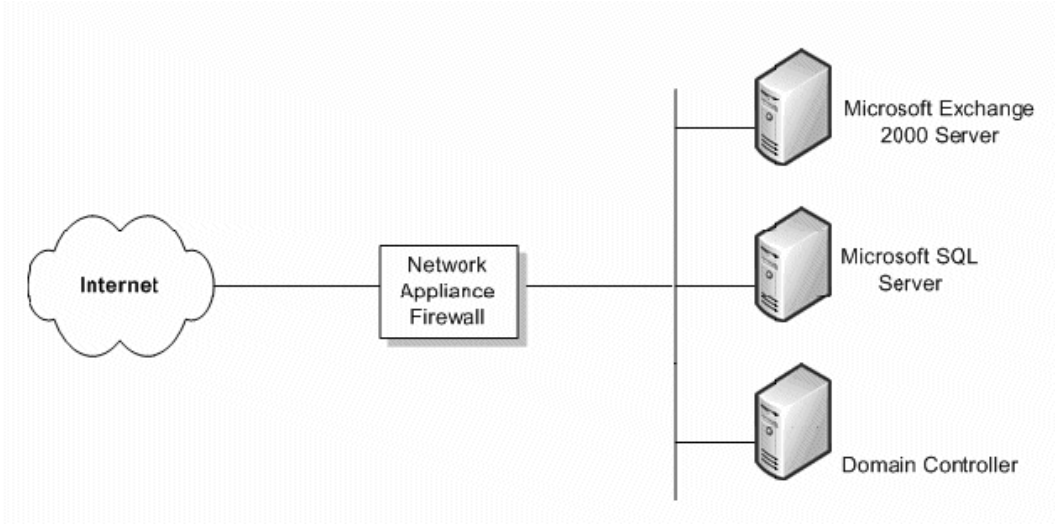
Der für die Organisation des Kunden erforderliche Grad an Netzwerksicherheit ist von verschiedenen Faktoren abhängig. Normalerweise wird ein Kompromiss zwischen den Kosten und dem Bedarf an Sicherheit für die Unternehmensdaten geschlossen. Es ist für ein kleines Unternehmen möglich, eine sehr komplexe Sicherheitsstruktur mit dem höchstmöglichen Grad an Netzwerksicherheit zu erzielen, jedoch kann ein kleines Unternehmen sich diese Sicherheit möglicherweise finanziell nicht leisten. In diesem Abschnitt werden vier Szenarios beschrieben und Empfehlungen für unterschiedliche Sicherheitsstufen zu jedem Szenario gegeben.

Keine Firewall

Wenn der Kunde über eine Verbindung mit dem Internet, jedoch nicht über eine Firewall verfügt, müssen einige Massnahmen für Netzwerksicherheit implementiert werden. Es gibt einfache Netzwerk-Firewallanwendungen, die genügend Sicherheit zum Abwehren der meisten unerfahrenen Hacker bieten.

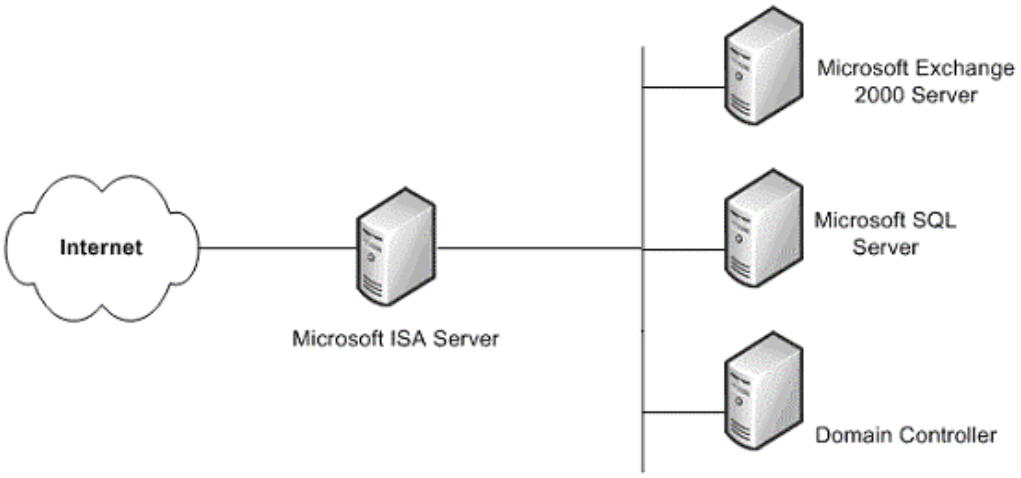
Eine einfache Firewall

Der geringste empfohlene Grad an Sicherheit ist eine einzelne Firewall zwischen dem Internet und den Daten des Kunden. Diese Firewall bietet eventuell keine erweiterte Sicherheit und sollte nicht als ausgesprochen sicher betrachtet werden. Sie ist jedoch einer Lösung ohne Firewall vorzuziehen.



Einfache Firewall

Es ist wünschenswert, dass die finanziellen Möglichkeiten des Kunden eine Lösung mit höherer Sicherheit für den Schutz der Unternehmensdaten ermöglichen. Eine solche Lösung ist ISA Server. Mit den höheren Kosten dieses zusätzlichen Servers steht eine wesentlich bessere Sicherheit als über die durchschnittliche Endbenutzerfirewall zur Verfügung, die häufig nur Netzwerkadressübersetzung (NAT) und Paketfilterung bietet.



ISA Server-Firewall

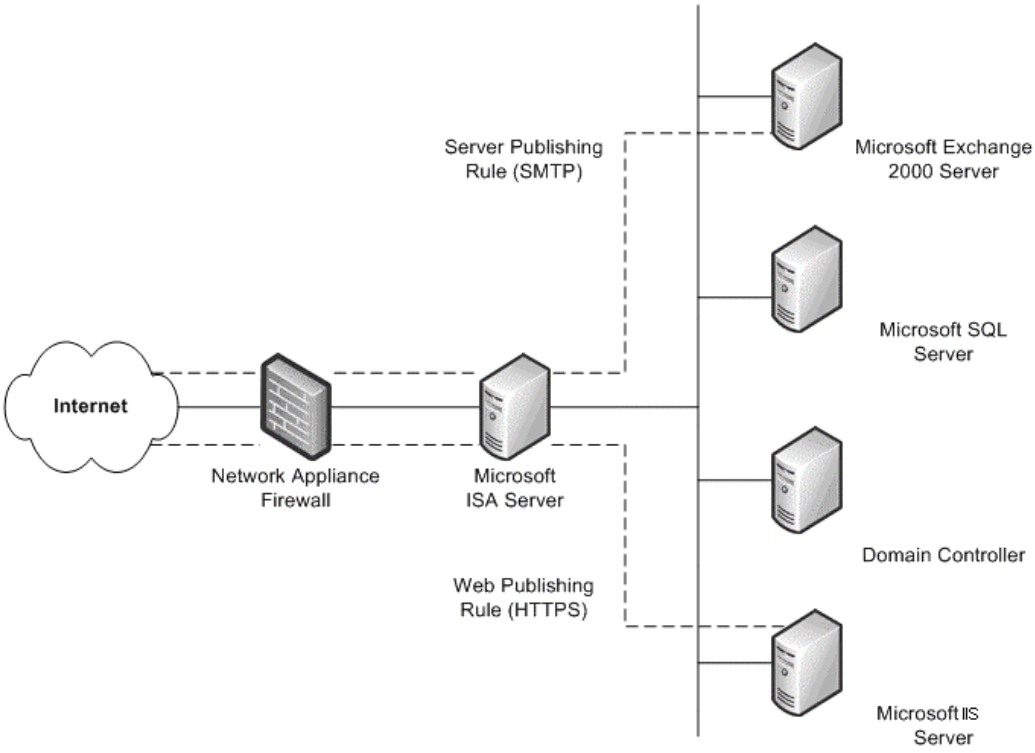
Diese Lösung mit einer einzelnen Firewall ist sicherer als eine einfache Firewallanwendung und bietet Windows-spezifische Sicherheitsdienste.

Eine vorhandene Firewall

Wenn der Kunde bereits über eine Firewall verfügt, die das Intranet vom Internet trennt, sollten Sie eine zusätzliche Firewall in Erwägung ziehen, die mehrere Möglichkeiten zum Konfigurieren der internen Ressourcen an das Internet bietet.

Eine solche Methode ist die Webveröffentlichung. Hierbei wird vor dem Webserver einer Organisation ein ISA-Server bereitgestellt, der den Zugriff für Internetbenutzer ermöglicht. Bei eingehenden Webanfragen kann ISA Server für die Aussenwelt einen Webserver darstellen, der Clientanforderungen nach Webinhalten aus seinem Cache erfüllt. ISA Server leitet Anforderungen nur dann an den Webserver weiter, wenn diese nicht aus dem Cache entnommen werden können.

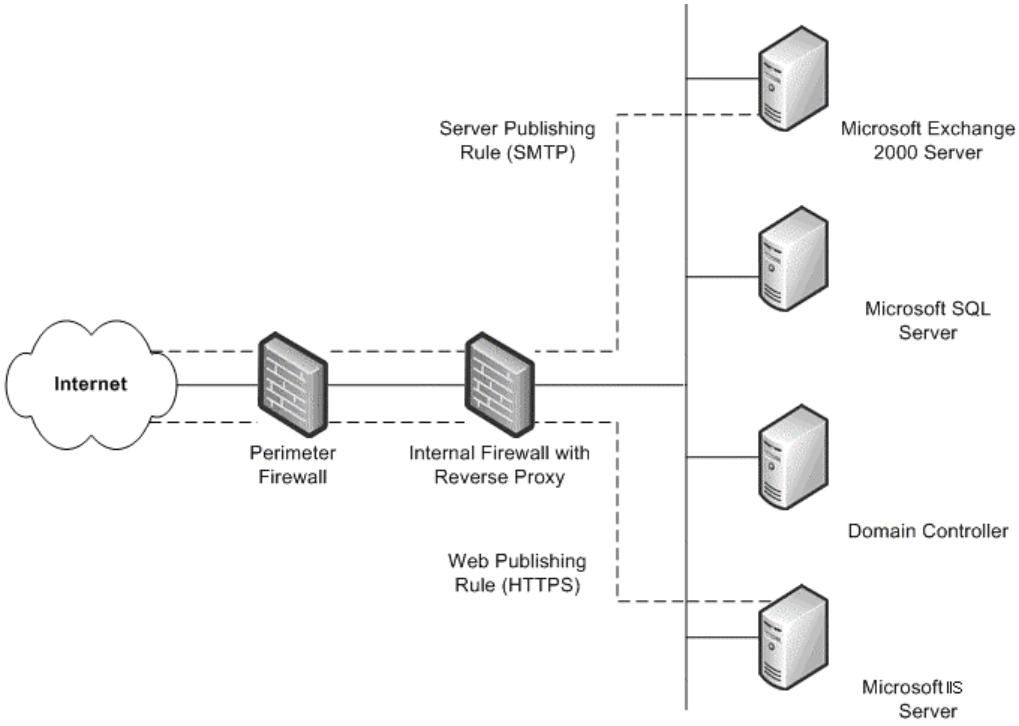
Eine weitere Methode ist die Serververöffentlichung. ISA Server ermöglicht die Veröffentlichung von internen Servern in das Internet, ohne die Sicherheit des internen Netzwerks zu beeinträchtigen. Sie können Webveröffentlichungs- und Serververöffentlichungsregeln konfigurieren, durch die festgelegt wird, welche Anforderungen an einen Server im lokalen Netzwerk gesendet werden sollten. Dies stellt eine erweiterte Sicherheitsschicht für die internen Server dar.



Vorhandene Firewall mit zusätzlichem ISA-Server

Zwei vorhandene Firewalls

Im vierten Szenario verfügt eine Organisation über zwei eingerichtete Firewalls mit einem etablierten Umkreisnetzwerk (DMZ). Mindestens einer dieser Server bietet Reverseproxydienste, sodass Internetclients keinen direkten Zugriff auf das Intranet erhalten. Stattdessen fängt eine der Firewalls, vorzugsweise die interne, Netzwerkanforderungen für interne Server ab, untersucht diese Pakete und leitet sie dann anstelle des Internethosts weiter.



Zwei vorhandene Firewalls

Dieses Szenario ist dem vorhergehenden Szenario nach dem Hinzufügen der zweiten Firewall ähnlich. Der einzige Unterschied besteht darin, dass es sich bei der internen Firewall mit Unterstützung von Reverseproxy nicht um einen ISA-Server handelt. In diesem Szenario sollten Sie in enger Zusammenarbeit mit den Verwaltern jeder Firewall Serververöffentlichungsregeln erstellen, die der Sicherheitsrichtlinie entsprechen.

Sicherheitspatchverwaltung

Betriebssysteme und Anwendungen sind häufig ausserordentlich komplex. Sie können aus Millionen Zeilen von Code bestehen, der von verschiedenen Programmierern geschrieben wurde. Es ist von ausschlaggebender Bedeutung, dass die Software zuverlässig funktioniert und die Sicherheit oder Stabilität des IT-Netzwerks nicht beeinträchtigt. Zum Minimieren von Problemen werden Programme vor der Veröffentlichung ausführlich getestet. Da Angreifer jedoch fortlaufend nach Schwächen in der Software suchen, können nicht alle zukünftigen Angriffe vorhergesehen werden.

In vielen Organisationen stellt die Patchverwaltung einen Teil der allgemeinen Änderungs- und Konfigurationsverwaltungsstrategie dar. Unabhängig von der Art und Grösse der Organisation ist es jedoch wichtig, über eine gute Patchverwaltungsstrategie zu verfügen, selbst wenn die Organisation noch keine effektive Änderungs- und Konfigurationsverwaltung eingerichtet hat. Der grösste Teil erfolgreicher Angriffe gegen Computersysteme tritt in den Systemen auf, bei denen keine Sicherheitspatches installiert wurden.

Sicherheitspatches stellen für die meisten Organisationen eine Herausforderung dar. Sobald eine Schwäche in der Software erkannt wurde, verbreiten Angreifer normalerweise diese Informationen schnell innerhalb der Hackergemeinschaft. Wenn eine Schwäche in der eigenen Software auftritt, versucht Microsoft, so schnell wie möglich einen Sicherheitspatch zu veröffentlichen. Bis der Patch bereitgestellt wurde, kann die Sicherheit, auf die der Kunde sich verlässt und die er erwartet, schwerwiegend beeinträchtigt sein.

In der Navision-Umgebung müssen Sie sicherstellen, dass Ihre Kunden auf allen Systemen die aktuellen Sicherheitspatches installieren. Achten Sie darauf, dass der Kunde eine der von Microsoft zur Verfügung gestellten Technologien verwendet. Diese umfassen die folgenden:

- **Microsoft Sicherheitsbenachrichtigungsdienst**
  Der Sicherheitsbenachrichtigungsdienst ist eine E-Mail-Liste, in der Benachrichtigungen verteilt werden, sobald eine Aktualisierung verfügbar ist. Diese Benachrichtigungen dienen als wertvoller Teil einer vorausschauenden Sicherheitsstrategie. Sie sind auch auf der Website für TechNet-Produktsicherheitsbenachrichtigungen verfügbar: http://www.microsoft.com/technet/security/bulletin/notify.mspx.
- **Microsoft Automatische Updates**
  Windows kann Sicherheitsaktualisierungen automatisch auf Ihre Computer anwenden.
- **Microsoft Suchtool für Sicherheitsinformationen**
  Das Suchtool für Sicherheitsinformationen ist auf der Security Bulletin Service-Website verfügbar: http://www.microsoft.com/technet/security/current.aspx. Der Kunde kann auf der Grundlage des verwendeten Betriebssystems, der Anwendungen und der Service Packs ermitteln, welche Aktualisierungen erforderlich sind.

- **Microsoft Baseline Security Analyzer (MBSA)**
  Dieses grafische Tool steht auf der Microsoft Baseline Security Analyzer-Website zur Verfügung: http://www.microsoft.com/technet/security/tools/mbsahome.mspx. Dieses Tool vergleicht den aktuellen Status eines Computers mit einer von Microsoft verwalteten Liste von Aktualisierungen. MBSA führt auch einige grundlegende Sicherheitsprüfungen der Einstellungen für Kennwortsicherheit und -ablauf, der Richtlinien für Gastkonten und verschiedener anderer Bereiche durch. MBSA sucht ausserdem nach Schwachstellen in Microsoft Internetinformationsdienste (IIS), SQL Server™ 2000, Exchange 5.5, Exchange 2000 und Exchange Server 2003.
- **Microsoft Software Update Services (SUS)**
  Dieses Tool war zuvor als Windows Update Corporate Edition bekannt. Mit ihm können Unternehmen alle wichtigen Aktualisierungen und Sicherheits-Roll-up-Pakete (SPRs) auf lokalen Computern speichern, die auf der öffentlichen Windows Update-Website verfügbar sind. Dieses Tool funktioniert in Verbindung mit einer neuen Version der Clients für automatische Updates (AU) und bildet die Grundlage einer ausgereiften Strategie für automatische Downloads und Installationen. Zu den neuen AU-Clients gehört ein Client für die Betriebssysteme Windows 2000 und Windows Server 2003, mit dem gedownloadete Aktualisierungen automatisch installiert werden können. Weitere Informationen über Microsoft SUS finden Sie unter http://www.microsoft.com/windows2000/windowsupdate/sus/default.asp.
- **Microsoft Systems Management Server (SMS) Software Update Services Feature Pack**
  Das SMS Software Update Services Feature Pack enthält mehrere Tools, mit denen der Vorgang der unternehmensweiten Ausgabe von Softwareaktualisierungen vereinfacht werden soll. Die Tools umfassen ein Sicherheitsupdate-Inventurtool, ein Microsoft Office-Inventurtool für Aktualisierungen, den Assistenten zum Verteilen von Softwareaktualisierungen und ein SMS-Webberichtstool mit dem Webberichts-Add-In für Softwareaktualisierungen. Weitere Informationen über jedes Tools finden Sie unter http://www.microsoft.com/smserver/downloads/20/featurepacks/suspack/.

Besprechen Sie jedes dieser Tools mit den Kunden, und empfehlen Sie ihre Verwendung. Es ist sehr wichtig, Sicherheitsproblemen so schnell wie möglich zu begegnen und gleichzeitig die Stabilität der Umgebung aufrechtzuerhalten.

Sicherheitseinstellungen für SQL Server 2000

Da Navision auch unter SQL Server 2000 ausgeführt werden kann, müssen Sie Massnahmen zum Erhöhen der Sicherheit für die SQL Server 2000-Installation des Kunden ergreifen. Die folgenden Schritte tragen zum Erhöhen der Sicherheit von SQL Server bei:

- Stellen Sie sicher, dass die aktuellen Service Packs und Aktualisierungen für das Betriebssystem und SQL Server 2000 installiert werden. Die aktuellsten Informationen finden Sie auf der Microsoft Security-Website unter http://www.microsoft.com/security/default.asp.
- Stellen Sie für Sicherheit auf Dateisystemebene sicher, dass alle Daten und Systemdateien von SQL Server 2000 auf NTFS-Partitionen installiert werden. Die Dateien sollten über NTFS-Berechtigungen nur administrativen und Systembenutzern verfügbar gemacht werden. Dadurch wird ein Schutz vor Benutzern hergestellt, die auf diese Dateien zugreifen, während der Dienst **MSSQLSERVER** nicht ausgeführt wird.

- Verwenden Sie für den SQL Server 2000-Dienst (**MSSQLSERVER**) ein Domänenkonto mit geringen Berechtigungen wie **NT-Autorität\Netzwerkdienst** oder **Lokales System** (empfohlen). Dieses Konto sollte über minimale Recht in der Domäne verfügen, sodass ein Angriff auf den Server im Fall einer Sicherheitsbeeinträchtigung eingeschränkt (jedoch nicht verhindert) werden kann. Mit anderen Worten: Dieses Konto sollte nur Berechtigungen auf der Ebene eines lokalen Benutzers in der Domäne aufweisen. Wenn SQL Server 2000 über ein Domänenadministratorkonto ausgeführt wird, führt eine Beeinträchtigung des Servers zu einer Beeinträchtigung der gesamten Domäne. Ändern Sie diese Einstellung mit SQL Server Enterprise Manager. Die Zugriffssteuerungslisten (ACLs) für Dateien, die Registrierung und Benutzerrechte werden automatisch geändert.
- Die meisten Editionen von SQL Server 2000 werden mit zwei Standarddatenbanken installiert: **Northwind** und **pubs**. Beide Datenbanken stellen Beispiele für Tests, Schulungen und als allgemeine Beispiele dar. Sie sollten nicht auf einem Produktionssystem bereitgestellt werden. Wenn ein böswilliger Benutzer weiss, dass diese Datenbanken vorhanden sind, kann er versuchen, die Standardeinstellungen und die Standardkonfiguration für Angriffe zu nutzen. Wenn **Northwind** und **pubs** auf dem SQL Server 2000-Produktionscomputer vorhanden sind, sollten sie entfernt werden.
- Die Überwachung des SQL Server 2000-Systems ist in der Standardeinstellung deaktiviert, sodass keine Bedingungen überwacht werden. Dadurch gestaltet sich die Erkennung von Eindringversuchen schwierig, und Angreifer können ihre Spuren verdecken. Sie sollten mindestens die Überwachung von fehlgeschlagenen Anmeldungen aktivieren.

Die aktuellsten Sicherheitsinformationen zu SQL Server 2000 finden Sie unter http://www.microsoft.com/sql/techinfo/administration/2000/security/default.asp.

Informationen über Microsoft Business Solutions

Microsoft Business Solutions ist ein Geschäftsbereich von Microsoft und bietet viele integrierte End-to-End-Geschäftsanwendungen und -dienste an, die kleinen, mittelgrossen und grossen Unternehmen dabei helfen, engere Bindungen zu Kunden, Mitarbeitern, Partnern und Lieferanten zu entwickeln. Mit den Anwendungen von Microsoft Business Solutions werden strategische Geschäftsvorgänge über Finanzverwaltung, Analyse, Mitarbeiterverwaltung, Projektleitung, Kundenbeziehungsmanagement, Kundendienstleistungs-verwaltung, Lieferkettenverwaltung, E-Commerce, Herstellung und Einzelhandelsmanagement optimiert. Die Anwendungen wurden entwickelt, um Kunden durch tiefgreifende Informationen zum Geschäftserfolg zu verhelfen. Weitere Informationen über Microsoft Business Solutions finden Sie unter http://www.microsoft.com/BusinessSolutions/.