Microsoft Business Solutions

Navision Security Hardening Guide

Date de publication : octobre 2004

Microsoft

Table des matières

Introduction....1

Meilleures pratiques de sécurité de Navision....2

Sécurité physique....4

Les employés....4

Les administrateurs....5

Comment sécuriser le système d'exploitation du serveur....6
- Authentification....7
- Mots de passe forts....7
- Contrôle d'accès....9
- Pare-feu externe....11

ISA Server 2004....12
- Stratégies relatives à ISA Server....12

Protection contre les virus....13
- Types de virus....13
- Recommandations en matière de protection contre les virus....14

Stratégies de sécurité du réseau....15
- Réseaux sans fil....16
- Scénarios de sécurité du réseau....17

Gestion des correctifs de sécurité....21

Paramètres de sécurité SQL Server 2000....22

À propos de Microsoft Business Solutions....24

Introduction

Microsoft® Windows® comporte des dispositifs perfectionnés et normalisés de sécurité du réseau. Au sens le plus large, la sécurité est une question de planification et de compromis. Par exemple, un ordinateur peut être enfermé dans une chambre forte et accessible uniquement à un administrateur système. L'ordinateur est alors sécurisé, mais il n'est pas très utile, car il n'est connecté à aucun autre ordinateur. Vous devez vous efforcer de sécuriser le réseau sans nuire à son utilisation.

Les organisations se protègent pour la plupart contre les attaques externes en construisant des pare-feu, mais un grand nombre de compagnies ne savent pas comment faire face à une atteinte à la sécurité lorsqu'un utilisateur malveillant réussit à franchir le pare-feu. Dans l'environnement de vos clients, les mesures de sécurité fonctionneront bien si les utilisateurs n'ont pas à se plier à un trop grand nombre de procédures et d'étapes pour travailler de façon sécurisée. La mise en œuvre des politiques de sécurité devrait être aussi conviviale que possible pour les utilisateurs, faute de quoi ceux-ci trouveront des moyens de contourner ces politiques.

Comme la taille des installations Navision peut varier énormément, il est important d'envisager avec soin les besoins de chaque client et de trouver un compromis entre l'efficacité de la sécurité et les dépenses à engager. En tant que conseiller de confiance de votre client, servez-vous de votre jugement pour recommander une politique qui réponde à ses besoins en matière de sécurité, sans pour autant créer une charge qui entraînera en bout de ligne l'abandon de la politique par le client.

Meilleures pratiques de sécurité de Navision

Voici les règles générales qui peuvent contribuer à améliorer la sécurité de l'environnement Navision :

- Si vous désirez que Navision Database Server s'exécute en tant que service ou si vous préférez utiliser le paramètre de ligne de commande installasservice lorsque vous démarrez le serveur, vous devez vous assurer que le service s'exécute en tant que compte Autorité NT\Service réseau. Ce type de compte existe uniquement dans Windows™ XP et Windows Server™ 2003. Si vous utilisez Windows 2000 Server, vous devrez créer pour le service un compte ayant le moins de privilèges possible, faute de quoi un compte Système local sera assigné au service. Ce compte devrait avoir au plus les mêmes privilèges qu'un compte d'utilisateur normal, ou être un compte de domaine qui n'est pas administrateur dans le domaine lui-même ou sur tout ordinateur local.

  Vous ne devez pas oublier d'accorder au compte Autorité NT\Service réseau ou au compte d'utilisateur sous lequel s'exécute le serveur un accès en lecture et écriture au(x) fichier(s) de base de données, afin que les utilisateurs puissent accéder à la base de données.

  Dans Windows XP, procédez comme suit pour donner au compte Autorité NT\Service réseau l'accès en lecture et écriture à un fichier de base de données :

  1. Dans l'Explorateur Windows, naviguez jusqu'au dossier qui contient le fichier de base de données.
  2. Cliquez avec le bouton droit sur ce fichier et sélectionnez ensuite **Propriétés**.
  3. Dans la fenêtre ***Propriétés***, cliquez sur l'onglet ***Sécurité***; dans le champ **Noms d'utilisateur ou de groupe**, cliquez sur **Ajouter**.
  4. Dans la boîte de dialogue ***Sélectionnez Utilisateurs, Ordinateurs ou Groupes***, entrez *Service réseau* et cliquez sur OK.
  5. Windows ajoute alors SERVICE RÉSEAU dans la zone **Noms d'utilisateur ou de groupe** de la fenêtre ***Propriétés***.
  6. Sélectionnez SERVICE RÉSEAU et, dans le champ, **Autorisations**, sélectionnez *Lecture* et *Écriture*.
- Le service Navision Application Server s'exécute par défaut en tant que compte Autorité NT\Service réseau, ce qui autorise l'accès local à Navision Database Server. Dans un réseau cependant, vous devez vous assurer que le service service Navision Application Server s'exécute en tant que compte de domaine Windows reconnu par Navision Database Server, afin que le service puisse accéder au serveur de base de données. Ce compte de domaine ne devrait pas être administrateur dans le domaine lui-même ou sur tout ordinateur local.
- Si vous exécutez l'option SQL Server pour Navision, le serveur Microsoft SQL Server™ s'exécute en tant que service. Pour que l'option SQL Server pour Navision fonctionne, il faut que SQL Server puisse consulter Active Directory afin d'obtenir les listes des groupes d'utilisateurs Windows pour les besoins d'authentification. Vous devez donc vous assurer que le service SQL Server s'exécute en tant que compte Autorité NT\ Service réseau.

  Pour cela, procédez comme suit :

  1. Sur l'ordinateur SQL Server, localisez le service MSSQLSERVER, cliquez avec le bouton droit sur ce service et cliquez ensuite sur **Propriétés**.
  2. Dans la fenêtre ***Propriétés***, cliquez sur l'onglet ***Connexion***.
  3. Sous l'onglet ***Connexion***, dans la zone **Se connecter en tant que**, cliquez sur ***Ce compte***, entrez *Autorité NT\Service réseau* et cliquez sur OK.

Pour un complément d'information sur la sécurité SQL Server, visitez les sites :
http://www.microsoft.com/security/guidance/prodtech/SQLServer.mspx
et http://www.microsoft.com/technet/security/prodtech/dbsql/default.mspx

- Si vous utilisez un produit de commerce électronique Navision comme Commerce Gateway, vous devez vous assurer que le serveur de requêtes Commerce Gateway a été correctement installé et que le paramètre de compte par défaut lui a été assigné pour les services. Ce paramètre de compte par défaut, appelé *CGRSUser*, permet au serveur Commerce Gateway d'accéder à l'ensemble minimum des autres services dont il a besoin, dont les services *MSSQLSERVER* et *BizTalk Service BizTalk Group : BizTalkServerApplication*; il ne comprend pas de paramètres de compte global comme le compte *Système local*.
- Toujours utiliser des mots de passe forts. Pour un complément d'information à ce sujet, reportez-vous à la section Mots de passe forts.
- Utilisez les connexions Windows. Navision vous permet de créer deux catégories de connexions – les connexions de base de données et les connexions Windows. Nous vous recommandons d'utiliser les connexions Windows car celles-ci nécessitent l'authentification Windows, ce qui vous permet de mettre en place une politique appropriée de mots de passe.
- Les mots de passe ne devraient pas être réutilisés. Il est de pratique courante de réutiliser des mots de passe entre différents systèmes ou domaines. Par exemple, un administrateur responsable de deux domaines peut créer dans chaque domaine des comptes d'administrateur qui utilisent le même mot de passe, et même définir sur tous les ordinateurs d'un domaine le même mot de passe d'administrateur local. Dans ce cas, si la sécurité d'un seul compte ou ordinateur est compromise, c'est le domaine dans son ensemble qui est menacé.
- Après avoir terminé l'installation de Navision et la création ou la mise à jour des bases de données, vous devez créer une connexion Windows et lui assigner le rôle SUPER dans Navision. C'est ce SUPER utilisateur qui s'occupera de l'administration de la base de données, des questions de sécurité, etc. Associez à ce nom de connexion un mot de passe fort. Protégez la confidentialité du mot de passe. La protection devrait être égale à celle du mot de passe AS dans SQL Server. Le rôle SUPER gère tous les accès à la base de données, c'est pourquoi il nécessite le plus haut niveau de protection. Seuls les administrateurs système devraient connaître le mot de passe du SUPER utilisateur.
- Accordez moins de privilèges à tous les autres utilisateurs qui doivent accéder à la base de données Navision. En d'autres termes, attribuez-leur dans Navision des rôles qui leur donnent accès uniquement aux fonctions dont ils ont besoin pour accomplir leurs tâches dans la compagnie.
- Seuls les utilisateurs dont le travail l'exige devraient être en mesure d'importer des fichiers FOB, de modifier des objets et de créer et restaurer des copies de sauvegarde de la base de données.
- Faites régulièrement des copies de sauvegarde de la base de données Navision et n'oubliez pas de vous assurer que la restauration du système est possible à partir des copies de sauvegarde.
- Rangez les copies de sauvegarde dans un lieu sûr afin de les protéger contre le feu, la fumée, la poussière, les températures élevées, la foudre et les désastres naturels (tremblements de terre, par exemple).

- Bien que Navision soit compatible avec plusieurs versions de Windows, il est recommandé d'utiliser les systèmes d'exploitation les plus récents, dotés des fonctions de sécurité les plus à jour. Actuellement, il s'agit des systèmes Windows XP, Service Pack 2 et Windows Server 2003.
- Utilisez le service de mise à jour Windows Update fourni avec Windows 2000, Windows XP et Windows Server 2003, pour appliquer les mises à jour de sécurité les plus récentes. Utilisez la fonction de mise à jour automatique de Windows pour distribuer à tous vos ordinateurs clients les plus récents correctifs de sécurité, service packs et mises à jour.
- Nous vous recommandons d'utiliser le protocole sécurisé TCPS pour les communications entre les clients Navision et Navision Database Server. TCPS est une version sécurisée de TCP/IP qui utilise l'interface SSPI (Security Support Provider Interface), avec cryptage activé et authentification Kerberos. TCPS est le protocole par défaut pour Navision Database Server.
- Le client devrait avoir mis en place un plan de reprise après sinistre, pour garantir le rétablissement rapide des services en cas de sinistre. Ce plan doit couvrir les points suivants :
  - Acquisition d'équipement temporaire ou neuf.
  - Restauration des copies de sauvegarde sur les nouveaux systèmes.
  - Vérification du bon fonctionnement du plan de reprise.

Sécurité physique

La sécurité physique est absolument essentielle car elle ne peut être remplacée d'aucune façon par la sécurité logicielle. En cas de vol d'un disque dur, par exemple, les données de ce disque finiront par être volées également. Pendant l'élaboration d'une politique de sécurité avec le client, discutez des questions de sécurité physique suivantes :

- Dans les grandes installations qui comportent des services TI spécialisés, les salles où se trouvent les serveurs et les endroits où sont stockés les logiciels doivent être verrouillés.
- Les machines qui entrent dans cette catégorie comprennent :
  - Le serveur Microsoft SQL Server 2000.
  - Le serveur de fichiers où résident les programmes exécutables Navision.
- Seuls les utilisateurs autorisés doivent avoir accès aux ordinateurs.
- Des détecteurs d'effraction doivent être installés, quel que soit le degré de confidentialité des données.
- Les copies de sauvegarde des données critiques doivent être entreposées à l'extérieur des lieux, dans des contenants résistants au feu.

Les employés

Il est recommandé de limiter les droits d'administration pour l'ensemble des produits et fonctions. En règle générale, les clients ne devraient donner à leurs employés qu'un accès en lecture aux fonctions du système, sauf s'ils ont besoin d'un accès accru pour accomplir leurs tâches. Microsoft suggère d'appliquer le principe des moindres privilèges : accorder aux utilisateurs le strict minimum des privilèges nécessaires pour l'accès aux données et à la fonctionnalité.

Les employés mécontents et les anciens employés constituent une menace pour la sécurité du réseau. Lorsque vous discutez de la sécurité avec vos clients, proposez-leur les politiques suivantes concernant les employés :

- Toujours faire une enquête sur les antécédents des candidats avant l'embauche.
- S'attendre à une « vengeance » de la part des employés mécontents et des anciens employés.
- Au moment du départ d'un employé, veiller à désactiver tous les comptes et mots de passe Windows associés à cet employé. Pour les besoins des rapports, ne pas supprimer les utilisateurs. Ne pas réutiliser les comptes.
- Demander aux utilisateurs d'être vigilants et de signaler toute activité suspecte.
- Ne jamais accorder automatiquement de privilèges. Si des utilisateurs n'ont pas besoin d'accéder à des ordinateurs, salles informatiques ou ensembles de fichiers, veiller à ce qu'ils n'y aient pas accès.
- Enseigner aux superviseurs à déceler les problèmes qui peuvent toucher les employés et à y réagir.
- Veiller à ce que les employés comprennent bien leur rôle dans le maintien de la sécurité du réseau.
- Remettre une copie des politiques de la compagnie à chaque employé.
- Interdire aux utilisateurs d'installer tout logiciel non autorisé.

Les administrateurs

Il est recommandé que les administrateurs système de vos clients installent régulièrement les correctifs de sécurité les plus récents de Microsoft. Les pirates sont très habiles à combiner de petites erreurs pour réussir une importante intrusion dans un réseau. Les administrateurs doivent d'abord veiller à sécuriser le plus possible chaque ordinateur, pour ensuite installer les mises à jour de sécurité et un logiciel antivirus. Le présent guide contient un grand nombre de liens et de ressources qui vous aideront à trouver de précieuses informations et les meilleures pratiques à ce sujet.

Vous devez également trouver un compromis entre la complexité et la sécurité du réseau. Plus un réseau est complexe, plus il est difficile à sécuriser ou à réparer une fois qu'un intrus a réussi à y accéder. L'administrateur doit documenter en détail la topographie du réseau, dans le but de le maintenir aussi simple que possible.

La sécurité est essentiellement une question de gestion des risques. Comme la technologie n'est pas une panacée, la sécurité nécessite une combinaison de technologie et de politiques. En d'autres termes, vous ne trouverez jamais un produit que vous pouvez simplement déballer et installer sur le réseau pour atteindre instantanément une sécurité parfaite. La sécurité résulte aussi bien de la technologie que des politiques – c'est la façon dont la technologie est employée qui détermine en bout de ligne le degré de sécurité du réseau. La technologie et les fonctions de Microsoft répondent aux impératifs de sécurité, mais seul l'administrateur pourra déterminer, en suivant vos conseils, les politiques qui conviennent à son organisation. Veillez à inclure les questions de sécurité dès le début du processus de mise en œuvre et de déploiement. Comprenez bien ce que le client désire protéger et ce qu'il est prêt à faire pour obtenir la protection voulue.

Enfin, élaborez des plans de secours en prévision des situations d'urgence. Votre client bénéficiera d'une excellente sécurité si vous combinez une planification en profondeur avec une solide technologie.

Pour un complément d'informations sur la sécurité en général, consultez le document « The Ten Immutable Laws of Security Administration », à l'adresse :
http://www.microsoft.com/technet/archive/community/columns/security/essays/10salaws.mspx.

et les articles sur la gestion de la sécurité à l'adresse :
http://www.microsoft.com/technet/community/columns/secmgmt/smarch.mspx

Comment sécuriser le système d'exploitation du serveur

Bien qu'un grand nombre de petits clients ne disposent pas de système d'exploitation de type serveur, il est important que vous compreniez et puissiez expliquer les meilleures pratiques de sécurité aux gros clients qui possèdent des environnements de réseau plus complexes. Vous devez également savoir que la plupart des politiques et pratiques décrites dans le présent document peuvent aisément s'appliquer aux entreprises qui possèdent uniquement des systèmes d'exploitation de type client.

Les concepts exposés dans cette section s'appliquent autant aux produits Microsoft Windows 2002 Server et Microsoft Windows Server 2003, bien que l'information provienne principalement de l'aide en ligne de Windows Server 2003. Ce dernier système d'exploitation offre un ensemble robuste de fonctions de sécurité. De plus, l'aide en ligne de Windows Server 2003 décrit en profondeur toutes les fonctions et procédures de sécurité.

Pour un complément d'information sur Windows 2000 Server, visitez le centre de sécurité Windows 2000 Server, à l'adresse :
http://www.microsoft.com/technet/security/prodtech/win2000/default.mspx.

et lisez le document « Windows 2000 Security Hardening Guide », à l'adresse :
http://www.microsoft.com/technet/security/prodtech/win2000/win2khg/default.mspx

Pour un complément d'information sur Windows Server 2003, consultez le document *Windows Server 2003 Security Guide*, à l'adresse :
http://www.microsoft.com/technet/security/prodtech/win2003/w2003hg/sgch00.mspx

Les principaux éléments du modèle de sécurité des serveurs Windows sont l'authentification, le contrôle d'accès et l'identification unique :

- L'authentification est le processus par lequel le système valide l'identité d'un utilisateur en vérifiant ses références d'ouverture de session. Le système vérifie que le nom et le mot de passe de l'utilisateur figurent sur la liste des utilisateurs autorisés. Dans l'affirmative, le système autorise l'accès, dans la mesure spécifiée par la liste des autorisations de l'utilisateur.

- Le contrôle d'accès limite l'accès des utilisateurs aux informations ou ressources informatiques, en fonction de l'identité des utilisateurs et sur leur appartenance à différents groupes prédéfinis. Ce type de contrôle est habituellement employé par les administrateurs de système pour limiter l'accès des utilisateurs aux ressources du réseau, telles que serveurs, répertoires et fichiers. Il est habituellement mis en œuvre en accordant à des utilisateurs et groupes l'autorisation d'accéder à des objets particuliers.
- L'identification unique permet à l'utilisateur d'ouvrir une session une seule fois sur un domaine Windows, en fournissant un seul mot de passe, et d'obtenir ainsi l'accès à tout ordinateur compris dans le domaine Windows. Cette fonction permet aux administrateurs de mettre en œuvre l'authentification par mot de passe dans l'ensemble du réseau Windows, tout en facilitant l'accès des utilisateurs.

Les sections qui suivent décrivent plus en détail ces trois éléments essentiels.

Authentification

L'authentification est un aspect fondamental de la sécurité du système; elle sert à confirmer l'identité de tout utilisateur qui tente d'ouvrir une session sur un domaine ou d'accéder à des ressources du réseau. Le maillon faible de la plupart des systèmes d'identification est le mot de passe de l'utilisateur.

Les mots de passe constituent la première ligne de défense contre tout accès non autorisé à un domaine et aux ordinateurs locaux. Recommandez au client d'appliquer les meilleures pratiques suivantes concernant les mots de passe :

- Toujours utiliser des mots de passe forts.
- Si les mots de passe doivent être écrits sur une feuille de papier, celle-ci doit être rangée dans un endroit sûr et détruite lorsqu'elle devient inutile.
- Les mots de passe ne doivent jamais être partagés.
- Chaque compte d'utilisateur doit avoir son propre mot de passe.
- Les mots de passe doivent être changés à intervalles fixes.
- Choisir avec soin l'emplacement où les mots de passe sont stockés sur les ordinateurs.

Mots de passe forts

Le rôle que jouent les mots de passe dans la sécurité d'un réseau est fréquemment sous-estimé et négligé. Tel que mentionné précédemment, les mots de passe constituent la première ligne de défense contre tout accès non autorisé au réseau. Vous devez donc vous assurer que vos clients demandent à leurs employés d'utiliser des mots de passe forts.

Toutefois, les outils de craquage de mots de passe ne cessent de s'améliorer et les ordinateurs qui servent au craquage sont plus puissants que jamais. Ces outils peuvent parvenir à percer tout mot de passe, s'ils disposent de suffisamment de temps. Cependant, les mots de passe forts sont beaucoup plus difficiles à percer que les mots de passe faibles.

Pour apprendre comment créer des mots de passe forts que les utilisateurs peuvent aisément mémoriser, consultez

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

et

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

Définition de la stratégie des mots de passe

Lorsque vous aidez un client à définir sa stratégie des mots de passe, veillez à créer une stratégie qui exige que tous les comptes d'utilisateur soient dotés d'un mot de passe fort. Pour la plupart des systèmes, les recommandations du document « Windows Server 2003 Security Guide » sont suffisantes :

- Définissez le paramètre **Conserver l'historique des mots de passe** de sorte que le système mette en mémoire un certain nombre des mots de passe précédents. Ce paramètre a pour but d'empêcher les utilisateurs d'employer le même mot de passe à l'expiration.

  Réglage recommandé : 24

- Définissez le paramètre **Durée de vie maximale du mot de passe** de sorte que les mots de passe expirent aussi souvent que nécessaire pour l'environnement du client.

  Réglage recommandé : entre 42 (valeur par défaut) et 90.

- Définissez le paramètre **Durée de vie minimale du mot de passe** de sorte que les mots de passe ne puissent être changés avant un certain nombre de jours de validité. Ce paramètre fonctionne conjointement avec le paramètre **Conserver l'historique des mots de passe**. Si vous définissez une durée de vie minimale des mots de passe, les utilisateurs ne peuvent changer plusieurs fois de suite leur mot de passe pour contourner le paramètre **Conserver l'historique des mots de passe** afin de revenir à leur mot de passe original. Les utilisateurs doivent attendre le nombre de jours spécifié pour changer leur mot de passe.

  Réglage recommandé : 2.

- Définissez le paramètre **Longueur minimale du mot de passe** de sorte que les mots de passe contiennent un certain nombre de caractères au minimum. Les mots de passe qui ont 7 caractères ou plus sont habituellement plus forts que les mots de passe courts. Ce paramètre empêche les utilisateurs de créer des mots de passe vides et les oblige à créer des mots de passe qui ont au moins un certain nombre de caractères.

  Réglage recommandé : 8.

- Activez le paramètre **Le mot de passe doit respecter des exigences de complexité**. Une fois ce paramètre activé, le système vérifie que tous les nouveaux mots de passe sont conformes aux exigences de base pour les mots de passe forts. Il vérifie que les mots de passe ont au moins trois signes pris dans quatre catégories (majuscules, minuscules, chiffres et symboles non alphanumériques) et qu'ils ne contiennent aucune partie du nom d'utilisateur, ni le prénom ou le nom de famille de l'utilisateur.

  Remarque
  Les mots de passe conformes à ces exigences ne sont pas nécessairement très forts. Le mot de passe « Motdepasse1 », par exemple, est conforme à ces exigences.

  Réglage recommandé : Oui

- Pour la liste complète de ces exigences, reportez-vous à la rubrique « Le mot de passe doit respecter des exigences de complexité » dans l'aide en ligne de Windows Server.
- Stockez les mots de passe avec le cryptage réversible – Le cryptage réversible est employé dans les systèmes où une application doit avoir accès à des mots de passe en texte clair. Il est inutile dans la plupart des déploiements.

  Réglage recommandé : Non.

Pour un complément d'information, voyez le document « Windows Server 2003 Security Guide », à l'adresse :

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

Définition d'une stratégie de verrouillage des comptes

Soyez prudent au moment de la définition d'une stratégie de verrouillage des comptes. Cette stratégie ne devrait jamais être employée dans une petite entreprise car elle risque fortement de bloquer l'accès à des utilisateurs autorisés, ce qui pourrait être très coûteux pour votre client.

Si le client décide d'appliquer la stratégie de verrouillage des comptes, réglez le paramètre **Seuil de verrouillage du compte** à une valeur suffisamment élevée pour que les utilisateurs autorisés ne voient pas leur compte bloqué simplement parce qu'ils ont fait une série d'erreurs de frappe pendant la saisie de leur mot de passe.

Pour un complément d'information sur la stratégie de verrouillage des comptes, voyez la rubrique « Aperçu de la stratégie de verrouillage du compte » dans l'aide en ligne de Windows Server.

Pour des instructions relatives à l'application ou à la modification de la stratégie de verrouillage des comptes, voyez la rubrique « Pour appliquer ou modifier une stratégie de verrouillage du compte » dans l'aide en ligne de Windows Server.

Contrôle d'accès

Il est possible de sécuriser un réseau Windows et ses ressources (y compris Navision) en considérant les droits dont les utilisateurs, groupes d'utilisateurs et autres ordinateurs disposent sur ce réseau. De la même manière, vous pouvez sécuriser un ou plusieurs ordinateurs en accordant certains droits à des utilisateurs ou groupes d'utilisateurs. Vous pouvez sécuriser un objet, comme un fichier ou un dossier, en lui attribuant des autorisations qui permettent à des utilisateurs ou des groupes d'exécuter certaines actions sur cet objet. Les principaux concepts du contrôle d'accès sont les suivants :

- Autorisations
- Propriété d'objets
- Héritage d'autorisations
- Droits d'utilisateur
- Audit d'objets

Autorisations

Les autorisations définissent le type d'accès accordé à un utilisateur ou groupe pour un objet ou une propriété d'objet, comme les fichiers, dossiers et objets du registre. Les autorisations s'appliquent à tous les objets sécurisés, tels que fichiers et objets du registre. Elles peuvent être accordées à tout utilisateur, groupe ou ordinateur. Il est recommandé d'accorder les autorisations au niveau des groupes.

Propriété d'objets

Au moment de la création d'un objet, le système attribue automatiquement un propriétaire à cet objet. Dans Windows 2000 Server, le propriétaire est par défaut le créateur de l'objet. Cette règle a été modifiée dans Windows Server 2003 pour les objets créés par des membres du groupe Administrateurs.

Lorsqu'un membre du groupe Administrateurs crée un objet dans Windows Server 2003, c'est le groupe Administrateurs qui devient le propriétaire de l'objet plutôt que la personne qui l'a créé. Cette règle peut être modifiée au moyen du composant logiciel enfichable de paramètres de sécurité locaux Microsoft Management Console (MMC), en réglant le paramètre **Objets système : propriétaire par défaut pour les objets créés par les membres du groupe Administrateurs**. Le propriétaire d'un objet peut toujours modifier les autorisations définies pour un objet, quelles que soient ces autorisations.

Pour un complément d'information, voyez la rubrique « Prise de possession » dans l'aide en ligne de Windows Server.

Héritage d'autorisations

Le concept d'héritage facilite l'attribution et la gestion des autorisations par les administrateurs. Lorsque cette fonction est activée, tous les objets compris dans un conteneur héritent automatiquement de toutes les autorisations de ce conteneur qui peuvent être héritées. Par exemple, lorsque vous créez des fichiers dans un dossier, les fichiers héritent des autorisations du dossier. L'héritage s'applique exclusivement aux autorisations qui sont marquées à cet effet.

Droits d'utilisateur

Les droits d'utilisateur accordent des privilèges et droits d'ouverture de session aux utilisateurs et groupes de votre environnement informatique.

Pour un complément d'information, voyez « Droits des utilisateurs » dans l'aide en ligne de Windows Server.

Audit d'objets

Vous pouvez créer un registre de l'accès des utilisateurs à des objets. Vous pouvez ensuite voir les éléments consignés dans le journal de sécurité au moyen de l'Observateur d'événements.

Pour un complément d'information, voyez « Audit » dans l'aide en ligne de Windows Server.

Meilleures pratiques du contrôle d'accès

- Accordez les autorisations à des groupes plutôt qu'à des utilisateurs. Comme il est inefficace de maintenir directement les comptes d'utilisateur, vous ne devriez accorder qu'exceptionnellement des autorisations à un utilisateur.
- La fonction Refuser les autorisations peut être employée dans certains cas. Elle peut servir, par exemple, à exclure un sous-ensemble d'un groupe auquel des autorisations ont été accordées.
- Ne refusez jamais au groupe Tout le monde l'accès à un objet, car ce groupe comprend les administrateurs. Il est préférable de supprimer le groupe Tout le monde, dans la mesure où vous accordez à d'autres utilisateurs, groupes ou ordinateurs des autorisations d'accès à cet objet. Rappelez-vous qu'il est impossible d'accéder à un objet si des autorisations n'ont pas été définies.
- Accordez les autorisations à l'objet le plus élevé possible sur l'arborescence et appliquez ensuite la fonction d'héritage pour propager les paramètres de sécurité dans l'ensemble de l'arbre. Vous pouvez rapidement et efficacement appliquer des paramètres de contrôle d'accès à tous les enfants d'un sous-arbre d'un objet parent. De cette manière, vous produisez le plus grand effet possible pour le moindre effort. Les paramètres d'autorisation que vous établissez devraient être suffisants pour la majorité des utilisateurs, groupes et ordinateurs.
- Les autorisations explicites peuvent parfois avoir priorité sur des autorisations héritées. Par exemple, l'héritage d'un refus d'autorisation n'empêche pas l'accès à un objet si une autorisation explicite a été accordée pour cet objet. Les autorisations explicites ont priorité sur les autorisations héritées et sur les refus d'autorisation hérités.
- Pour les autorisations relatives à des objets Active Directory®, assurez-vous de bien comprendre les meilleures pratiques qui ont été définies pour ces objets.

Pour un complément d'information, voyez la rubrique « Recommandations pour l'attribution des autorisations pour les objets Active Directory » dans l'aide en ligne de Windows Server 2003.

Pare-feu externe

Un pare-feu est un composant matériel ou logiciel qui empêche des paquets de données d'entrer ou de quitter un certain réseau. Le contrôle du flux du trafic s'obtient en ouvrant ou en fermant certains ports du pare-feu pour les paquets d'information. Le pare-feu recherche certains éléments d'information dans chaque paquet, à savoir : le protocole sous lequel le paquet est livré, la destination ou l'émetteur du paquet, le type du contenu du paquet et le numéro du port auquel le paquet est adressé. Le pare-feu laisse le paquet entrer si le port de destination est configuré pour accepter le protocole spécifié. Microsoft Windows Small Business Server 2003, Édition Premium est livré avec Microsoft Internet Security and Acceleration (ISA) Server 2000 en tant que solution de pare-feu. Le logiciel Small Business Server, Édition Standard comprend également un pare-feu.

ISA Server 2004

Le système ISA (Internet Security and Acceleration) Server 2004 achemine en toute sécurité les requêtes et réponses qui circulent entre Internet et les ordinateurs clients sur le réseau interne.

ISA Server fait fonction de passerelle sécurisée vers Internet pour les clients du réseau local. L'ordinateur ISA Server est transparent pour tous les autres utilisateurs du trajet de communication. Normalement, les utilisateurs d'Internet ne devraient pas être capables de détecter la présence d'un serveur pare-feu, sauf s'ils tentent d'accéder à un service ou un site pour lequel l'ordinateur ISA Server refuse l'accès. Le serveur Internet qui fait l'objet de l'accès interprète les requêtes de l'ordinateur ISA Server comme si elles provenaient de l'application client.

Si vous activez le filtrage des fragments IP (Internet Protocol), vous permettez aux services de pare-feu et Proxy Web de filtrer les fragments de paquet. Ceci a pour effet d'éliminer tous les paquets IP fragmentés. Une méthode d'attaque bien connue consiste à envoyer des paquets fragmentés et à les réassembler ensuite de telle façon qu'ils puissent nuire au système.

ISA Server comporte un mécanisme de détection d'intrusion, qui détermine le moment auquel une attaque est tentée contre un réseau et qui exécute alors une série d'actions configurées (ou alertes).

Si les services IIS (Internet Information Services) ont été installés sur l'ordinateur ISA Server, vous devez les configurer de façon qu'ils n'utilisent pas les ports utilisés par l'ordinateur ISA Server pour les requêtes Web sortantes (port 8080, par défaut) et pour les requêtes Web entrantes (port 80, par défaut). Par exemple, vous pouvez configurer les services IIS pour qu'ils surveillent le port 81 et configurer ensuite l'ordinateur ISA Server pour qu'il dirige les requêtes Web entrantes vers le port 81 de l'ordinateur local qui exécute IIS.

S'il y a conflit entre les ports utilisés par ISA Server et IIS, le programme d'installation arrête le service de publication IIS. Dans ce cas, vous pouvez configurer les services IIS pour qu'ils surveillent un autre port et redémarrer le service de publication IIS.

Stratégies relatives à ISA Server

Vous pouvez définir une stratégie ISA Server qui régit les accès entrants et sortants. Les règles de sites et contenus spécifient les sites et les contenus auxquels les utilisateurs peuvent accéder. Les règles de protocoles spécifient si un certain protocole est utilisable ou non pour les communications entrantes et sortantes.

Vous pouvez créer des règles de sites et de contenus, des règles de protocole, des règles de publication Web et des filtres de paquets IP. Ces règles déterminent comment les clients ISA Server communiquent avec Internet et quelles communications sont autorisées.

Protection contre les virus

Un virus informatique est un fichier exécutable qui est conçu pour se reproduire, effacer ou altérer des fichiers de données et programmes et éviter d'être détecté. Il arrive fréquemment que les virus soient réécrits et modifiés pour éviter la détection. Les virus sont souvent envoyés sous forme de pièces jointes à un message électronique. Les programmes antivirus doivent être continuellement mis à jour pour être capables de détecter les nouveaux virus et les virus modifiés. Les virus constituent la méthode par excellence de vandalisme informatique.

Les logiciels antivirus sont spécifiquement conçus pour la détection et la prévention des virus. Comme les pirates créent sans cesse de nouveaux virus, de nombreux fabricants de produits antivirus offrent à leur clientèle des mises à jour périodiques de leur logiciel. Microsoft recommande fortement l'implantation d'un logiciel antivirus dans l'environnement de vos clients.

Habituellement, un logiciel antivirus doit être installé dans chacun des trois emplacements suivants : les postes de travail des utilisateurs, les serveurs et le réseau par lequel les messages électroniques entrent dans l'organisation (et, dans certains cas, en sortent).

Types de virus

Les virus qui infectent les systèmes informatiques se répartissent en trois grandes catégories : virus du secteur de démarrage, virus qui infectent des fichiers et chevaux de Troie.

Virus du secteur de démarrage

Lorsqu'il démarre, l'ordinateur balaie le secteur de démarrage du disque dur avant de charger le système d'exploitation et les autres fichiers de démarrage. Les virus du secteur de démarrage sont conçus pour remplacer par leur propre code l'information contenue dans le secteur de démarrage du disque dur. Lorsqu'un ordinateur est infecté par un virus du secteur de démarrage, il charge le code de ce virus en mémoire avant toute autre information. Une fois que le virus est en mémoire, il peut se reproduire sur tous les autres disques qui sont utilisés dans l'ordinateur infecté.

Virus qui infectent des fichiers

Ce type de virus est le plus courant; il se fixe à un fichier de programme exécutable en y ajoutant son propre code. L'ajout du code se fait habituellement de façon à éviter toute détection. Lorsque le fichier infecté est exécuté, le virus peut se fixer sur d'autres fichiers exécutables. Les fichiers infectés par ce type de virus portent habituellement une extension .com, .exe ou .sys.

Certains virus qui infectent des fichiers sont destinés à des programmes particuliers. Les types de programme fréquemment ciblés sont les fichiers overlay (.ovl) et les fichiers de bibliothèque de liens dynamiques (.dll). Ces fichiers ne sont pas exécutés, mais ils sont appelés par des fichiers exécutables. Le virus est transmis au moment de l'appel.

L'altération des données a lieu au moment du déclenchement du virus. Un virus peut être déclenché lors de l'exécution d'un fichier infecté ou de l'activation d'un certain paramètre de l'environnement (comme une date système).

Chevaux de Troie

Un cheval de Troie n'est pas réellement un virus. Ce qui le distingue d'un virus, c'est le fait qu'il ne se reproduit pas; son rôle consiste simplement à détruire l'information stockée sur le disque dur. Un cheval de Troie se fait passer pour un programme légitime, comme un jeu ou un utilitaire. Cependant, au moment de son exécution, il peut détruire ou embrouiller les données.

Recommandations en matière de protection contre les virus

Il est possible d'empêcher les virus macros de se répandre. Voici certains conseils que vous devriez transmettre à vos clients :

- Installez une solution antivirus qui balaie les messages provenant d'Internet afin de détecter les virus avant que les messages ne franchissent le routeur. Ceci garantira la détection des virus connus dans les messages électroniques.
- Sachez d'où proviennent les documents reçus. N'ouvrez jamais les documents s'ils ne proviennent pas d'une personne en qui vous avez confiance.
- Parlez à la personne qui a créé le document. Si vous n'êtes pas certain qu'un document est sécuritaire, vous devriez entrer en contact avec la personne qui l'a créé.
- Servez-vous de la protection contre les virus macros de Microsoft Office. Les applications Office préviennent l'utilisateur lorsqu'un document contient des macros. Cette fonction permet à l'utilisateur d'activer ou de désactiver les macros au moment de l'ouverture du document.
- Servez-vous d'un logiciel de détection de virus pour détecter et supprimer les virus macros. Ce type de logiciel peut détecter et souvent supprimer les virus macros que contiennent les documents. Microsoft recommande d'utiliser un logiciel antivirus homologué par l'International Computer Security Association (ICSA).

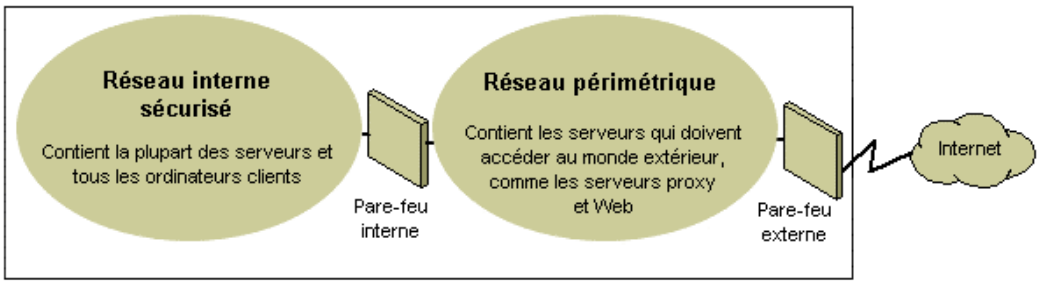
Pour un complément d'information sur les virus et la sécurité informatique en général, visitez les sites Web Microsoft suivants :

- Microsoft Security, à l'adresse http://www.microsoft.com/security/default.asp.
- Documentation sur la sécurité de Microsoft TechNet, à l'adresse http://www.microsoft.com/technet/security/Default.mspx.

Stratégies de sécurité du réseau

La conception et le déploiement d'un environnement d'interconnexion de réseaux IP nécessitent un équilibre entre les intérêts des réseaux privés et publics. Pour cette raison, le pare-feu est devenu l'ingrédient de choix dans la protection de l'intégrité des réseaux. Le pare-feu n'est pas un composant unique. Selon la définition de la National Computer Security Association (NCSA), un pare-feu est « un système ou une combinaison de systèmes qui crée une frontière entre deux ou plusieurs réseaux ». Bien que différents termes soient employés, cette frontière est fréquemment appelée réseau périmétrique. Le réseau périmétrique protège votre intranet ou votre réseau local d'entreprise contre toute intrusion en contrôlant les accès en provenance d'Internet ou d'autres grands réseaux.

Le schéma ci-dessous présente un réseau périmétrique, délimité par des pare-feu et placé entre un réseau privé et Internet afin de sécuriser le réseau privé :



Réseau périmétrique de base

Il existe différentes façons d'utiliser les pare-feu pour assurer la sécurité d'un réseau. Le filtrage de paquets IP offre une protection limitée, est difficile à gérer et peut aisément être déjoué. Les passerelles d'applications offrent une meilleure protection que les filtres de paquets et sont plus faciles à gérer, car elles s'appliquent uniquement à un petit nombre d'applications, comme un certain système de courrier électronique. Les passerelles de circuit sont plus efficaces lorsque les utilisateurs d'une application réseau causent plus de risques que les données transmises par cette application. Le serveur proxy est un outil complet de sécurité, qui comprend une passerelle d'applications, un accès sécurisé pour les utilisateurs anonymes et d'autres services. Voici quelques informations sur ces différentes options :

- **Filtrage de paquets IP**
  Le filtrage de paquets IP a été la première mise en œuvre de la technologie des pare-feu. Cette fonction extrait des en-têtes de paquets les adresses source et de destination, les numéros de port TCP (Transmission Control Protocol) et UDP (User Datagram Protocol) et d'autres informations. Le filtrage de paquets est cependant une technologie limitée qui convient idéalement aux environnements dans lesquels les règles de sécurité sont claires; il peut s'agir, par exemple, d'un environnement où tout ce qui est à l'extérieur du réseau périmétrique n'est pas fiable alors que tout ce qui est à l'intérieur l'est. Au cours des dernières années, certains fournisseurs ont amélioré la méthode de filtrage de paquets en y incorporant des fonctions de prise de décision intelligentes, créant ainsi une nouvelle forme de filtrage de paquets appelée *stateful*

protocol inspection (inspection dynamique de protocoles). Il existe deux configurations possibles pour le filtrage des paquets, soit l'acceptation de certains types de paquets et le refus de tous les autres, ou le refus de certains types de paquets et l'acceptation de tous les autres.

- **Passerelles d'applications**
  Les passerelles d'applications s'emploient lorsque le contenu d'une application est la principale cause de risque. Le fait que ces passerelles se rapportent à certaines applications constitue aussi bien leur force que leur limite, car elles ne peuvent s'adapter aisément aux changements technologiques.
- **Passerelles de circuit**
  Les passerelles de circuit sont des tunnels qui traversent un pare-feu pour connecter un certain nombre de processus ou systèmes de part et d'autre du pare-feu. Elles conviennent idéalement aux situations où les utilisateurs d'une application constituent un risque potentiel plus élevé que les informations transmises par l'application. Elles se distinguent des filtres de paquets en ce qu'elles peuvent se connecter à un mécanisme d'application hors bande qui peut ajouter des informations additionnelles.
- **Serveurs proxy**
  Les serveurs proxy sont des outils complets de sécurité, comprenant un pare-feu et une passerelle d'applications qui gère le trafic Internet en provenance et à destination d'un réseau local. Ils assurent en outre la mise en cache de documents et le contrôle d'accès. Ils peuvent améliorer les performances en fournissant directement à partir d'un cache les données fréquemment demandées, comme une page Web populaire. Ils peuvent également filtrer et rejeter les requêtes que le propriétaire ne juge pas appropriées, comme les requêtes d'accès non autorisé à des fichiers exclusifs.

Veillez à ce que vos clients mettent en place les fonctions de sécurité par pare-feu qui peuvent les aider. Dans la topologie du réseau, prévoyez un réseau périmétrique à l'endroit où doit passer tout le trafic provenant de l'extérieur du réseau de l'entreprise, et protégez le réseau périmétrique par un pare-feu externe. Vous pouvez préciser les paramètres de contrôle d'accès du pare-feu afin de répondre aux besoins du client et vous le configurer pour qu'il identifie toutes les tentatives d'accès non autorisées.

Pour réduire au minimum le nombre de ports que vous devez ouvrir sur le pare-feu interne, vous pouvez utiliser un pare-feu de couche application, comme l'ISA Server 2000.

Pour un complément d'informations sur les réseaux TCP/IP, voyez « Designing a TCP/IP Network », à l'adresse http://www.microsoft.com/resources/documentation/WindowsServ/2003/all/deployguide/en-us/dnsbb_tcp_overview.asp.

Réseaux sans fil

La configuration par défaut des réseaux sans fil permet généralement l'écoute clandestine des signaux. Ils sont vulnérables aux intrusions en raison des paramètres par défaut de certains éléments matériels, de l'accessibilité qu'ils offrent et des méthodes actuelles de cryptage. Ils comportent des options et outils de configuration qui protègent le réseau contre l'écoute clandestine, mais il faut garder à l'esprit que ces options et outils ne protègent en rien les ordinateurs contre les pirates et virus qui pénètrent dans le réseau par la connexion Internet. Par conséquent, il est extrêmement important d'inclure un pare-feu pour protéger les ordinateurs contre les intrusions à partir d'Internet.

Pour un complément d'informations sur la protection d'un réseau sans fil, voyez « How to Make Your 802.11b Wireless Home Network More Secure », à l'adresse http://support.microsoft.com/default.aspx?scid=kb;en-us;309369.

Scénarios de sécurité du réseau

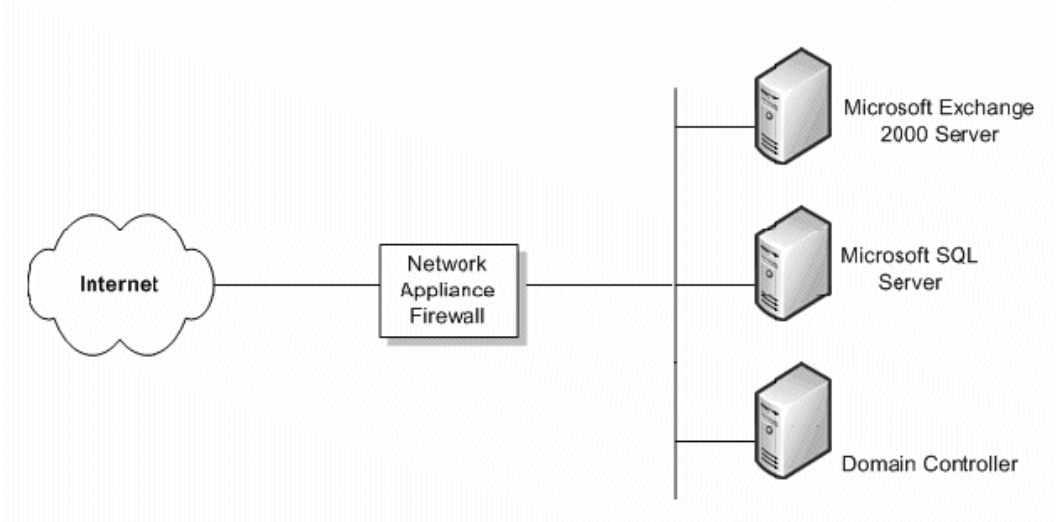
Le niveau de sécurité de réseau dont l'organisation cliente a besoin dépend d'un certain nombre de facteurs. La décision résulte habituellement d'un compromis entre le budget du client et la nécessité d'assurer la sécurité des données de l'entreprise. Il est possible d'équiper une petite entreprise d'une structure de sécurité très complexe qui fournit le plus haut niveau possible de sécurité au réseau, mais le prix d'une telle structure peut être prohibitif. La présente section examine quatre scénarios possibles et fait des recommandations qui procurent différents niveaux de sécurité.

Pas de pare-feu

Si votre client a une connexion Internet mais pas de pare-feu, vous devez mettre en place certaines mesures de sécurité du réseau. Il existe sur le marché des serveurs monofonctionnels de pare-feu qui fournissent une protection suffisante pour décourager la plupart des pirates.

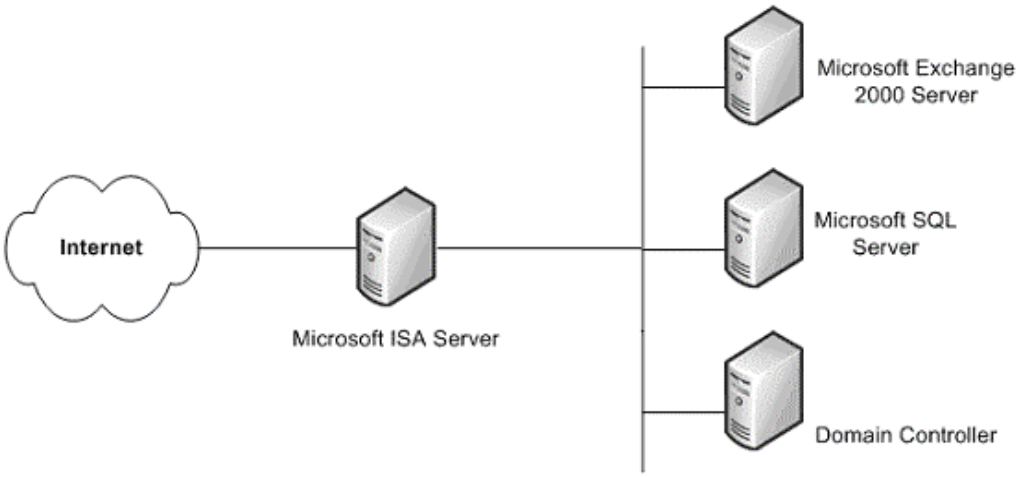
Un pare-feu simple

Le niveau minimum de sécurité consiste à installer un pare-feu simple entre Internet et les données de votre client. Ce pare-feu ne fournit pas nécessairement un niveau élevé de sécurité et ne devrait pas être considéré comme très sûr. Mais il est préférable à l'absence de pare-feu.



Un pare-feu simple

Il est à espérer que le budget du client autorisera une meilleure solution pour la protection des données de l'entreprise. Dans ce cas, vous pouvez installer un serveur Microsoft ISA Server. Malgré son coût plus élevé, ce serveur additionnel fournit un niveau de sécurité de beaucoup supérieur à celui d'un pare-feu bas de gamme, car ce dernier n'assure habituellement que le filtrage de paquets et la traduction d'adresses réseau (NAT).



Pare-feu ISA Server

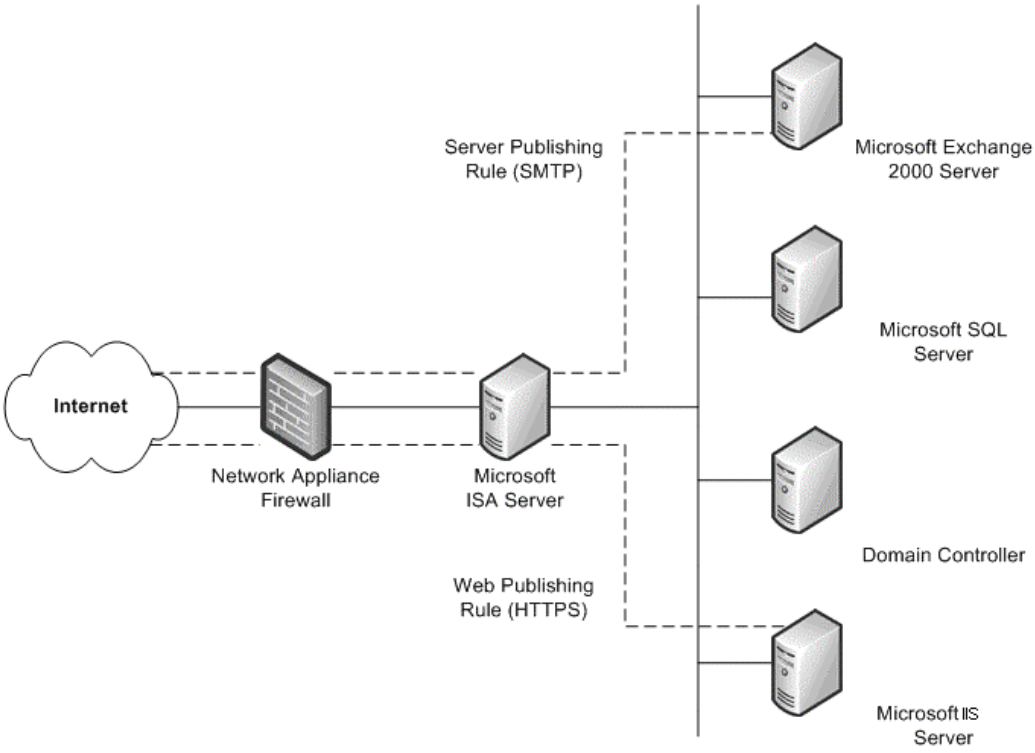
Cette solution de pare-feu unique est supérieure à celle d'un pare-feu bas de gamme et fournit en outre des services de sécurité propres à Windows.

Un pare-feu existant

Si le client est déjà équipé d'un pare-feu qui sépare son intranet d'Internet, vous pouvez envisager d'installer un pare-feu additionnel qui fournira de multiples moyens de configurer l'accès à Internet par les ressources internes.

Une des méthodes possibles est la publication Web. Cette méthode s'emploie lorsqu'un pare-feu ISA Server est installé en avant du serveur Web qui permet aux utilisateurs de l'organisation d'accéder à Internet. L'ordinateur ISA Server peut se présenter au monde extérieur comme un serveur Web, en répondant aux requêtes Web entrantes et en envoyant aux clients les contenus Web stockés dans son cache. L'ordinateur ISA Server ne transmet au serveur Web que les requêtes auxquelles il ne peut répondre à partir de son cache.

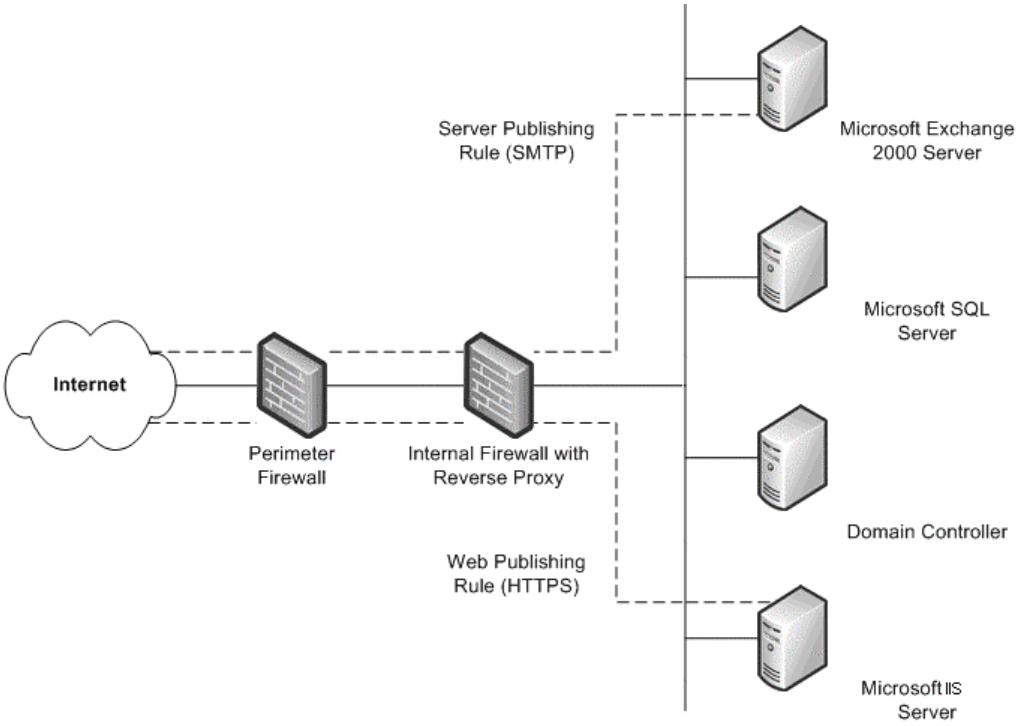
La publication de serveurs est une autre méthode possible. ISA Server permet de publier les serveurs internes sur Internet sans compromettre la sécurité du réseau interne. Vous pouvez configurer des règles de publication de serveurs et de publication Web afin de déterminer les requêtes qui doivent être envoyées à un certain serveur du réseau local, formant ainsi une couche additionnelle de sécurité pour les serveurs internes.



Pare-feu existant avec ISA Server

Deux pare-feu existants

Le quatrième scénario est celui où l'organisation a déjà installé deux pare-feu qui délimitent un réseau périmétrique (zone démilitarisée). Au moins un de ces pare-feu fournit des services de proxy inverse afin d'empêcher les clients Internet d'accéder directement aux serveurs de l'intranet. L'un des pare-feu, idéalement le pare-feu interne, intercepte les requêtes réseau pour les serveurs internes, inspecte les paquets et les transmet ensuite pour le compte de l'hôte Internet.



Deux pare-feu existants

Ce scénario est semblable au scénario précédent une fois que le second pare-feu a été ajouté. La seule différence est que le pare-feu interne qui agit comme proxy inverse n'est pas un pare-feu ISA Server. Dans ce scénario, vous devrez collaborer étroitement avec les administrateurs de chaque pare-feu afin de définir des règles de publication de serveurs qui respectent la stratégie de sécurité de l'entreprise.

Gestion des correctifs de sécurité

Les systèmes d'exploitation et les applications sont souvent d'une immense complexité. Ils peuvent se composer de millions de lignes de code, rédigées par un grand nombre de programmeurs. Il est essentiel que le logiciel fonctionne de façon fiable, sans compromettre la sécurité ni la stabilité de l'environnement TI. Pour réduire au minimum les problèmes éventuels, les programmes sont soumis à des tests rigoureux avant leur publication. Cependant, comme les pirates s'efforcent continuellement de découvrir les points faibles des logiciels, il est impossible de prévoir toutes les attaques futures.

Pour de nombreuses organisations, la gestion des correctifs fait partie intégrante de leur stratégie globale de gestion des configurations et des changements. Cependant, quelle que soit la nature et la taille d'une organisation, il est essentiel qu'elle possède une bonne stratégie de gestion des correctifs, même si elle n'a pas encore une stratégie efficace de gestion des configurations et changements. Dans la majorité des cas, les attaques contre des systèmes informatiques réussissent lorsque les correctifs de sécurité n'ont pas été installés sur ces systèmes.

Les correctifs de sécurité constituent un défi particulier pour la plupart des organisations. Une fois qu'une faiblesse a été exposée dans un logiciel, l'information se répand très rapidement dans l'ensemble de la communauté des pirates. À partir de cet instant, Microsoft s'efforce de publier le plus rapidement possible le correctif de sécurité. Dans l'intervalle, la sécurité à laquelle s'attend le client et de laquelle il dépend peut être gravement réduite.

Vous devez vous assurer que vos clients ont installé les plus récents correctifs de sécurité dans l'ensemble de leur système Navision. Veillez à ce que le client utilise l'une des technologies offertes par Microsoft, à savoir :

- **Service de notification de sécurité de Microsoft**
  Ce service envoie à une liste de courrier électronique des notifications chaque fois qu'une mise à jour devient disponible. Les notifications forment un précieux élément de toute stratégie de sécurité proactive. Elles sont également disponibles sur le site Web de TechNet Product Security Notification, à l'adresse : http://www.microsoft.com/technet/security/bulletin/notify.mspx.
- **Mises à jour automatiques de Microsoft**
  Windows peut automatiquement appliquer les mises à jour de sécurité aux machines des clients.
- **Outil de recherche sur les bulletins de sécurité Microsoft**
  Cet outil est disponible sur le site Web Security Bulletin Service, à l'adresse : http://www.microsoft.com/technet/security/current.aspx. Il permet au client de déterminer les mises à jour dont il a besoin, en fonction du système d'exploitation, des applications et des service packs qu'il utilise actuellement.

- **Microsoft Baseline Security Analyzer (MBSA)**
  Cet outil graphique est disponible sur le site Web Microsoft Baseline Security Analyzer, à l'adresse : http://www.microsoft.com/technet/security/tools/mbsahome.mspx. Il fonctionne en comparant l'état actuel d'un ordinateur à la liste des mises à jour de Microsoft. Il effectue également certains contrôles de sécurité de base, concernant la force des mots de passe et les paramètres d'expiration, les stratégies relatives aux comptes d'invité et un certain nombre d'autres domaines. Il recherche également les vulnérabilités dans les services Internet IIS, SQL Server™ 2000, Exchange 5.5, Exchange 2000 et Exchange Server 2003.
- **Microsoft Software Update Services (SUS)**
  Anciennement appelé Windows Update Corporate Edition, cet outil permet aux entreprises d'installer sur des ordinateurs locaux toutes les mises à jour critiques et les SRP (Security Rollup Packages) disponibles sur le site public de mise à jour Windows. Il fonctionne avec une nouvelle version des clients AU (Automatic Update), formant ainsi la base d'une puissante stratégie de téléchargement et d'installation automatiques. Le nouvel ensemble de clients AU comprend un client pour les systèmes d'exploitation Windows 2000 et Windows Server 2003 et peut installer automatiquement les mises à jour téléchargées. Pour un complément d'information sur les services Microsoft SUS, consultez le site http://www.microsoft.com/windows2000/windowsupdate/sus/default.asp.
- **Microsoft Systems Management Server (SMS) Software Update Services Feature Pack**
  Le SMS Software Update Services Feature Pack contient un certain nombre d'outils qui ont pour but de faciliter la distribution des mises à jour de logiciel dans l'ensemble de l'entreprise. Ces outils comprennent un outil d'inventaire des mises à jour de sécurité, un outil d'inventaire des mises à jour pour Microsoft Office, un assistant de distribution des mises à jour de logiciel et un outil de production de rapports Web SMS, avec logiciel complémentaire Web Reports pour les mises à jour de logiciel. Pour un complément d'informations sur chaque outil, consultez le site http://www.microsoft.com/smserver/downloads/20/featurepacks/suspack/.

Parlez à vos clients de chacun de ces outils et encouragez-les à les utiliser. Il est très important de régler le plus rapidement possible les questions de sécurité, tout en maintenant la stabilité de l'environnement.

Paramètres de sécurité SQL Server 2000

Comme Navision peut également s'exécuter sur SQL Server 2000, il est important que vous preniez les mesures nécessaires pour améliorer la sécurité de l'installation SQL Server 2000 de vos clients. Les principales étapes à exécuter sont les suivantes :

- Veillez à installer les plus récents service packs et les dernières mises à jour sur le système d'exploitation et sur l'ordinateur SQL Server 2000. Pour un complément d'informations, consultez le site Web Microsoft Security, à l'adresse : http://www.microsoft.com/security/default.asp.
- Pour la sécurité de niveau système des fichiers, veillez à ce que toutes les données et tous les fichiers système SQL Server 2000 soient installés dans des partitions NTFS. Ces fichiers ne devraient être accessibles qu'aux utilisateurs de niveau administration ou système, par l'intermédiaire d'autorisations NTFS. De cette manière, vous empêcherez les utilisateurs d'accéder à ces fichiers lorsque le service MSSQLSERVER ne fonctionne pas.

- Servez-vous d’un compte de domaine à faibles privilèges, tel que Autorité NT\ Service réseau ou Sytème local (recommandé), pour le service SQL Server 2000 (MSSQLSERVER). Ce compte devrait avoir le minimum de droits dans le domaine, ce qui devrait contribuer à contenir (sans nécessairement arrêter) une attaque contre le serveur, si la sécurité est compromise. En d’autres termes, ce compte ne devrait disposer que d'autorisations de niveau utilisateur local dans le domaine. Lorsqu’un compte d’administrateur de domaine est utilisé pour fournir le service SQL Server 2000, c’est tout le domaine qui est menacé lorsque la sécurité du serveur est compromise. Pour modifier ce paramètre, servez-vous de l’outil SQL Server Enterprise Manager. Cet outil change automatiquement les listes de contrôle d’accès (ACL) sur fichiers, le registre et les droits d’utilisateur.
- Les éditions de SQL Server 2000 sont pour la plupart installées avec deux bases de données par défaut, **Northwind** et **pubs**. Ces deux bases de données contiennent des exemples qui servent aux essais et à la formation. Elles ne devraient pas être installées dans le système de production. La présence de ces bases de données peut en effet encourager les pirates à tenter d’exploiter les faiblesses des paramètres et des configurations par défaut. Si les bases de données **Northwind** et **pubs** sont présentes sur l’ordinateur SQL Server 2000 de production, elles devraient être supprimées.
- L’audit du système SQL Server 2000 est désactivé par défaut, de sorte qu’aucune condition n’est vérifiée. Ceci rend plus difficile la détection des intrusions et aide les attaquants à brouiller leurs pistes. Vous devriez au minimum activer l’audit des échecs d’ouverture de session.

Pour les informations les plus récentes sur la sécurité SQL Server 2000, voyez http://www.microsoft.com/sql/techinfo/administration/2000/security/default.asp.

À propos de Microsoft Business Solutions

Microsoft Business Solutions, une division de Microsoft, offre une gamme étendue d'applications et de services de gestion entièrement intégrée, afin d'aider les PME et les grandes entreprises à développer leurs relations avec leurs clients, employés, partenaires et fournisseurs. Les logiciels de Microsoft Business Solutions optimisent les processus stratégiques dans les domaines de la gestion financière, de l'analyse, des ressources humaines, de la gestion de projet, de la relation client, du service après vente, de la chaîne logistique d'approvisionnement, du commerce électronique, de la fabrication et de la vente au détail. Ces applications sont conçues pour fournir les informations indispensables à la réussite des entreprises. De plus amples informations sur Microsoft Business Solutions sont disponibles sur le site http://www.microsoft.com/BusinessSolutions/