Microsoft Business Solutions

Navision Security Hardening Guide

Data di pubblicazione: ottobre 2004

Microsoft

Sommario

Introduzione

Microsoft® Windows® offre una protezione di rete sofisticata basata su standard. Nel senso più ampio del termine, protezione significa pianificazione e considerazione delle conseguenze. Si supponga che un computer venga chiuso in una camera blindata a cui possa accedere solo un amministratore di sistema. Il computer risulta protetto, ma non è molto utile perché non è connesso a nessun altro computer. È quindi necessario considerare le modalità per ottenere la massima protezione della rete senza sacrificarne l'usabilità.

La maggior parte delle organizzazioni si prepara ad affrontare attacchi esterni installando firewall, ma molti non pensano a come affrontare una violazione della protezione quando un utente malintenzionato ha superato il firewall. Le misure di protezione nell'ambiente del cliente funzionano bene se agli utenti non viene chiesto di osservare troppe procedure e regole per lavorare in modo sicuro. L'implementazione dei criteri di protezione dovrebbe essere il più semplice possibile per gli utenti, altrimenti essi tenderanno a trovare modi meno sicuri per fare le cose.

Poiché la dimensione delle installazioni Navision può variare di molto, è importante considerare attentamente le necessità di ogni cliente e soppesare l'efficacia della protezione a fronte dei costi da sostenere. In qualità di consulente in cui il cliente ripone la propria fiducia, occorre utilizzare il buon senso e consigliare una soluzione che soddisfi le necessità di protezione senza creare un onere che potrebbe indurre il cliente a smettere di applicare i criteri di protezione.

Procedure consigliate per la protezione di Navision

Le regole generali illustrate di seguito possono aiutare a migliorare la protezione dell'ambiente Navision:

- Se si desidera eseguire Navision Database Server come servizio o utilizzare il parametro della riga di comando *installasservice* quando si avvia il server, accertarsi che il servizio sia eseguito come account NT Authority\Servizio di rete. L'account NT Authority\Servizio di rete esiste solo in Windows™ XP e Windows Server™ 2003. Se il sistema operativo è Windows 2000 Server, occorre creare un account con privilegi minimi, altrimenti il servizio verrà assegnato a un account Sistema locale. Tale account dovrebbe avere al massimo gli stessi privilegi del normale account Users oppure essere un account di dominio che non sia un amministratore né del dominio, né di alcun computer locale.

  Ricordare di assegnare l'account NT Authority\Servizio di rete o l'account utente eseguito dal server con l'accesso in lettura e scrittura al file di database per consentire agli utenti di connettersi al database.

  Per assegnare all'account NT Authority\Servizio di rete i diritti di lettura e scrittura per un file di database in Windows XP:

  1. In Esplora risorse passare alla cartella contenente il file di database.
  2. Selezionare il file di database, fare clic con il pulsante destro del mouse su di esso e scegliere Proprietà.
  3. Nella finestra ***Proprietà*** fare clic sulla scheda ***Protezione*** e sotto il campo **Nomi di utenti o gruppi** scegliere Aggiungi.
  4. Nella finestra ***Seleziona utenti, computer o gruppi*** immettere *Servizio di rete* e scegliere OK.
  5. SERVIZIO DI RETE è stato aggiunto al campo **Nomi di utenti o gruppi** nella finestra ***Proprietà***.
  6. Selezionare SERVIZIO DI RETE e nel campo **Autorizzazioni** selezionare *Lettura* e *Scrittura*.
- Il servizio Navision Application Server viene eseguito come account NT Authority\Servizio di rete per impostazione predefinita e questo consente di accedere a Navision Database Server a livello locale. È tuttavia necessario che il servizio Navision Application Server sia eseguito come account di dominio Windows riconosciuto da Navision Database Server se si desidera accedere al server di database. Tale account non dovrebbe essere un amministratore né del dominio, né di alcun computer locale.
- Se si esegue l'Opzione SQL Server per Navision, Microsoft SQL Server™ viene eseguito come servizio. L'Opzione SQL Server per Navision richiede che SQL Server sia in grado di cercare in Active Directory gli elenchi dei gruppi di utenti Windows a scopo di autenticazione. È quindi necessario verificare che il servizio SQL Server sia eseguito come account NT Authority\Servizio di rete.

  Per verificare che il servizio sia eseguito come NT Authority\Servizio di rete:

  1. Sul computer SQL Server individuare il servizio MSSQLSERVER, fare clic con il pulsante destro del mouse su di esso e scegliere Proprietà.
  2. Nella finestra ***Proprietà*** fare clic sulla scheda ***Connessione***.
  3. Nella scheda ***Connessione***, sotto Connessione, fare clic su Account, immettere *NT Authority\Servizio di rete* e scegliere OK.

Per ulteriori informazioni sulla protezione di SQL Server visitare i siti ai seguenti indirizzi (informazioni in lingua inglese):

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

e

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

- Se si esegue un prodotto Navision di commercio elettronico come Commerce Gateway, accertarsi che Commerce Gateway Request Server sia stato installato correttamente con l'impostazione dell'account predefinito per i servizi. L'impostazione dell'account predefinito è denominata *CGRSUser* e consente l'accesso di Commerce Gateway Server al set minimo degli altri servizi necessari, inclusi il servizio *MSSQLSERVER* e *BizTalk Service BizTalk Group : BizTalkServerApplication* e non include impostazioni di account globali previste invece con l'account *Sistema locale*.
- Utilizzare sempre password complesse. Per ulteriori informazioni sulle password complesse, consultare la sezione Password complesse.
- Utilizzare i login Windows. Navision consente di creare due tipi di login: login Database e login Windows. Si consiglia di utilizzare i login Windows perché, grazie all'autenticazione Windows, consentono di applicare criteri di password appropriati.
- Le password non dovrebbero essere riutilizzate. È una pratica comune riutilizzare le password nei sistemi e nei domini. Un amministratore responsabile di due domini, ad esempio, potrebbe creare in entrambi degli account di amministratore di dominio che utilizzino la stessa password e impostare le password degli amministratori locali sui computer di dominio che siano uguali nel dominio. In questo caso, la violazione di un solo account o computer può compromettere l'intero dominio.
- Dopo l'installazione di Navision e la creazione o l'aggiornamento dei database, occorre creare un login Windows e assegnarvi il ruolo SUPER in Navision. Tale utente SUPER potrà gestire i database, la protezione e così via. Assegnare a questo login una password complessa. La password dovrebbe rimanere riservata e dovrebbe avere la stessa protezione della password SA in SQL Server. Tutti gli accessi al database sono gestiti dal ruolo SUPER, che richiede il massimo livello di protezione. La password dell'utente SUPER dovrebbe essere nota solo agli amministratori di sistema.
- Tutti gli altri utenti che hanno accesso al database di Navision dovrebbero avere i privilegi minimi. Questo significa che occorre assegnare loro dei ruoli in Navision che consentano l'accesso solo alle funzionalità necessarie per eseguire le loro attività nell'azienda.
- Accertarsi che solo gli utenti il cui ruolo nell'azienda lo richieda siano in grado di importare file FOB, di ridisegnare oggetti o creare e ripristinare i backup del database.
- Effettuare backup regolari del database di Navision e ricordare di testare i backup per verificare che possano essere ripristinati correttamente.
- Archiviare i backup in un luogo sicuro per limitare l'impatto dei rischi provocati da incendi, fumo, polvere, alte temperature, lampi e disastri ambientali, ad esempio un terremoto.
- Sebbene Navision possa essere installato su diverse versioni di Windows, si consiglia di utilizzare i sistemi operativi più recenti con le funzionalità di protezione più avanzate, che attualmente corrispondono a Windows XP Service Pack 2 e Windows Server 2003.
- Utilizzare il servizio Windows Update fornito con Windows 2000, Windows XP e Windows Server 2003 per applicare gli aggiornamenti più recenti relativi alla protezione. Utilizzare la funzionalità Aggiornamenti automatici di Windows per garantire che tutti i computer client siano sempre aggiornati con le patch di protezione e i service pack più recenti.

- Si consiglia di utilizzare il protocollo protetto TCPS per la comunicazione tra i client Navision e Navision Database Server. TCPS è una versione protetta di TCP/IP e utilizza l'interfaccia SSPI (Security Support Provider Interface) con crittografia abilitata e autenticazione Kerberos. TCPS è il protocollo predefinito per Navision Database Server.
- Il cliente dovrebbe disporre di un piano di ripristino di emergenza che consenta una rapida ripresa dei servizi dopo un'emergenza. Un piano di ripristino dovrebbe includere i seguenti aspetti:
  - Acquisizione di attrezzature nuove o temporanee.
  - Ripristino dei backup sui nuovi sistemi.
  - Test di funzionamento del piano di ripristino.

Protezione fisica

La protezione fisica è assolutamente indispensabile, in quanto non esiste modo di sostituirla con la protezione software. Se ad esempio un disco rigido viene rubato, i dati che risiedono su quell'unità verranno alla fine rubati anch'essi. Mentre si discutono i criteri da implementare con il cliente, affrontare le seguenti problematiche relative alla protezione fisica:

- Per grandi installazioni con reparti IT dedicati, verificare che le stanze con i server e i luoghi in cui è archiviato il software siano chiusi a chiave.
- I computer in questa categoria comprendono:
  - Il server Microsoft SQL Server 2000.
  - Il file server in cui risiedono gli eseguibili di Navision.
- Vietare l'accesso ai computer agli utenti non autorizzati.
- Verificare che siano installati impianti d'allarme, indipendentemente dal grado di riservatezza dei dati.
- Accertarsi che i backup dei dati critici siano archiviati in siti esterni e in contenitori antincendio.

Gli impiegati

È consigliabile limitare i diritti amministrativi su tutti i prodotti e le funzionalità. Come impostazione predefinita, i clienti dovrebbero assegnare ai loro impiegati solo l'accesso in lettura per le funzioni di sistema, a meno che non abbiano necessità di privilegi maggiori per svolgere le loro mansioni. Microsoft suggerisce di applicare il principio del privilegio minimo: assegnare agli utenti solo i privilegi minimi indispensabili per accedere ai dati e alle funzionalità.
Gli ex impiegati o quelli insoddisfatti sono una minaccia alla sicurezza della rete. Mentre si discutono le caratteristiche della protezione con i clienti, suggerire i seguenti criteri relativi agli impiegati:

- Condurre delle indagini prima dell'assunzione.
- Aspettarsi delle "vendette" dagli ex dipendenti o dagli impiegati scontenti.
- Accertarsi che vengano disattivati tutti gli account Windows e le relative password di un dipendente che lascia l'impiego. Per consentire l'eventuale creazione di report, non eliminare alcun utente. Non riutilizzare gli account.

- Addestrare gli utenti a essere attenti e a segnalare le attività sospette.
- Non assegnare privilegi automaticamente. Accertarsi che gli utenti non abbiano accesso a computer, stanze o file non necessari.
- Addestrare i supervisori a identificare e affrontare potenziali problemi creati dagli impiegati.
- Accertarsi che gli impiegati capiscano il loro ruolo nella protezione della rete.
- Dare una copia dei criteri di protezione dell'azienda a ogni impiegato.
- Impedire agli utenti di installare software non autorizzato.

L'amministratore

Gli amministratori di sistema dei clienti dovrebbero avere sempre cura di implementare le correzioni di protezione più recenti rilasciate da Microsoft. Gli aggressori sono molto abili nel creare tanti piccoli bug per consentire intrusioni su larga scala nelle reti. Gli amministratori dovrebbero come prima cosa accertarsi che ogni singolo computer sia protetto nella massima misura possibile e in seguito applicare aggiornamenti della protezione e utilizzare software antivirus. In questa guida sono indicati numerosi collegamenti e risorse per trovare informazioni valide e procedure consigliate.

La complessità comporta un'altra conseguenza per la protezione della rete. Più è complessa la rete e più è difficile proteggerla o sanarla dopo che un intruso è riuscito a penetrarla. L'amministratore dovrebbe documentare accuratamente la topografia della rete, allo scopo di mantenerla il più semplice possibile.

Uno degli aspetti principali che riguarda la protezione è la gestione dei rischi. Poiché la sola tecnologia non è una panacea, la protezione richiede una combinazione di tecnologia e criteri. In altre parole, non è sufficiente disimballare e installare un prodotto sulla rete perché raggiunga immediatamente la perfetta protezione. La protezione è il risultato di tecnologia e criteri: in ultima analisi il livello di protezione di una rete è determinato dalle modalità di utilizzo della tecnologia. Microsoft rilascia tecnologia e funzionalità di cui la protezione è parte integrante, ma solo l'amministratore, con la guida del consulente, può decidere i criteri adatti per ciascuna organizzazione. Accertarsi di pianificare gli aspetti relativi alla protezione in uno stadio preliminare del processo di implementazione e distribuzione. Cercare di capire che cosa il cliente desidera proteggere e cosa è disposto a fare per proteggerlo.

Sviluppare infine dei piani per affrontare le emergenze prima che si verifichino. Una pianificazione completa unita a una solida tecnologia può garantire al cliente un'ottima protezione.

Per ulteriori informazioni sulla protezione in generale, vedere l'articolo "The Ten Immutable Laws of Security Administration" all'indirizzo: http://www.microsoft.com/technet/archive/community/columns/security/essays/10salaws.mspx (informazioni in lingua inglese) e gli articoli sulla gestione della protezione all'indirizzo: http://www.microsoft.com/technet/community/columns/secmgmt/smarch.mspx (informazioni in lingua inglese).

Protezione del sistema operativo del server

Nonostante molti piccoli clienti non dispongano di un sistema operativo server, è importante capire e riuscire a comunicare ai clienti con strutture più grandi le procedure consigliate per la protezione degli ambienti di rete più complessi. È inoltre bene sapere che molti dei criteri e delle procedure descritti in questo documento possono essere applicati facilmente ai clienti che dispongono solo di sistemi operativi client.

I concetti trattati in questa sezione sono applicabili a entrambi i prodotti Microsoft Windows 2000 Server e Microsoft Windows Server 2003, nonostante le informazioni siano tratte principalmente dalla Guida in linea di Windows Server 2003. Windows Server 2003 offre una corposa serie di funzionalità di protezione. La Guida in linea di Windows Server 2003 contiene informazioni complete su tutte le funzionalità e le procedure di protezione.

Per ulteriori informazioni su Windows 2000 Server, visitare il sito Windows 2000 Server Security Center all'indirizzo http://www.microsoft.com/technet/security/prodtech/win2000/default.mspx (informazioni in lingua inglese).

e leggere la Windows 2000 Security Hardening Guide all'indirizzo: http://www.microsoft.com/technet/security/prodtech/win2000/win2khg/default.mspx (informazioni in lingua inglese).

Per informazioni aggiuntive su Windows Server 2003, vedere la *Windows Server 2003 Security Guide* all'indirizzo http://www.microsoft.com/technet/security/prodtech/win2003/w2003hg/sgch00.mspx (informazioni in lingua inglese).

Le caratteristiche principali del modello di protezione del server Windows sono l'autenticazione, il controllo dell'accesso e il punto di accesso singolo:

- L'autenticazione è il processo con il quale il sistema convalida l'identità di un utente mediante le credenziali di accesso. Il nome e la password di un utente vengono confrontati con un elenco di utenti autorizzati. Se il sistema rileva una corrispondenza, all'utente viene concesso l'accesso con i privilegi specificati nell'elenco delle autorizzazioni per quell'utente.
- Il controllo dell'accesso limita l'accesso dell'utente alle informazioni o alle risorse in base all'identità dell'utente e alla sua appartenenza a gruppi predefiniti. Il controllo dell'accesso è tipicamente utilizzato dagli amministratori di sistema per controllare l'accesso degli utenti alle risorse di rete quali server, directory e file. Questo tipo di protezione viene in genere implementata concedendo l'accesso a oggetti specifici.
- Il punto di accesso singolo consente a un utente di accedere al dominio Windows una sola volta, utilizzando una sola password, e permette l'autenticazione in qualunque computer all'interno del dominio Windows. Il punto di accesso singolo consente agli amministratori di implementare l'autenticazione delle password sulla rete Windows facilitando al contempo l'accesso agli utenti finali.

Le sezioni seguenti contengono descrizioni più dettagliate di questi tre aspetti chiave.

Autenticazione

L'autenticazione è un aspetto fondamentale della protezione del sistema ed è utilizzata per confermare l'identità di chiunque tenti di accedere a un dominio o a risorse di rete. L'anello debole nella maggior parte dei sistemi di autenticazione è la password dell'utente.

Le password rappresentano la prima linea di difesa contro l'accesso non autorizzato al dominio e ai computer locali. Le procedure consigliate relative alle password sono le seguenti:

- Utilizzare sempre password complesse.
- Se occorre scrivere le password su un foglio di carta, riporre il foglio in un posto sicuro e distruggerlo quando non è più necessario.
- Non condividere mai le password con altri utenti.
- Utilizzare password diverse per tutti gli account utente.
- Cambiare le password a intervalli regolari.
- Scegliere con attenzione l'area del computer in cui vengono salvate le password.

Password complesse

Il ruolo rivestito dalle password nella protezione della rete di un'organizzazione viene spesso sottostimato e trascurato. Come menzionato in precedenza, le password rappresentano la prima linea di difesa contro l'accesso non autorizzato alla rete. È quindi necessario che i clienti istruiscano i propri impiegati sull'uso delle password complesse.

Gli strumenti per identificare le password, tuttavia, continuano a migliorare e i computer utilizzati per identificare le password sono sempre più potenti. Con sufficiente tempo a disposizione, uno strumento automatizzato è in grado di identificare qualunque password. Nondimeno le password complesse sono molto più difficili da identificare rispetto a quelle semplici.

Per istruzioni sulla creazione di password complesse che l'utente è in grado di ricordare, visitare i siti ai seguenti indirizzi (informazioni in lingua inglese):

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

e

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

Definizione dei criteri per le password

Durante l'assistenza al cliente per la definizione dei criteri per le password, assicurarsi di creare criteri che richiedano a tutti gli account utente l'utilizzo di password complesse.

Per la maggior parte dei sistemi è sufficiente seguire i consigli forniti nella Windows Server 2003 Security Guide:

- Definire l'impostazione del criterio **Imponi cronologia delle password**, in modo che parecchie password precedenti siano ricordate. Con l'impostazione di questo criterio, gli utenti non possono utilizzare la stessa password dopo la sua scadenza.

  Impostazione consigliata: 24

- Definire l'impostazione del criterio **Validità massima password**, in modo che le password scadano secondo la tempistica necessaria per l'ambiente del cliente.

  Impostazione consigliata: tra 42 (impostazione predefinita) e 90.

- Definire l'impostazione del criterio **Validità minima password**, in modo che le password non possano essere cambiate se non dopo un certo numero di giorni. Questo criterio funziona in combinazione con l'impostazione del criterio **Imponi cronologia delle password**. Se viene definita una validità minima delle password, gli utenti non possono cambiare ripetutamente le password per aggirare l'impostazione del criterio **Imponi cronologia delle password** e utilizzare le loro password originali. Gli utenti devono attendere il numero di giorni specificato per cambiare la password.

  Impostazione consigliata: 2

- Definire l'impostazione del criterio **Lunghezza minima password**, in modo che le password debbano essere composte come minimo dal numero di caratteri specificato. Le password lunghe, composte da sette o più caratteri, sono generalmente più sicure di quelle brevi. Grazie all'impostazione di questo criterio gli utenti non possono utilizzare password vuote e devono creare password formate da un certo numero di caratteri.

  Impostazione consigliata: 8

- Abilitare l'impostazione del criterio **Le password devono essere conformi ai requisiti di complessità**. Con questo criterio tutte le nuove password vengono controllate affinché soddisfino i requisiti di base delle password complesse. Questa impostazione verifica che le password contengano almeno tre simboli di quattro categorie (maiuscole, minuscole, numeri e simboli non alfanumerici) e non contengano alcuna parte del nome utente e del nome o del cognome dell'utente.

  Nota
  Le password che soddisfano questi requisiti non sono necessariamente complesse. La password “Password1”, ad esempio, soddisfa questi requisiti.

  Impostazione consigliata: Sì

- Per un elenco completo dei requisiti, consultare l'argomento "Le password devono essere conformi ai requisiti di complessità" nella Guida in linea di Windows Server.

- Archiviare le password mediante crittografia reversibile. La crittografia reversibile è utilizzata nei sistemi in cui un'applicazione deve accedere a password non crittografate. Nella maggior parte delle installazioni non è necessaria.

  Impostazione consigliata: No

Per ulteriori informazioni, consultare la Windows Server 2003 Security Guide all'indirizzo:

http://www.microsoft.com/technet/security/prodtech/Win2003/W2003HG/SGCH00.mspx
(informazioni in lingua inglese).

Definizione di un criterio di blocco account

Quando si definisce un criterio di blocco account occorre essere prudenti. Il criterio di blocco account non dovrebbe mai essere impostato in una piccola azienda poiché è molto probabile che blocchi utenti autorizzati, un fatto che potrebbe rivelarsi molto dispendioso per il cliente.

Se il cliente decide di applicare il criterio di blocco account, regolare l'impostazione del criterio **Limite di blocchi dell'account** su un numero sufficientemente alto per garantire che un utente autorizzato non sia escluso dal proprio account utente semplicemente perché ha digitato la password più volte in modo non corretto.

Per ulteriori informazioni sul criterio di blocco account, consultare l'argomento "Cenni preliminari sul criterio di blocco account" nella Guida in linea di Windows Server.

Per informazioni sull'applicazione o la modifica del criterio di blocco account, consultare l'argomento "Applicare o modificare il criterio di blocco account" nella Guida in linea di Windows Server.

Controllo dell'accesso

Una rete Windows e le sue risorse (incluso Navision) possono essere protette prendendo in considerazione i diritti di cui dispongono gli utenti, i gruppi di utenti e gli altri computer. La protezione di uno o più computer può essere implementata concedendo agli utenti o ai gruppi di utenti diritti specifici. È possibile proteggere un oggetto, ad esempio un file o una cartella, assegnando autorizzazioni che consentono agli utenti o ai gruppi di eseguire azioni specifiche su quell'oggetto. I concetti chiave relativi al controllo dell'accesso includono:

- Autorizzazioni
- Proprietà degli oggetti
- Ereditarietà delle autorizzazioni
- Diritti utente
- Controllo degli oggetti

Autorizzazioni

Le autorizzazioni definiscono il tipo di accesso consentito a un utente o a un gruppo per un oggetto o la proprietà di un oggetto, quali file, cartelle e oggetti del Registro di sistema. Le autorizzazioni sono applicate a qualunque oggetto protetto, quali i file o gli oggetti del Registro di sistema, e possono essere concesse a qualunque utente, gruppo o computer. È una buona abitudine assegnare le autorizzazioni ai gruppi.

Proprietà degli oggetti

Un proprietario viene assegnato a un oggetto nel momento in cui quest'ultimo viene creato. Per impostazione predefinita, in Windows 2000 Server il proprietario è il creatore dell'oggetto. Questa impostazione è stata modificata in Windows Server 2003 per gli oggetti creati dai membri del gruppo Administrators.

Quando un membro del gruppo Administrators crea un oggetto in Windows Server 2003, l'oggetto diventa di proprietà del gruppo Administrators anziché del singolo account che lo ha creato. Questo comportamento può essere modificato mediante lo snap-in MMC (Microsoft Management Console) Impostazioni protezione locale, utilizzando l'impostazione **Oggetti di sistema: proprietario predefinito per gli oggetti creati dai membri del gruppo Administrators**. Indipendentemente dalle autorizzazioni assegnate a un oggetto, il proprietario dell'oggetto può sempre modificarle.

Per ulteriori informazioni, vedere "Proprietà" nella Guida in linea di Windows Server.

Ereditarietà delle autorizzazioni

L'ereditarietà consente agli amministratori di assegnare e gestire facilmente le autorizzazioni. Grazie a questa caratteristica, gli oggetti all'interno di un contenitore ereditano automaticamente tutte le autorizzazioni ereditabili del contenitore. Quando si creano dei file all'interno di una cartella, ad esempio, essi ereditano le autorizzazioni assegnate alla cartella. Vengono ereditate solo le autorizzazioni contrassegnate come ereditabili.

Diritti utente

I diritti utente concedono privilegi e diritti di accesso specifici a utenti e gruppi nell'ambiente informatico.

Per informazioni sui diritti utente, consultare l'argomento "Diritti utente" nella Guida in linea di Windows Server.

Controllo degli oggetti

L'accesso degli utenti agli oggetti può essere controllato. Gli eventi relativi alla protezione possono essere visualizzati nel registro di protezione mediante il Visualizzatore eventi.

Per ulteriori informazioni, consultare l'argomento "Controllo" nella Guida in linea di Windows Server.

Procedure consigliate per il controllo dell'accesso

- Assegnare le autorizzazioni ai gruppi anziché ai singoli utenti. Poiché la gestione diretta degli account utente è inefficiente, l'assegnazione di autorizzazioni ai singoli utenti dovrebbe essere un'eccezione.
- Utilizzare le autorizzazioni Nega in alcuni casi speciali. Le autorizzazioni Nega possono essere utilizzate, ad esempio, per escludere un sottoinsieme di un gruppo che possiede autorizzazioni Consenti.
- Non negare mai l'accesso a un oggetto al gruppo Everyone. Il gruppo Everyone infatti include anche gli amministratori. Una soluzione migliore consiste nel rimuovere il gruppo Everyone, a condizione che si assegnino le autorizzazioni per quell'oggetto ad altri utenti, gruppi o computer. Ricordare che se non vengono definite le autorizzazioni, non è consentito alcun accesso.
- Cercare di assegnare le autorizzazioni agli oggetti che si trovano nella parte più alta della struttura e applicare quindi i principi di ereditarietà per propagare le impostazioni di protezione lungo tutta la struttura. È possibile applicare le impostazioni di controllo dell'accesso in modo rapido ed efficace a tutti gli oggetti figlio o alla sottostruttura di un oggetto padre. Così facendo si ottiene la migliore efficacia con il minimo sforzo. Le autorizzazioni impostate dovrebbero essere adeguate per la maggioranza degli utenti, dei gruppi e dei computer.
- Le autorizzazioni esplicite possono a volte prevalere sulle autorizzazioni ereditate. Le autorizzazioni Nega ereditate non impediscono l'accesso a un oggetto se tale oggetto dispone di un'autorizzazione Consenti esplicita. Le autorizzazioni esplicite hanno la precedenza sulle autorizzazioni ereditate, anche sulle autorizzazioni Nega.
- Per quanto riguarda le autorizzazioni sugli oggetti Active Directory®, accertarsi di comprendere le procedure consigliate specifiche per gli oggetti Active Directory.

Per ulteriori informazioni, consultare l'argomento "Procedure ottimali per l'assegnazione di autorizzazioni per gli oggetti Active Directory" nella Guida in linea di Windows Server 2003.

Firewall di protezione esterna

Un firewall è un dispositivo hardware o software che impedisce ai pacchetti di dati di entrare o di uscire da una rete specifica. Per controllare il flusso del traffico, le porte del firewall vengono aperte o chiuse ai pacchetti di informazioni. Il firewall controlla diverse informazioni in ciascun pacchetto di dati: il protocollo mediante il quale viene recapitato il pacchetto, la destinazione o il mittente del pacchetto, il tipo di contenuto del pacchetto e il numero di porta a cui viene inviato. Se il firewall è configurato per accettare il protocollo specificato attraverso la porta indicata, il pacchetto viene fatto passare. La soluzione firewall fornita con Microsoft Windows Small Business Server 2003 Premium Edition è Microsoft Internet Security and Acceleration (ISA) Server 2000. Anche Small Business Server Standard Edition include un firewall.

ISA Server 2004

Internet Security and Acceleration (ISA) Server 2000 esegue il routing in modo protetto delle richieste e delle risposte tra Internet e i computer client nella rete interna.

ISA Server agisce come gateway protetto verso Internet per i client sulla rete locale. Il computer ISA Server è trasparente alle altre parti del percorso di comunicazione. L'utente Internet non dovrebbe essere in grado di rilevare la presenza di un server firewall, a meno che non tenti di accedere a un servizio o di visitare un sito a cui il computer ISA Server neghi l'accesso. Il server Internet interpreta le richieste provenienti dal computer ISA Server come se fossero generate dall'applicazione client.

Se si sceglie di filtrare i frammenti IP (Internet Protocol), i servizi Web Proxy e Firewall vengono abilitati a filtrare i frammenti di pacchetti. Filtrando i frammenti di pacchetti, tutti i pacchetti IP frammentati vengono rimossi. Un attacco ben noto consiste nell'inviare pacchetti frammentati per riassemblarli in seguito in modo tale da poter danneggiare il sistema.

ISA Server è dotato di un meccanismo di rilevamento delle intrusioni che identifica il momento in cui la rete viene attaccata ed esegue un insieme di azioni configurate (denominate avvisi) in caso di attacco.

Se nel computer ISA Server è installato IIS (Internet Information Services), quest'ultimo deve essere configurato per non utilizzare le porte impiegate da ISA Server per le richieste Web in uscita e in ingresso (per impostazione predefinita le porte 8080 e 80 rispettivamente). È possibile, ad esempio, impostare IIS per monitorare la porta 81 e quindi configurare il computer ISA Server per indirizzare le richieste Web in ingresso alla porta 81 sul computer locale che esegue IIS.

Se si determina un conflitto tra le porte utilizzate da ISA Server e IIS, il programma di installazione arresta il servizio di pubblicazione IIS. Sarà quindi possibile impostare IIS per monitorare una porta diversa e riavviare il servizio di pubblicazione IIS.

Criteri di ISA Server

È possibile definire i criteri di ISA Server per determinare l'accesso in ingresso e in uscita. Le regole relative ai siti e al contenuto specificano a quali siti e a quale contenuto è possibile accedere. Le regole di protocollo indicano se un determinato protocollo sia accessibile per le comunicazioni in ingresso e in uscita.

È possibile creare regole per i siti, il contenuto, i protocolli, la pubblicazione Web e i filtri dei pacchetti IP. Tali criteri determinano la modalità di comunicazione dei client ISA Server con Internet e il tipo di comunicazione consentita.

Protezione dai virus

Un virus è un file eseguibile progettato per replicarsi, cancellare o danneggiare file di dati e programmi ed evitare di essere rilevato. I virus sono spesso riscritti e adattati in modo da non essere rilevati e vengono frequentemente inviati come allegati di posta elettronica. I programmi antivirus devono essere aggiornati continuamente per cercare virus nuovi e modificati. I virus rappresentano il metodo principale di vandalismo informatico.

Il software antivirus è progettato in modo specifico per il rilevamento e la prevenzione dei virus. Poiché vengono continuamente creati nuovi virus, molti produttori di programmi antivirus offrono aggiornamenti periodici del loro software ai clienti. Microsoft consiglia vivamente di implementare software antivirus nell'ambiente dei clienti.

I virus vengono generalmente installati nelle workstation degli utenti, nei server e nella rete in cui arriva (o a volte parte) la posta elettronica dell'organizzazione.

Tipi di virus

Esistono tre tipi di virus principali che infettano i sistemi informatici: i virus del settore di avvio, i virus che infettano i file e i programmi trojan horse.

Virus del settore di avvio

All'avvio di un computer, viene eseguita la scansione del settore di avvio del disco rigido prima di caricare il sistema operativo o altri file di avvio. Un virus del settore di avvio è progettato per sostituire le informazioni nei settori di avvio del disco rigido con il proprio codice. Quando un computer viene infettato da un virus del settore di avvio, il codice del virus viene letto nella memoria prima di qualunque altra cosa. Una volta entrato nella memoria, il virus può replicarsi in altri dischi utilizzati dal computer infetto.

Virus che infettano i file

Il tipo più comune di virus si aggrega a un file di programma aggiungendo il proprio codice al file eseguibile. Il codice del virus viene generalmente inserito in modo tale da sfuggire al rilevamento. Quando il file infetto viene eseguito, il virus può aggredire qualunque altro file eseguibile. I file colpiti da questo tipo di virus hanno in genere un'estensione COM, EXE o SYS.

Alcuni virus che infettano i file sono progettati per programmi specifici. I tipi di programma che sono spesso presi di mira sono file overlay (OVL) e librerie di collegamento dinamico (DLL). Questi file non sono eseguiti, ma vengono richiamati dai file eseguibili. Il virus si trasmette quando viene effettuata la chiamata.

I dati vengono danneggiati quando il virus viene attivato. Un virus può essere attivato quando un file infetto viene eseguito oppure quando incontra un determinata impostazione dell'ambiente, ad esempio una particolare data del sistema.

Programmi trojan horse

Un programma trojan horse non è virus vero e proprio. La distinzione principale tra un virus e un trojan horse è che quest'ultimo non replica sé stesso, ma distrugge le informazioni presenti sul disco rigido. Un programma trojan horse si presenta come un programma legittimo, ad esempio un gioco o un'utilità, ma quando viene eseguito può distruggere o danneggiare i dati.

Procedure consigliate per la protezione dai virus

La diffusione di un virus macro può essere ostacolata. Ecco alcuni suggerimenti da condividere con i clienti per impedire le infezioni:

- Installare una soluzione per la protezione dai virus che rilevi la presenza di eventuali virus nei messaggi in ingresso da Internet prima che i messaggi passino dal router. In questo modo i messaggi di posta elettronica verranno analizzati per individuare la presenza di virus noti.
- Conoscere l'origine dei documenti ricevuti. I documenti non dovrebbero essere aperti a meno che non provengano da mittenti affidabili.
- Parlare alla persona che ha creato il documento. Se l'utente non è certo che il documento sia sicuro, dovrebbe contattare la persona che l'ha creato.
- Utilizzare la protezione dai virus macro di Microsoft Office. Le applicazioni Office avvisano l'utente se un documento contiene delle macro. Questa funzionalità consente all'utente di attivare o disattivare le macro all'apertura del documento.
- Utilizzare software per la scansione di virus per rilevare e rimuovere virus macro. Il software per la scansione di virus è in grado di rilevare e spesso rimuovere i virus macro dai documenti. Microsoft consiglia l'utilizzo di software antivirus certificato dalla International Computer Security Association (ICSA).

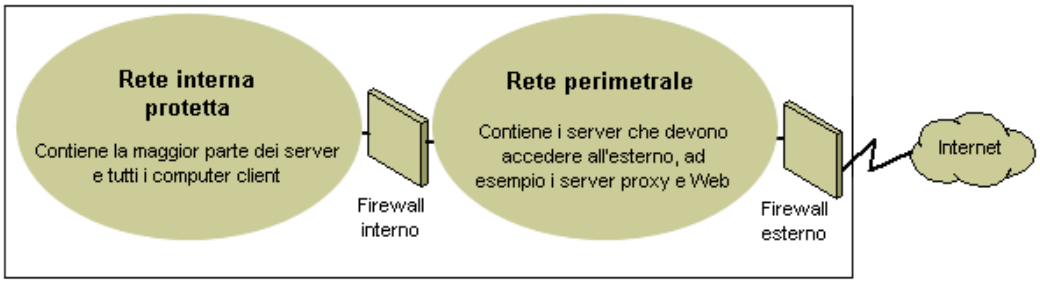
Per ulteriori informazioni sui virus e sulla protezione dei computer in generale, visitare i seguenti siti Web Microsoft (informazioni in lingua inglese):

- Microsoft Security all'indirizzo http://www.microsoft.com/security/default.asp.
- Documentazione sulla protezione in Microsoft TechNet http://www.microsoft.com/technet/security/Default.mspx.

Strategie di protezione della rete

Poiché la progettazione e la distribuzione di un ambiente di interconnessione IP richiede il bilanciamento di interessi pubblici e privati, il firewall è diventato un fattore chiave nella salvaguardia dell'integrità della rete. Un firewall non è un singolo componente. La National Computer Security Association (NCSA) definisce un firewall come "un sistema o combinazione di sistemi che impone un confine tra due o più reti". Nonostante siano utilizzati termini diversi, quel confine è spesso noto come rete perimetrale. La rete perimetrale protegge l'Intranet o la rete locale (LAN) aziendale dalle intrusioni controllando l'accesso da Internet o da altre reti di grandi dimensioni.

Il diagramma seguente illustra una rete perimetrale delimitata da firewall e situata tra una rete privata e Internet allo scopo di proteggere la rete privata:



Rete perimetrale di base

Le organizzazioni hanno approcci diversificati nell'utilizzo di firewall per la protezione. Il filtro dei pacchetti IP offre una protezione debole, è scomodo da gestire ed è facilmente superato. I gateway per le applicazioni sono più sicuri del filtro dei pacchetti e più semplici da gestire, perché si applicano solo ad alcune applicazioni specifiche, ad esempio un determinato sistema di posta elettronica. I gateway di circuito sono più efficaci quando l'interesse è puntato più verso l'utente di un'applicazione di rete piuttosto che verso i dati passati dall'applicazione. Il server proxy è uno strumento di protezione complessivo che include un gateway per le applicazioni, l'accesso sicuro per gli utenti anonimi e altri servizi. Di seguito sono elencate alcune informazioni su queste tre diverse opzioni:

- **Filtro di pacchetti IP**
  Il filtro di pacchetti IP è stata la prima implementazione della tecnologia firewall. Le intestazioni dei pacchetti sono esaminate per identificare gli indirizzi di origine e di destinazione, i numeri delle porte per i protocolli TCP (Transmission Control Protocol) e UDP (User Datagram Protocol) e altre informazioni. Il filtro dei pacchetti è una tecnologia limitata che funziona al meglio in ambienti di protezione ben definiti, dove, ad esempio, tutto ciò che è al di fuori della rete perimetrale viene considerato non affidabile e tutto ciò che è all'interno è considerato sicuro. In anni recenti, diversi produttori hanno migliorato il metodo di filtro dei pacchetti aggiungendo funzionalità di supporto decisionale intelligente, creando una nuova forma di filtro dei pacchetti denominata *stateful protocol inspection* (verifica dei protocolli basata sullo stato). Il filtro dei pacchetti può essere configurato per accettare tipi specifici di pacchetti rifiutando tutti gli altri oppure per rifiutare tipi specifici di pacchetti accettando tutti gli altri.
- **Gateway per le applicazioni**
  I gateway per le applicazioni sono utilizzati quando il contenuto di un'applicazione riveste la massima importanza. Il fatto che siano specifici per le applicazioni rappresenta sia la loro forza che il loro limite, perché non si adattano facilmente alle modifiche tecnologiche.
- **Gateway di circuito**
  I gateway di circuito sono tunnel creati attraverso un firewall che connettono processi o sistemi specifici su un lato con processi o sistemi specifici sull'altro lato. La migliore applicazione dei gateway di circuito è nelle situazioni in cui la persona che utilizza un'applicazione è potenzialmente un rischio maggiore delle informazioni trasportate dall'applicazione. Il gateway di circuito si differenzia dal filtro di pacchetti nella sua capacità di connettersi a uno schema di applicazioni fuori banda in grado di aggiungere ulteriori informazioni.

- **Server proxy**
  I server proxy sono strumenti di protezione completi, che includono funzionalità di firewall e gateway per applicazioni in grado di gestire il traffico Internet da e verso una LAN. I server proxy forniscono anche funzioni di controllo dell'accesso e di memorizzazione nella cache dei documenti. Un server proxy può migliorare le prestazioni memorizzando nella cache e fornendo direttamente i dati più richiesti, ad esempio le pagine Web visitate frequentemente. Un server proxy è anche in grado di filtrare e scartare le richieste che il proprietario non considera appropriate, quali le richieste di accesso non autorizzato a file proprietari.

Accertarsi che il cliente sfrutti le funzionalità di protezione dei firewall che possono essere utili. Implementare una rete perimetrale in un punto della topologia di rete in cui tutto il traffico proveniente dall'esterno della rete aziendale debba passare attraverso il perimetro gestito dal firewall esterno. È possibile ottimizzare il controllo dell'accesso per soddisfare le esigenze del cliente, nonché configurare i firewall affinché segnalino tutti i tentativi di accesso non autorizzato.

Per minimizzare il numero di porte che occorre aprire sul firewall interno, è possibile utilizzare un firewall a livello di applicazione come ISA Server 2000.

Per ulteriori informazioni su TCP/IP, vedere il documento "Designing a TCP/IP Network" all'indirizzo: http://www.microsoft.com/resources/documentation/WindowsServ/2003/all/deployguide/en-us/dnsbb_tcp_overview.asp (informazioni in lingua inglese).

Reti wireless

Per impostazione predefinita, le reti wireless sono configurate in modo da consentire l'intercettazione dei segnali senza fili. Le cause che le rendono vulnerabili agli aggressori esterni che riescono ad accedere sono le impostazioni predefinite di alcuni hardware senza fili, l'accessibilità che offrono le reti wireless e gli attuali metodi di crittografia. Esistono strumenti e opzioni di configurazione che possono proteggere dall'intercettazione, ma che non hanno alcuna efficacia nel proteggere i computer da pirati informatici e virus che penetrano attraverso la connessione Internet. È quindi estremamente importante includere un firewall per proteggere i computer da intrusi indesiderati su Internet.

Per ulteriori informazioni sulla protezione delle reti wireless, vedere l'articolo "How to Make Your 802.11b Wireless Home Network More Secure" all'indirizzo http://support.microsoft.com/default.aspx?scid=kb;en-us;309369 (informazioni in lingua inglese).

Scenari di protezione della rete

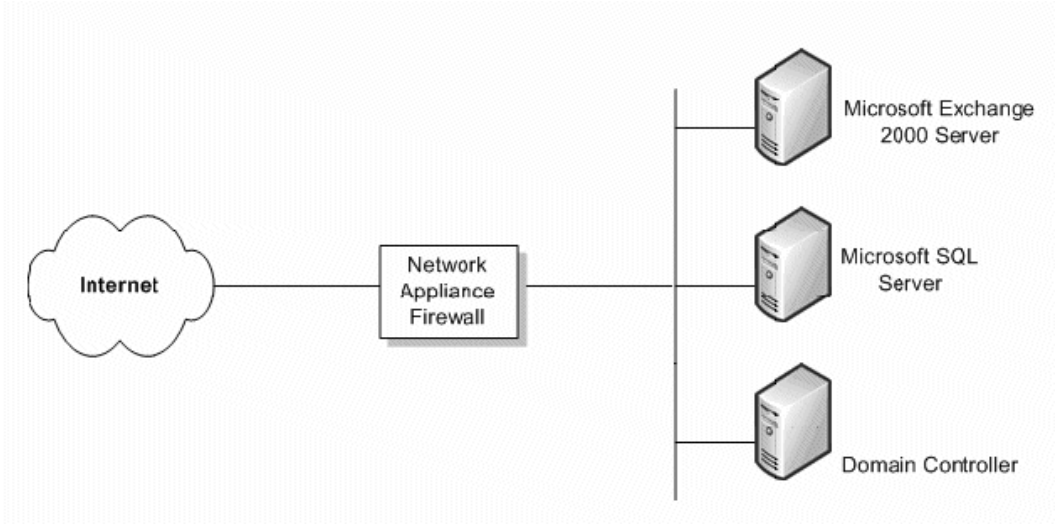
Il livello di protezione della rete richiesto dall'organizzazione del cliente dipende da diversi fattori. Si tratta in genere di un compromesso tra il budget a disposizione e la necessità di proteggere i dati dell'azienda. Una piccola azienda potrebbe desiderare una struttura di protezione molto complessa che fornisca il più alto livello possibile di protezione della rete, ma non potersela permettere economicamente. In questa sezione verranno presentati quattro scenari e i consigli per ognuno di esso relativamente ai vari livelli di protezione.

Senza firewall

Se il cliente dispone di una connessione a Internet senza firewall, è necessario implementare alcune misure di protezione della rete. Esistono dispositivi firewall semplici che forniscono protezione sufficiente per scoraggiare la maggior parte dei pirati informatici.

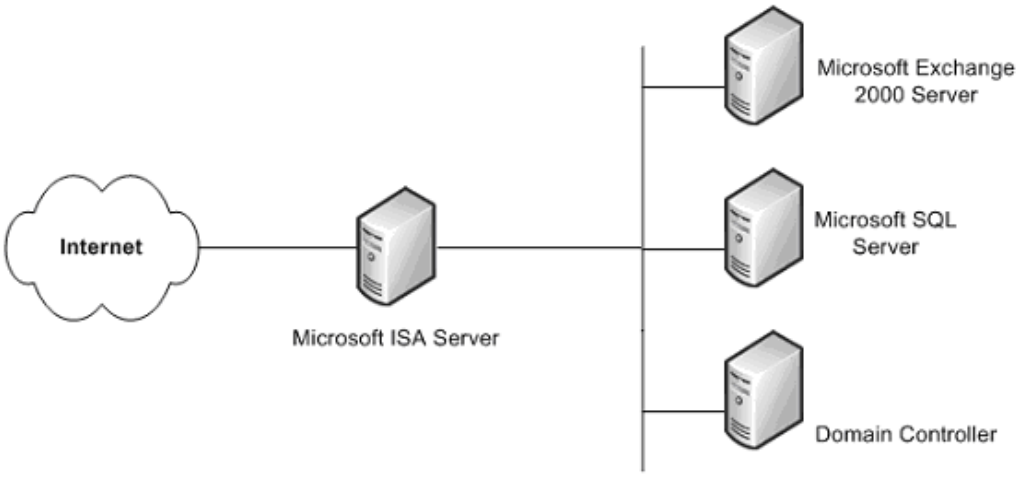
Un firewall semplice

Il livello minimo di protezione consigliato è un singolo firewall posto tra Internet e i dati del cliente. Questo tipo di firewall potrebbe non fornire livelli di protezione avanzata e non dovrebbe essere considerato molto sicuro. Tuttavia è sempre meglio di niente.



Firewall semplice

Se il budget del cliente consente di scegliere una soluzione più efficace per proteggere i dati aziendali, tale soluzione è ISA Server. Questo server aggiuntivo ha un costo maggiore, ma fornisce molta più protezione di un firewall mediocre, le cui funzioni si limitano alla conversione degli indirizzi di rete (NAT, Network Address Translation) e al filtro dei pacchetti.



Firewall ISA Server

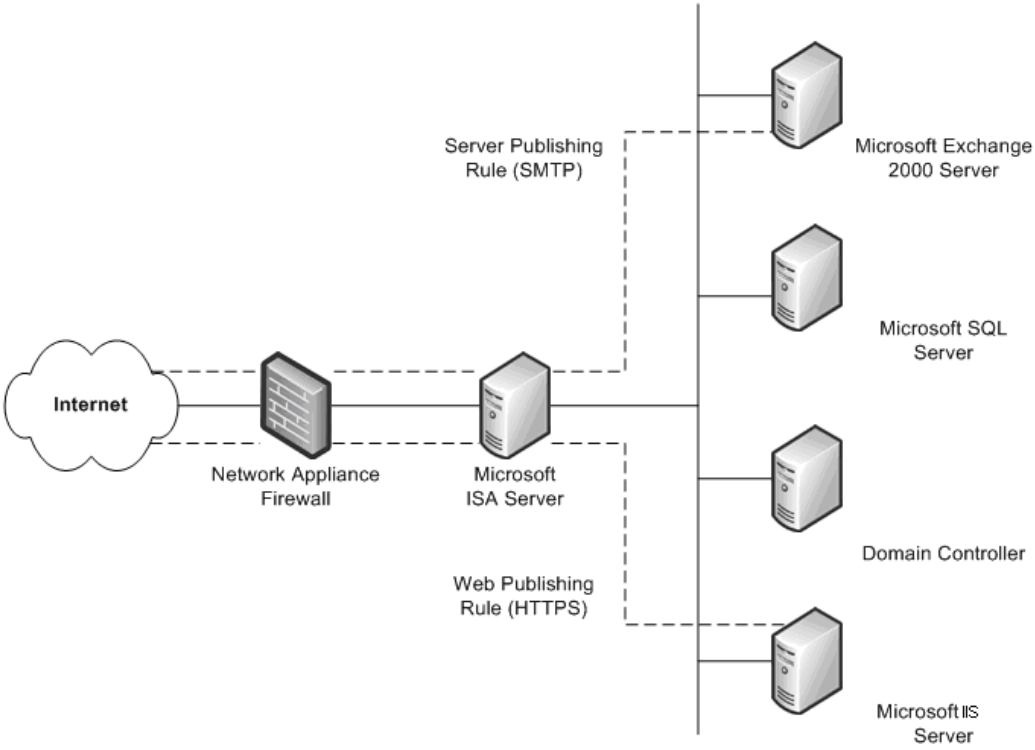
Questa soluzione con un singolo firewall è più sicura di un dispositivo firewall di basso livello e fornisce servizi di protezione specifici per Windows.

Un firewall esistente

Se il cliente dispone di un firewall esistente che separa l'Intranet da Internet, occorre prendere in considerazione l'eventualità di un firewall aggiuntivo che fornisca più modi di configurare le risorse interne per Internet.

Un metodo consiste nella pubblicazione Web. Questa soluzione è costituita da un computer ISA Server distribuito davanti al server Web dell'organizzazione che fornisce l'accesso agli utenti Internet. Quando arrivano le richieste Web, ISA Server può impersonare un server Web per il mondo esterno, soddisfacendo le richieste di contenuto Web con la propria cache. Le richieste vengono inoltrate al server Web solo quando non possono essere soddisfatte dalla cache di ISA Server.

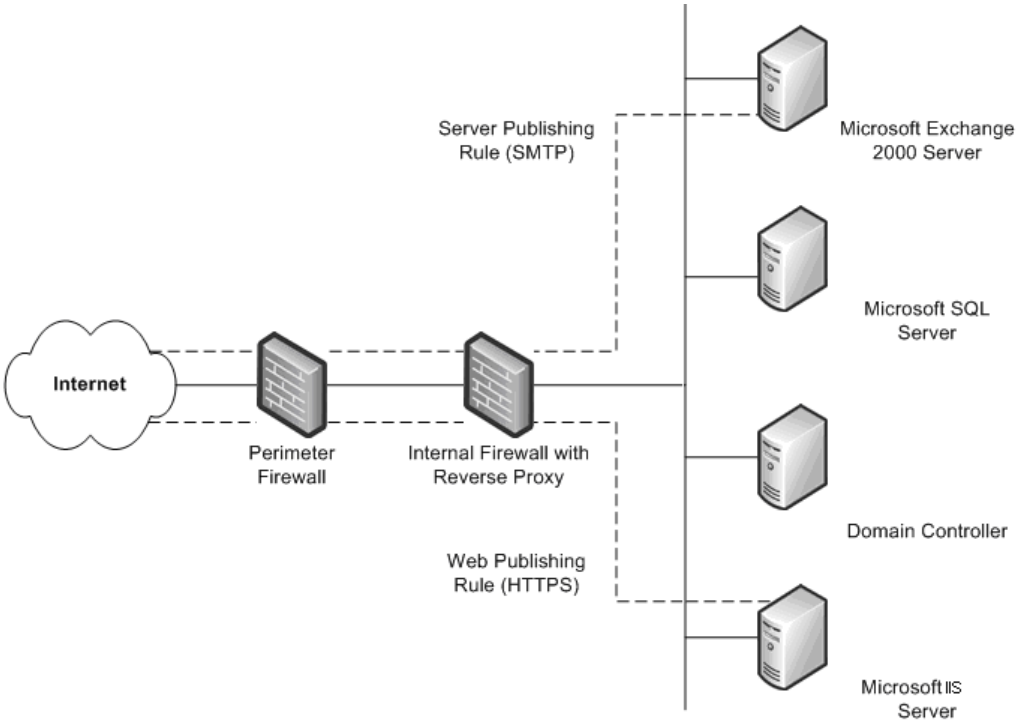
Un altro metodo è la pubblicazione server. ISA Server consente la pubblicazione di server interni su Internet senza compromettere la protezione della rete interna. È possibile configurare le regole di pubblicazione server e Web che determinano quali richieste inviare a un server sulla rete locale, fornendo un ulteriore livello di protezione per i server interni.



Firewall esistente con l'aggiunta di ISA Server

Due firewall esistenti

Il quarto scenario prevede che l'organizzazione disponga di due firewall con una rete perimetrale (DMZ). Uno o più di questi server forniscono servizi di proxy inverso, impedendo ai client Internet di accedere direttamente ai server sulla Intranet. Uno dei firewall, idealmente il firewall interno, intercetta le richieste di rete per i server interni, verificando i pacchetti e inoltrandoli per conto dell'host Internet.



Due firewall esistenti

Questo scenario è simile al precedente dopo aver aggiunto il secondo firewall. L'unica differenza è data dal fatto che il firewall interno che supporta il proxy inverso non è ISA Server. In questo scenario è necessario collaborare strettamente con gli amministratori dei firewall per definire le regole di pubblicazione server che soddisfano i criteri di protezione.

Gestione delle patch di protezione

I sistemi operativi e le applicazioni sono spesso enormemente complessi. Possono essere composti da milioni di righe di codice, scritte da numerosi programmatori. È essenziale che il software funzioni in modo affidabile e non comprometta la protezione o la stabilità dell'ambiente informatico. Per minimizzare i problemi, i programmi vengono testati accuratamente prima del rilascio. Tuttavia, gli aggressori tentano continuamente di trovare punti deboli nel software e non è possibile prevedere tutti i futuri attacchi.

Per molte organizzazioni la gestione delle patch costituisce una parte della loro strategia generale di gestione della configurazione e dei cambiamenti. Indipendentemente dalla natura e dalle dimensioni dell'organizzazione, è vitale avere una buona strategia di gestione delle patch, anche se l'organizzazione non ha ancora predisposto alcuna gestione della configurazione e dei cambiamenti. La vasta maggioranza degli attacchi riusciti si verificano in quei sistemi informatici in cui non sono state installate le patch di protezione.

Le patch di protezione rappresentano una vera sfida per la maggior parte delle organizzazioni. Quando viene rilevato un punto debole nel software, l'informazione si divulga rapidamente nella comunità dei pirati informatici.

Quando il suo software presenta una vulnerabilità, Microsoft tenta di rilasciare una patch di protezione il più presto possibile. Fino a quando la patch non viene distribuita, la protezione che il cliente si aspetta e su cui fa affidamento potrebbe diminuire drasticamente.

Nell'ambiente Navision occorre verificare che nei sistemi dei clienti siano installate le patch di protezione più recenti. Accertarsi che il client utilizzi una delle tecnologie predisposte da Microsoft. Esse sono:

- **Microsoft Security Notification Service**
  Si tratta di un servizio basato su posta elettronica che distribuisce avvisi quando un aggiornamento diventa disponibile. Questi avvisi sono un utile strumento per un'attiva strategia di protezione. Gli avvisi sono disponibili anche nel sito Web Technet Product Security Notification all'indirizzo:
  http://www.microsoft.com/technet/security/bulletin/notify.mspx
  (informazioni in lingua inglese).
- **Aggiornamenti automatici Microsoft**
  Windows è in grado di applicare automaticamente gli aggiornamenti di protezione ai computer.
- **Strumento di ricerca dei bollettini Microsoft sulla sicurezza**
  Questo strumento è disponibile nel sito Web dedicato ai bollettini sulla sicurezza: http://www.microsoft.com/technet/security/bulletin/notify.mspx (informazioni in lingua inglese). Il cliente può determinare quali aggiornamenti sono necessari in base al sistema operativo, alle applicazioni e ai service pack attualmente installati.
- **Microsoft Baseline Security Analyzer (MBSA)**
  Questo strumento grafico è disponibile nel sito Web Microsoft Baseline Security Analyzer all'indirizzo: http://www.microsoft.com/technet/security/tools/mbsahome.mspx (informazioni in lingua inglese). Questo strumento consente di confrontare lo stato corrente di un computer con un elenco di aggiornamenti gestito da Microsoft. MBSA esegue inoltre alcuni controlli di base sulle impostazioni relative alla scadenza e alla complessità delle password, sui criteri degli account Guest e su una serie di altre aree. MBSA è anche in grado di cercare vulnerabilità in Microsoft Internet Information Services (IIS), SQL Server™ 2000, Exchange 5.5, Exchange 2000 ed Exchange Server 2003.
- **Microsoft Software Update Services (SUS)**
  Noto in precedenza con il nome Windows Update Corporate Edition, questo strumento consente alle aziende di ospitare su computer locali tutti gli aggiornamenti critici e i pacchetti di protezione cumulativi disponibili sul sito Windows Update. Questo strumento funziona con una nuova versione dei client di aggiornamento automatico e forma la base di una potente strategia di download e installazione automatici. Il nuovo client di aggiornamento automatico è disponibile per i sistemi operativi Windows 2000 e Windows 2003 ed è in grado di installare automaticamente gli aggiornamenti scaricati. Per ulteriori informazioni su Microsoft SUS, visitare il sito all'indirizzo
  http://www.microsoft.com/windows2000/windowsupdate/sus/default.asp
  (informazioni in lingua inglese).
- **Microsoft Systems Management Server (SMS) Software Update Services Feature Pack**
  SMS Software Update Services Feature Pack contiene una serie di strumenti il cui scopo è facilitare il processo di distribuzione degli aggiornamenti software nell'azienda. Gli strumenti inclusi sono: Security Update Inventory Tool, Microsoft Office Inventory Tool for Updates, Distribute Software Updates Wizard e SMS Web Reporting Tool con Web Reports Add-in for Software Updates. Per ulteriori informazioni su ciascun strumento, visitare il sito all'indirizzo
  http://www.microsoft.com/smserver/downloads/20/featurepacks/suspack/
  (informazioni in lingua inglese).

Parlare ai clienti di ognuno di questi strumenti e incoraggiarli a utilizzarli. È molto importante che i problemi di protezione siano affrontati nel più breve tempo possibile, mantenendo allo stesso tempo la stabilità dell'ambiente.

Impostazioni di protezione di SQL Server 2000

Poiché Navision viene eseguito su SQL Server 2000, è importante prendere provvedimenti per incrementare la protezione dell'installazione di SQL Server 2000 del cliente. Le seguenti indicazioni aiutano ad aumentare la protezione di SQL Server:

- Accertarsi che siano installati il sistema operativo, i service pack e gli aggiornamenti più recenti per SQL Server 2000. Per informazioni aggiornate visitare il sito Web Microsoft Security all'indirizzo http://www.microsoft.com/security/default.asp (informazioni in lingua inglese).
- Per la protezione a livello di file system, verificare che tutti i dati e i file di sistema di SQL Server 2000 siano installati in partizioni NTFS. Rendere i file accessibili solo agli utenti a livello di sistema o amministrativo mediante autorizzazioni NTFS. In questo modo i file saranno protetti dall'accesso quando il servizio MSSQLSERVER non è in esecuzione.
- Utilizzare un account di dominio con privilegi minimi, come l'account NT Authority\Servizio di rete o LocalSystem (consigliato) per il servizio SQL Server 2000 (MSSQLSERVER). Tale account dovrebbe avere i diritti minimi nel dominio, contribuendo a contenere (anche se non a fermare) un attacco al server in caso di violazione. In altre parole, questo account dovrebbe disporre solo delle autorizzazioni a livello utente locale nel dominio. Se per eseguire i servizi di SQL Server 2000 viene utilizzato un account di amministratore di dominio, una violazione del server può portare a una violazione dell'intero dominio. Per modificare questa impostazione, utilizzare SQL Server Enterprise Manager. Gli elenchi di controllo di accesso (ACL, Access Control List) sui file, il Registro di sistema e i diritti utente verranno modificati automaticamente.
- La maggior parte delle versioni di SQL Server 2000 sono installate con due database predefiniti, **Northwind** e **pubs**. Entrambi sono database di esempio utilizzati a scopo di test, formazione e per esemplificazioni generali. Non distribuirli in un sistema di produzione. La presenza di questi database può incoraggiare un aggressore a tentare violazioni che coinvolgano la configurazione e le impostazioni predefinite. Se i database **Northwind** e **pubs** sono presenti nel computer SQL Server 2000 di produzione, dovrebbero essere rimossi.
- Il controllo del sistema SQL Server 2000 è disattivato per impostazione predefinita, quindi le condizioni non sono controllate. Questo rende difficile il rilevamento delle intrusioni e aiuta gli aggressori a coprire le loro tracce. È necessario attivare almeno il controllo degli accessi non riusciti.

Per informazioni aggiornate sulla protezione di SQL Server 2000, visitare il sito all'indirizzo:

http://www.microsoft.com/sql/techinfo/administration/2000/security/default.asp
(informazioni in lingua inglese).

Informazioni su Microsoft Business Solutions

Microsoft Business Solutions, un reparto di Microsoft, offre una vasta gamma di servizi e applicazioni aziendali end-to-end integrati, progettati per aiutare le piccole, medie e grandi aziende a migliorare la comunicazione con i clienti, i dipendenti, i partner e i fornitori. Le applicazioni Microsoft Business Solutions ottimizzano i processi aziendali strategici nella gestione finanziaria, nei processi di analisi, nella gestione delle risorse umane, nella gestione dei progetti, nella gestione delle relazioni con i clienti, nella gestione dei servizi, nella gestione dei fornitori e nella gestione della produzione, della vendita al dettaglio e dell'e-commerce. Le applicazioni sono progettate per aiutare i clienti a raggiungere il successo desiderato. Ulteriori informazioni su Microsoft Business Solutions sono disponibili nel sito all'indirizzo http://www.microsoft.com/BusinessSolutions/ (informazioni in lingua inglese).