Microsoft Business Solutions

Navision Security Hardening Guide

Publication : octobre 2004

Microsoft

Table des matières

Introduction

Microsoft® Windows® fournit un système de sécurisation de réseau sophistiqué et normatif. De manière générale, la sécurité implique la planification et l'instauration de compromis. Par exemple, il est possible d'enfermer un ordinateur dans un coffre et de n'en donner l'accès qu'à un seul administrateur système. Cet ordinateur sera sécurisé, mais pas très utile car il ne sera connecté à aucun autre ordinateur. Vous devez donc envisager de sécuriser le réseau au maximum, sans porter préjudice à sa commodité d'utilisation.

Si la plupart des organisations installent des pare-feu en prévision d'attaques de l'extérieur, peu d'entre elles envisagent le moyen de limiter la brèche de sécurité en cas d'irruption d'un utilisateur malintentionné dans le réseau protégé par le pare-feu. Les mesures de sécurité protégeant l'environnement de votre client seront efficaces si les utilisateurs n'ont pas trop de procédures et d'étapes à suivre pour sécuriser leurs activités. La mise en œuvre des stratégies de sécurité doit être aussi simple que possible pour les utilisateurs, faute de quoi ils trouveront le moyen d'agir en contournant les règles de sécurité.

La taille des installations de Navision pouvant varier fortement, il importe de prendre en compte précisément les besoins de chaque client et d'évaluer l'efficacité du système de sécurité comparé aux coûts qu'il implique. En tant que conseiller de votre client, vous devez procéder avec discernement et lui recommander une stratégie qui réponde à ses besoins en matière de sécurité tout en étant assez souple pour qu'il l'applique sans faille.

Navision : recommandations en matière de sécurité

Les grands principes ci-dessous permettent d'accroître la sécurité d'un environnement Navision :

- Si vous exécutez le serveur de base de données Navision en tant que service ou que vous utilisez le paramètre de ligne de commande *installasservice* au démarrage du serveur, assurez-vous que le service est exécuté en tant que compte NT Authority\Network Service. Le compte NT Authority\Network Service n'existe que sous Windows™ XP et Windows Server™ 2003. Si vous exécutez Windows 2000 Server, créez un compte doté des privilèges minimaux pour ce service, faute de quoi un compte Local System sera affecté au service. Ce compte doit, au maximum, comporter les mêmes droits que le compte Utilisateurs normal ou être un compte de domaine qui ne soit ni administrateur du domaine, ni administrateur d'un ordinateur local.

  Pensez à donner au compte NT Authority\Network Service ou au compte utilisateur sous lequel le serveur est exécuté l'accès en lecture et en écriture aux fichiers de la base de données afin que les utilisateurs puissent se connecter à celle-ci.

  Pour donner au compte NT Authority\Network Service des droits d'accès en lecture et en écriture à un fichier de base de données sous Windows XP :

  1. Parcourez l'Explorateur Windows jusqu'au dossier contenant le fichier de base de données.
  2. Sélectionnez le fichier de base de données et cliquez dessus avec le bouton droit de la souris, puis cliquez sur Propriétés.
  3. Dans la fenêtre ***Propriétés***, cliquez sur l'onglet ***Sécurité***, puis dans le champ **Noms de groupe et d'utilisateur**, cliquez sur Ajouter.
  4. Dans la fenêtre ***Sélectionner les utilisateurs, les ordinateurs ou les groupes***, entrez *Service réseau* et cliquez sur OK.
  5. La valeur SERVICE RESEAU est ajoutée au champ **Noms de groupe et d'utilisateur** de la fenêtre ***Propriétés***.
  6. Sélectionnez SERVICE RESEAU, puis dans le champ **Autorisations**, activez les droits *Lecture* et *Ecriture*.

- Le service Navision Application Server est maintenant exécuté en tant que compte NT Authority\Network Service par défaut, ce qui lui permet d'accéder localement au serveur de base de données Navision. Toutefois, dans un réseau, vous devez vous assurer que le service Navision Application Server est exécuté en tant que compte utilisateur de domaine Windows reconnu par le serveur de base de données Navision si vous souhaitez qu'il ait accès au serveur de base de données. Ce compte ne doit pas non plus être un administrateur du domaine ni un administrateur d'un ordinateur local.

- Si vous exécutez la version SQL Server pour Navision, Microsoft SQL Server™ est exécuté en tant que service. L'exécution de la version SQL Server pour Navision suppose que SQL Server puisse consulter Active Directory afin d'obtenir des listes de groupes d'utilisateurs Windows à des fins d'authentification. Vous devez donc vérifier que le service SQL Server est exécuté en tant que compte NT Authority\Network Service.

  Pour exécuter ce service en tant que compte NT Authority\Network Service :

  1. Dans l'ordinateur sur lequel est exécuté SQL Server, accédez au service MSSQLSERVER, cliquez dessus avec le bouton droit de la souris, puis cliquez sur Propriétés.
  2. Dans la fenêtre ***Propriétés***, cliquez sur l'onglet ***Se connecter à***.
  3. Dans l'onglet ***Se connecter à***, cliquez sur Ce compte dans le champ Se connecter en tant que et entrez *NT Authority\NetworkService*, puis cliquez sur OK.

  Pour plus d'informations sur la sécurité de SQL Server, consultez les sites : http://www.microsoft.com/security/guidance/prodtech/SQLServer.mspx

  et

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

- Si vous exécutez un produit de commerce électronique Navision tel que Commerce Gateway, vérifiez que Commerce Gateway Request Server est installé correctement et que les services sont bien exécutés avec le compte configuré par défaut. Le compte configuré par défaut s'appelle *CGRSUser* et permet à Commerce Gateway Server d'accéder à l'ensemble minimum de services requis, notamment au service *MSSQLSERVER* et à *BizTalk Service BizTalk Group : BizTalkServerApplication*. A la différence du compte *Local System*, il ne comprend aucun paramètre de compte global.
- Utilisez toujours des mots de passe difficiles à deviner. Pour plus d'informations sur les mots de passe difficiles à deviner, consultez la section Mots de passe difficiles à deviner.
- Utilisez des logins Windows. Navision vous permet de créer deux types de logins : les logins de base de données et les logins Windows. Nous vous recommandons d'employer les logins Windows car ils utilisent l'authentification Windows, ce qui vous permet d'appliquer une stratégie adéquate en matière de mot de passe.
- Les mots de passe ne doivent pas être réutilisés. La réutilisation des mots de passe dans les différents systèmes et les domaines est une pratique courante. Par exemple, un administrateur chargé de deux domaines peut créer dans chacun d'eux des comptes administrateur de domaine utilisant le même mot de passe, voire créer des mots de passe identiques pour les administrateurs locaux de tous les ordinateurs d'un domaine. Dans ce cas, la défaillance d'un compte ou d'un ordinateur met en danger l'ensemble du domaine.
- Une fois Navision installé et les bases de données créées ou mises à jour, vous devez créer un login Windows et lui affecter le rôle SUPER dans Navision. Cet utilisateur SUPER sera chargé de gérer l'administration de la base de données, la sécurité, etc. Octroyez à ce login un mot de passe difficile à deviner. Préservez la confidentialité de ce mot de passe. Il nécessite le même degré de protection que celui accordé au mot de passe SA dans SQL Server. L'ensemble des accès à la base de données est géré par le rôle SUPER, qui nécessite donc le degré de protection le plus élevé. Le mot de passe de l'utilisateur SUPER ne doit être connu que des administrateurs système.
- Tous les autres utilisateurs ayant accès à la base de données Navision doivent être dotés des privilèges minimaux. Il convient donc de leur assigner dans Navision des rôles qui ne leur permettent d'accéder qu'aux fonctions et aux fonctionnalités dont ils ont besoin pour réaliser leurs tâches au sein de la société.
- Assurez-vous que seuls les utilisateurs dont le rôle au sein de la société le justifie ont la possibilité d'importer des fichiers FOB, de modifier des objets, ainsi que de créer et de restaurer des sauvegardes de base de données.
- Effectuez des sauvegardes régulières de la base de données Navision et pensez à les tester afin de vous assurer qu'elles peuvent être restaurées sans problème.
- Conservez vos sauvegardes dans un endroit sûr afin de les mettre à l'abri des risques provoqués par les incendies, la fumée, la poussière, les températures élevées, la foudre et les catastrophes naturelles (telles que les tremblements de terre).
- Bien que Navision puisse être exécuté sur différentes versions de Windows, nous vous recommandons d'utiliser les systèmes d'exploitation les plus récents avec les fonctions de sécurité les plus à jour. A l'heure actuelle, il convient d'utiliser 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 appliquer à tous les ordinateurs clients les derniers correctifs de sécurité, les derniers services packs et les mises à jour les plus récentes, afin qu'ils soient constamment à jour.
- Nous vous recommandons d'utiliser le protocole de sécurité TCPS pour la communication entre les clients Navision et le serveur de base de données Navision. Le protocole TCPS est une version sécurisée du protocole TCP/IP qui utilise l'interface SSPI (Security Support Provider Interface) et une authentification Kerberos avec cryptage. Le protocole TCPS est le protocole utilisé par défaut par le serveur de base de données Navision.

- Le client doit avoir un plan anti-catastrophe permettant la reprise rapide des services après un sinistre. Un tel plan doit notamment comporter les points suivants :
    - acquisition d'équipement neuf ou temporaire,
    - restauration de sauvegardes dans les nouveaux systèmes,
    - vérification du fonctionnement effectif du plan anti-catastrophe.

Sécurité physique

La sécurité physique est impérative car la sécurité logicielle ne peut pas y suppléer. Par exemple, en cas de vol d'un disque dur, les données figurant sur ce disque finiront aussi par être volées. Lors de la mise au point d'une stratégie de sécurité physique, abordez les points suivants avec le client :

- Dans les grandes installations comportant des services informatiques spécialisés, vérifiez que les salles des serveurs et les lieux de stockage des logiciels sont fermés à clé.
- Les machines concernées sont notamment :
    - le serveur Microsoft SQL Server 2000,
    - le serveur de fichiers où résident les fichiers exécutables Navision.
- Bloquez l'accès des utilisateurs non autorisés aux ordinateurs.
- Quel que soit le degré de confidentialité des données, installez des alarmes antivol.
- Conservez les sauvegardes des données essentielles dans un site externe et stockez les sauvegardes dans des coffres ignifuges.

Les employés

Il est recommandé de limiter les droits d'administration de l'ensemble des produits et des fonctions. Par défaut, les clients ne doivent accorder à leurs employés que des droits de lecture pour les fonctions du système, à moins que l'accomplissement des fonctions de ces employés ne requière des droits d'accès plus étendus. Microsoft recommande l'application du principe du moindre privilège : n'accordez aux utilisateurs que le minimum de droits d'accès aux données et aux fonctionnalités.
Les anciens employés et les mécontents sont une menace pour la sécurité du réseau. Lors des entretiens avec vos clients, proposez-leur d'appliquer la stratégie suivante à l'égard des employés :

- Renseignez-vous sur les antécédents d'un candidat avant l'embauche.
- Anticipez les « vengeances » d'anciens employés ou d'employés mécontents.
- Assurez-vous que vos clients désactivent les comptes Windows et les mots de passe associés au départ d'un employé. En vue du reporting, ne supprimez pas les utilisateurs. Ne réutilisez pas les comptes.
- Sensibilisez les utilisateurs pour qu'ils soient vigilants et signalent toute activité suspecte.
- N'accordez pas de privilèges de façon automatique. Si les utilisateurs n'ont pas besoin d'accéder à des ordinateurs, des salles d'ordinateurs ou des ensembles de fichiers, assurez-vous qu'il n'y ont pas accès.
- Formez les responsables à identifier d'éventuels problèmes avec les employés et à répondre à ces problèmes.
- Assurez-vous que les employés comprennent bien leur rôle en matière de sécurisation du réseau.

- Donnez à chaque employé un exemplaire des stratégies de la société.
- Ne permettez pas aux utilisateurs d'installer des logiciels non autorisés par leurs employeurs.

L'administrateur

Nous recommandons que les administrateurs système de vos clients appliquent les derniers correctifs de sécurité mis à disposition par Microsoft. Les pirates combinent avec une grande habilité de petits bogues qui leur permettent d'opérer d'importantes intrusions dans le réseau. Les administrateurs doivent d'abord vérifier que chaque ordinateur est sécurisé au maximum, puis ajouter des mises à jour de sécurité et utiliser un logiciel antivirus. Ce guide comporte de nombreux liens et ressources pour vous aider à trouver des recommandations et des informations pertinentes.

La complexité présente un autre inconvénient en matière de sécurité du réseau. Plus le réseau est complexe, plus il est difficile à sécuriser ou à rétablir après une intrusion. L'administrateur doit donc soigneusement documenter la topographie du réseau afin qu'elle reste aussi simple que possible.

La sécurité est principalement affaire de gestion des risques. La technologie n'étant pas une panacée, la sécurité nécessite d'allier technologie et stratégie. Autrement dit, un produit qu'il suffirait de déballer et d'installer dans le réseau pour obtenir instantanément une sécurité parfaite est une utopie. La sécurité nécessite technologie et stratégie : la manière d'utiliser la technologie détermine donc le degré de sécurité du réseau. Microsoft fournit des technologies et des fonctions axées sur la technologie, mais seul l'administrateur est à même de déterminer, en fonction de vos directives, les stratégies appropriées pour chaque organisation. Prévoyez les mesures de sécurité dès la phase initiale du processus d'implémentation et de déploiement. Sachez comprendre ce que votre client souhaite protéger et ce qu'il est prêt à faire pour y arriver.

Enfin, prévoyez des plans de secours en cas d'urgence avant qu'une urgence ne se produise. Alliez planification méticuleuse et technologie fiable pour que votre client bénéficie d'une sécurité renforcée.

Pour plus d'informations sur la sécurité en général, consultez « The Ten Immutable Laws of Security Administration » (Les 10 lois incontournables de l'administration de la sécurité) sur le site :
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

Sécurisation du système d'exploitation du serveur

Si, comme vous le constaterez souvent, bon nombre de petits clients ne possèdent pas de système d'exploitation serveur, il importe que vous compreniez les recommandations et que vous sachiez les communiquer aux gros clients dotés d'environnements réseau plus complexes. Notez également qu'une grande partie des stratégies et des recommandations décrites dans ce document s'appliquent aisément aux clients possédant uniquement des systèmes d'exploitation client.

Les concepts exposés dans cette section s'appliquent aux produits Microsoft Windows 2000 Server comme aux produits Microsoft Windows Server 2003, bien que ces informations soient principalement extraites de l'aide en ligne de Windows Server 2003. Windows Server 2003 offre un ensemble de fonctions de sécurité fiable. L'aide en ligne de Windows Server 2003 contient des informations complètes sur toutes les fonctions et les procédures de sécurité de ce produit.

Pour plus d'informations sur Windows 2000 Server, consultez le Centre de sécurité Windows 2000 Server, à l'adresse :
http://www.microsoft.com/technet/security/prodtech/win2000/default.mspx

et reportez-vous au guide sur le renforcement de la sécurité Windows 2000 à l'adresse :
http://www.microsoft.com/technet/security/prodtech/win2000/win2khg/default.mspx

Pour plus d'informations sur Windows Server 2003, consultez le guide de sécurité *Windows Server 2003 Security Guide*, à l'adresse :
http://www.microsoft.com/technet/security/prodtech/win2003/w2003hg/sgch00.mspx

Les principales fonctions du modèle de sécurité pour les serveurs Windows sont l'authentification, le contrôle d'accès et l'authentification unique :

- L'authentification est le processus par lequel le système valide l'identité d'un utilisateur grâce à ses informations de connexion. Le nom et le mot de passe de l'utilisateur sont donc comparés à une liste d'informations autorisées. Si le système constate une correspondance, il autorise l'utilisateur à accéder au contenu défini dans la liste d'autorisations d'accès de cet utilisateur.
- Le contrôle d'accès limite l'accès des utilisateurs aux informations ou aux ressources informatiques en fonction de l'identité de cet utilisateur et de son appartenance à divers groupes prédéfinis. Le contrôle d'accès est généralement utilisé par les administrateurs système pour contrôler l'accès des utilisateurs aux ressources du réseau, telles que les serveurs, les répertoires et les fichiers. Pour le mettre en œuvre, on accorde généralement aux utilisateurs et aux groupes d'utilisateur des droits d'accès à certains objets.
- L'authentification unique permet à l'utilisateur de se connecter une fois au domaine Windows à l'aide d'un mot de passe unique, puis de s'authentifier auprès de n'importe quel ordinateur de ce domaine Windows. L'authentification unique permet aux administrateurs d'instaurer une authentification par mot de passe dans le réseau Windows tout en en simplifiant l'accès pour les utilisateurs finals.

Les sections suivantes contiennent des descriptions plus détaillées de ces trois fonctions-clés.

Authentification

L'authentification est un aspect essentiel de la sécurité du système. Elle permet de valider l'identité de tout utilisateur qui tente de se connecter à un domaine ou d'accéder à des ressources du réseau. Le talon d'Achille de la plupart des systèmes d'authentification est le mot de passe utilisateur.

Les mots de passe sont une protection frontale contre les accès non autorisés au domaine et aux ordinateurs locaux. Présentez à vos clients la liste suivante de recommandations en matière de mot de passe :

- Utilisez toujours des mots de passe difficiles à deviner.
- Si vous devez noter votre mot de passe sur un bout de papier, conservez ce papier en lieu sûr et détruisez-le lorsque vous n'en avez plus besoin.

- Ne confiez jamais votre mot de passe à un tiers.
- Utilisez un mot de passe différent pour chaque compte utilisateur.
- Changez les mots de passe à intervalle régulier.
- Soyez prudent quant à l'endroit où vous stockez votre mot de passe dans l'ordinateur.

Mots de passe difficiles à deviner

Le rôle des mots de passe dans la sécurisation du réseau d'une organisation est souvent sous-estimé ou négligé. Comme indiqué ci-dessus, les mots de passe protègent de façon frontale contre les accès non autorisés au réseau. Vérifiez donc que vos clients exigent de leurs employés qu'ils utilisent des mots de passe difficiles à deviner.

Toutefois, les outils permettant de « casser » les mots de passe s'améliorent constamment et les ordinateurs utilisés à cet effet sont de plus en plus puissants. Un outil automatique spécialisé permet de casser n'importe quel mot de passe ; ce n'est qu'une question de temps. Les mots de passe difficiles à deviner sont néanmoins bien plus compliqués à casser que les mots de passe faciles à décrypter.

Pour obtenir des instructions sur la création de mots de passe difficiles à deviner que l'utilisateur peut mémoriser, consultez les sites :

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

et

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

Définition de la stratégie en matière de mot de passe

Lorsque vous aidez votre client à définir une stratégie régissant les mots de passe, veillez à créer une stratégie instaurant l'attribution, à tous les comptes utilisateur, de mots de passe difficiles à deviner. Les recommandations du guide de sécurité Windows Server 2003 Security Guide suffisent pour la plupart des systèmes :

- Définissez le paramètre de stratégie **Conserver l'historique des mots de passe** afin que le système mémorise plusieurs mots de passe antérieurs. Ce paramètre de stratégie empêche les utilisateurs de réutiliser le même mot de passe après son expiration.

  Paramétrage recommandé : 24.

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

  Paramétrage recommandé : de 42 (valeur par défaut) à 90.

- Définissez le paramètre de stratégie **Durée de vie minimale du mot de passe** de manière à ne pouvoir changer les mots de passe que lorsqu'ils ont plus qu'un certain nombre de jours. Ce paramètre de stratégie fonctionne en combinaison avec le paramètre **Conserver l'historique des mots de passe**. Lorsqu'un âge minimum est défini pour les mots de passe, les utilisateurs ne peuvent pas modifier leurs mots de passe de manière répétée afin de contourner le paramètre **Conserver l'historique des mots de passe**, puis réutiliser leurs mots de passe initiaux. Les utilisateurs doivent attendre le nombre de jours spécifié pour pouvoir modifier leur mot de passe.

  Paramétrage recommandé : 2.

- Définissez un paramètre de stratégie **Longueur minimale du mot de passe** de manière à ce que les mots de passe comportent au moins le nombre de caractères spécifié. Les mots de passe longs, comportant sept caractères ou plus, sont généralement plus difficiles à deviner que les mots de passe courts. Avec ce paramètre, les utilisateurs ne peuvent pas utiliser des mots de passe vides et doivent créer des mots de passe comportant au moins le nombre de caractères donné.

  Paramétrage recommandé : 8.

- Activez le paramètre de stratégie **Le mot de passe doit respecter des exigences de complexité**. Ce paramètre active le contrôle de tous les nouveaux mots de passe pour vérifier leur conformité aux exigences de base concernant les mots de passe difficiles à deviner. Ce paramètre garantit que les mots de passe comportent au moins trois symboles appartenant aux quatre catégories définies (majuscule, minuscule, chiffre, symbole non alphanumérique) et qu'ils ne contiennent aucune partie du nom d'utilisateur, ni du prénom ni du nom de famille de l'utilisateur.

  Remarque
  Les mots de passe conformes à ces exigences ne sont pas forcément très difficiles à deviner. Par exemple, le mot de passe « Motdepasse1 » répond à ces exigences.

  Paramétrage recommandé : Oui.

- Pour obtenir la liste complète de ces exigences, consultez la rubrique « Password Must Meet Complexity Requirements » (Le mot de passe doit respecter des exigences de complexité) de l'aide en ligne de Windows Server.
- Stockez les mots de passe en utilisant le cryptage réversible. Le cryptage réversible est utilisé dans les systèmes dont les applications nécessitent l'accès à des mots de passe non cryptés. Ce type de cryptage n'est pas nécessaire dans la plupart des installations.

  Paramétrage recommandé : Non.

Pour plus d'informations, reportez-vous au guide de sécurité Windows Server 2003 Security Guide :

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

Définition d'une stratégie de verrouillage des comptes

Soyez prudent lorsque vous définissez une stratégie de verrouillage des comptes. La stratégie de verrouillage des comptes ne doit jamais être activée dans une petite entreprise car elle risque de bloquer l'accès aux utilisateurs autorisés, ce qui peut coûter très cher à votre client.

Si le client décide d'appliquer une stratégie de verrouillage des comptes, choisissez une valeur suffisamment élevée pour le paramètre **Stratégie de verrouillage du compte** pour que l'accès des utilisateurs autorisés à leur compte ne soit pas bloqué simplement parce qu'ils se sont trompés plusieurs fois en entrant leur mot de passe.

Pour plus d'informations sur la stratégie de verrouillage des comptes, reportez-vous à la rubrique « Account Lockout Policy Overview » (Vue d'ensemble de la stratégie de verrouillage des comptes) de l'aide en ligne de Windows Server.

Pour plus d'informations sur la manière d'appliquer ou de modifier une stratégie de verrouillage des comptes, reportez-vous à la rubrique « To Apply or Modify Account Lockout Policy » (Application ou modification d'une stratégie de verrouillage des comptes) de l'aide en ligne de Windows Server.

Contrôle d'accès

Vous pouvez sécuriser un réseau Windows et ses ressources (y compris Navision) en gérant les droits des utilisateurs, des groupes d'utilisateurs et des autres ordinateurs dans le réseau. Vous pouvez sécuriser un ordinateur ou plusieurs ordinateurs en accordant aux utilisateurs ou aux groupes des droits d'utilisateur spécifiques. Vous pouvez sécuriser un objet, tel qu'un fichier ou un dossier, en lui assignant des droits autorisant les utilisateurs ou les groupes à effectuer certaines actions en rapport avec cet objet. Le contrôle d'accès comporte les notions-clés suivantes :

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

Autorisations

Les autorisations définissent le type de droits d'accès accordés à un utilisateur ou à un groupe concernant une propriété d'objet ou un objet tel que des fichiers, des dossiers et des objets de la base de registre. Les autorisations sont appliquées à tout objet sécurisé tel que des fichiers ou des objets de la base de registre. Les autorisations peuvent être accordées à tout utilisateur, groupe ou ordinateur. Il est judicieux d'affecter des autorisations aux groupes.

Propriété d'objets

Un propriétaire est affecté à un objet lors de la création de celui-ci. Dans Windows 2000 Server, le propriétaire d'un objet est par défaut son créateur. Cette fonction est modifiée dans Windows Server 2003 pour les objets créés par les membres du groupe Administrateurs.

Lorsqu'un membre du groupe Administrateurs crée un objet dans Windows Server 2003, le groupe Administrateurs en devient propriétaire plutôt que le compte qui a créé cet objet. Ce comportement peut être modifié à l'aide des paramètres de sécurité locaux du composant logiciel enfichable Microsoft Management Console (MMC) en paramétrant l'option **Objets système : propriétaire par défaut pour les objets créés par les membres du groupe Administrateurs**. Quelles que soient les autorisations définies pour un objet, son propriétaire peut toujours les modifier.

Pour plus d'informations, reportez-vous à la rubrique « Ownership » (Propriété) de l'aide en ligne de Windows Server.

Héritage d'autorisations

L'héritage permet aux administrateurs d'affecter et de gérer aisément les autorisations. Cette fonction attribue automatiquement à tous les objets d'un conteneur l'ensemble des autorisations de ce conteneur qui peuvent être héritées. Par exemple, lorsque vous créez des fichiers dans un dossier, ils héritent des autorisations de ce dossier. Seules les autorisations marquées pour héritage sont héritées.

Droits d'utilisateur

Les droits d'utilisateur accordent des privilèges et des droits d'accès spécifiques à des utilisateurs et à des groupes de l'environnement informatique.

Pour plus d'informations sur les droits d'utilisateur, reportez-vous à la rubrique « User Rights » (Droits utilisateur) de l'aide en ligne de Windows Server.

Audit d'objet

Vous pouvez auditer l'accès des utilisateurs à des objets. Vous pouvez ensuite visualiser ces événements liés à la sécurité dans le journal sécurité à l'aide de l'Observateur d'événements.

Pour plus d'informations, reportez-vous à la rubrique « Auditing » (Audit) de l'aide en ligne de Windows Server.

Recommandations en matière de contrôle d'accès

- Affectez des autorisations aux groupes plutôt qu'aux utilisateurs. La gestion directe des comptes utilisateur étant une pratique inefficace, l'attribution d'autorisations à des utilisateurs individuels doit être exceptionnelle.
- Utilisez des autorisations de type Refuser dans certains cas. Par exemple, vous pouvez utiliser les autorisations de type Refuser pour exclure un sous-ensemble d'un groupe possédant des autorisations de type Autoriser.
- Ne refusez jamais l'accès à un objet au groupe Tous les utilisateurs. Si vous refusez à tous les utilisateurs l'accès à un objet, vous le refusez également aux administrateurs. Il vaut mieux supprimer le groupe Tous les utilisateurs, du moment que vous autorisez l'accès à cet objet à d'autres utilisateurs, d'autres groupes ou d'autres ordinateurs. Souvenez-vous que si aucune autorisation n'est définie, aucun accès n'est autorisé.
- Attribuez des autorisations à l'objet placé le plus haut possible dans l'arborescence, puis appliquez un paramètre d'héritage afin de propager les paramètres de sécurité dans l'arborescence. Vous pouvez appliquer rapidement et efficacement des paramètres de contrôle d'accès à tous les enfants ou à la sous-arborescence d'un objet parent. Ainsi, vous obtenez le maximum d'effets avec le minimum d'efforts. Les paramètres d'autorisation que vous définissez doivent convenir à la majorité des utilisateurs, des groupes et des ordinateurs.
- Les autorisations explicites peuvent parfois remplacer les autorisations héritées. Les autorisations de type Refuser héritées n'empêchent pas l'accès à un objet si cet objet possède un paramètre d'autorisation Autoriser explicite. Les autorisations explicites sont prioritaires par rapport aux autorisations héritées, même par rapport aux autorisations Refuser.
- Pour les autorisations concernant les objets Active Directory®, assurez-vous de bien comprendre les recommandations propres aux objets Active Directory.

Pour plus d'informations, reportez-vous à la rubrique « Best Practices for Assigning Permissions on Active Directory Objects » (Recommandations en matière d'attribution d'autorisation sur des objets Active Directory) de l'aide en ligne de Windows Server 2003.

Pare-feu de sécurité externe

Un pare-feu est un logiciel ou un élément matériel empêchant les paquets de données d'entrer ou de quitter un réseau donné. Pour contrôler le flux des données, les ports du pare-feu envoyant ou recevant les paquets d'informations sont ouverts ou fermés. Le pare-feu analyse plusieurs informations de chaque paquet de données : le protocole utilisé pour la transmission du paquet, la destination ou l'expéditeur du paquet, le type de contenu du paquet et le numéro de port auquel il est envoyé. Si le pare-feu est configuré pour accepter le protocole défini et le port ciblé, la transmission du paquet est autorisée. Microsoft Windows Small Business Server 2003 Premium Edition inclut la solution de pare-feu Microsoft Internet Security and Acceleration (ISA) Server 2000. Le logiciel Small Business Server Standard Edition comprend aussi un pare-feu.

ISA Server 2004

Internet Security and Acceleration (ISA) Server 2000 achemine en toute sécurité les demandes et réponses échangées entre Internet et les ordinateurs client sur le réseau interne.

ISA Server sert de passerelle d'accès sécurisé à Internet aux clients du réseau local. L'ordinateur ISA Server est transparent pour les autres parties intervenant sur le canal de transmission. Les utilisateurs Internet ne doivent pas être à même de détecter la présence d'un serveur pare-feu, excepté s'ils tentent d'accéder à un service ou à un site dont l'ordinateur ISA Server refuse l'accès. Le serveur Internet qui fait l'objet d'une tentative d'accès interprète les demandes émanant de l'ordinateur ISA Server comme si elles provenaient de l'application client.

Lorsque vous optez pour le filtrage des fragments IP (Internet Protocol), vous activez les services de proxy Web et de pare-feu pour filtrer les fragments de paquets. Avec un tel filtrage, tous les paquets IP fragmentés sont perdus. Une attaque connue implique l'envoi de paquets fragmentés, puis leur réassemblage d'une manière telle que le système risque d'être endommagé.

ISA Server est doté d'un mécanisme de détection d'intrusion qui identifie toute tentative d'attaque sur le réseau et effectue un ensemble d'actions (ou d'alertes) prédéfinies en cas d'attaque avérée.

Si les services IIS (Internet Information Services) sont installés sur l'ordinateur ISA Server, vous devez les configurer pour qu'ils ne se servent pas des ports utilisés par ISA Server pour les demandes Internet sortantes (par défaut, 8080) et entrantes (par défaut, 80). Par exemple, vous pouvez paramétrer les services IIS pour qu'ils gèrent le port 81, puis configurer l'ordinateur ISA Server pour acheminer les demandes Internet entrantes vers le port 81 de l'ordinateur local exécutant les services IIS.

En cas de conflit entre les ports utilisés par l'ordinateur ISA Server et les services IIS, le programme de configuration arrête le service de publication IIS.

Vous pouvez ensuite paramétrer les services IIS pour qu'ils gèrent un autre port et redémarrer le service de publication IIS.

Stratégies ISA Server

Vous pouvez définir une stratégie ISA Server régissant les accès entrants et sortants. Les règles de site et de contenu spécifient les sites et contenus accessibles. Les règles de protocole déterminent les protocoles qui sont accessibles pour les communications entrantes et sortantes.

Vous pouvez créer des règles de site et de contenu, des règles de protocole et de publication Web, ainsi que des filtres de paquets IP. Ces règles déterminent le mode de communication des clients ISA Server avec Internet et les types de communication autorisés.

Protection antivirus

Un virus informatique est un fichier exécutable qui est conçu pour s'auto-propager, pour effacer ou endommager des fichiers de données et des programmes, et éviter tout dispositif de détection. Dans la réalité, les virus sont souvent réécrits et adaptés pour ne pas être détectés. Les virus sont souvent transmis sous forme de pièce jointe. Les programmes antivirus doivent être mis à jour régulièrement pour pouvoir détecter les nouveaux virus et les virus modifiés. Les virus sont la première cause d'agressions informatiques.

Les programmes antivirus sont spécialement conçus pour détecter et bloquer les virus. Comme de nouveaux virus sont créés en permanence, de nombreux fabricants de produits antivirus proposent régulièrement à leurs clients des mises à jour de leurs logiciels. Microsoft vous recommande fortement d'installer un logiciel antivirus sur votre environnement client.

Les virus sont généralement installés dans l'un des trois emplacements suivants : postes de travail utilisateur, serveurs et réseau (point d'entrée et parfois point de sortie des messages électroniques de la société).

Types de virus

Il existe trois grands types de virus infectant les systèmes informatiques : les virus d'amorçage, les virus programme et les chevaux de Troie.

Virus d'amorçage

Quand un ordinateur démarre, le secteur d'amorçage du disque dur est analysé avant le chargement du système d'exploitation ou de tout autre fichier de démarrage. Un virus d'amorçage est conçu pour remplacer les informations des secteurs d'amorçage du disque dur par son propre code. Quand un ordinateur est infecté par un virus d'amorçage, le code de ce virus est lu en mémoire avant toute chose. Une fois le virus en mémoire, il peut se propager sur les disques de l'ordinateur infecté.

Virus programme

Les virus programme (virus les plus courants) se fixent à un fichier exécutable en y ajoutant leur propre code. Le code du virus est généralement ajouté de

telle manière qu'il échappe à toute détection. Lors de l'exécution du fichier infecté, le virus peut se fixer à d'autres fichiers exécutables. Les fichiers infectés par ce type de virus portent généralement l'extension .com, .exe ou .sys.

Certains virus programme s'attaquent à des programmes bien précis. Les types de programmes souvent attaqués sont les fichiers de superpositions (.ovl) et les fichiers de bibliothèques de liens dynamiques (.dll). Ces fichiers ne sont pas exécutés à proprement parler, mais des fichiers exécutables les appellent. Le virus est alors transmis lors de l'appel.

Les données sont endommagées lors du déclenchement du virus. Un virus peut être déclenché lors de l'exécution d'un fichier infecté ou quand un paramètre d'environnement précis se produit (comme une date système particulière).

Chevaux de Troie

Un cheval de Troie n'est pas réellement un virus. Contrairement à un virus, un cheval de Troie ne s'auto-propage pas. Il « se contente » de détruire les informations du disque dur. Un cheval de Troie se déguise sous la forme d'un programme autorisé, comme un jeu ou un utilitaire. Cependant, au moment de son exécution, il peut détruire ou endommager des données.

Recommandations en matière de protection antivirus

Il est possible de bloquer la propagation d'un virus de macro. Vous trouverez ci-dessous quelques astuces permettant d'éviter une infection. Pour plus de sécurité, communiquez-les à vos clients :

- Installez une solution antivirus qui recherche les virus dans les messages provenant d'Internet avant que ces derniers ne franchissent le routeur. De cette manière, les virus connus sont recherchés dans tous les messages électroniques.
- Identifiez la source des documents reçus. N'ouvrez aucun document si leur expéditeur n'est pas digne de confiance.
- Parlez à l'auteur du document. Si les utilisateurs doutent de la fiabilité du document, ils peuvent contacter son auteur.
- Utilisez la protection Microsoft Office contre les virus de macro. Dans Office, les applications avertissent l'utilisateur si un document contient des macros. Cette fonction permet à l'utilisateur d'activer ou de désactiver les macros à l'ouverture du document.
- Utilisez un logiciel antivirus pour détecter et supprimer les virus de macro. Ces logiciels peuvent détecter et souvent supprimer les virus de macro dans les documents. Microsoft recommande d'utiliser un logiciel antivirus certifié par l'ISCA (International Computer Security Association).

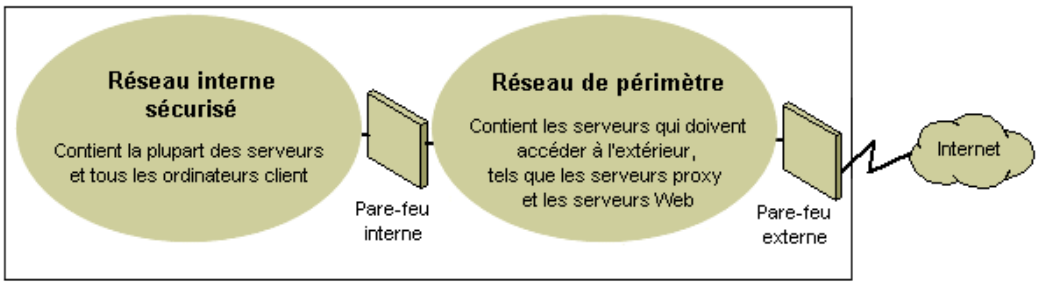
Pour plus d'informations sur les virus et la sécurité informatique en général, visitez les sites Web Microsoft Security suivants :

- Microsoft Security : http://www.microsoft.com/security/default.asp
- Documentation relative à la sécurité sur Microsoft TechNet : http://www.microsoft.com/technet/security/Default.mspx

Stratégies de sécurité réseau

Etant donné que la conception et le déploiement d'un environnement IP d'interconnexion réseau implique d'équilibrer les problèmes liés aux réseaux publics et privés, le pare-feu devient un élément essentiel au maintien de l'intégrité du réseau. Un pare-feu n'est pas un composant unique. L'ICSA (anciennement NCSA, National Computer Security Association) définit un pare-feu comme « un système ou une combinaison de systèmes instaurant une frontière entre plusieurs réseaux ». Bien que plusieurs termes soient utilisés pour définir cette frontière, celle-ci est souvent appelée « réseau de périmètre ». Le réseau de périmètre protège votre intranet ou le réseau local de votre société (LAN) contre toute intrusion en contrôlant les accès provenant d'Internet ou d'autres réseaux importants.

Le schéma suivant représente un réseau de périmètre entouré de pare-feu et placé entre un réseau privé et Internet afin de sécuriser le réseau privé :



Réseau de périmètre standard

Concernant l'utilisation des pare-feu, les sociétés n'ont pas toutes la même approche pour assurer la sécurité de leur réseau. Le filtrage des paquets IP offre une protection faible, est complexe à gérer et s'avère souvent inutile. Les passerelles d'application sont plus sûres que les filtres de paquets et sont plus simples à gérer car elles appartiennent uniquement à quelques applications, par exemple à un logiciel de messagerie électronique. Les passerelles de circuit sont plus efficaces lorsqu'il est plus important de surveiller l'utilisateur d'une application réseau que les données transférées par cette application. Le serveur proxy est un outil de sécurité complet qui comprend une passerelle d'application, un accès sécurisé pour les utilisateurs anonymes et d'autres services. Vous trouverez ci-dessous des informations sur ces différentes possibilités :

- **Filtrage de paquets IP**
  Il s'agit de la première technologie de pare-feu mise en place. De nombreuses informations sont analysées dans les en-têtes des paquets : adresse de l'expéditeur et du destinataire, numéros de port TCP (Transmission Control Protocol) et UDP (User Datagram Protocol). Le filtrage des paquets est une technologie limitée dont le fonctionnement est optimal dans des environnements de sécurité clairs, où, par exemple, tout ce qui se trouve à l'extérieur du réseau de périmètre est considéré comme non fiable, contrairement à tout ce qui se trouve au sein du réseau de périmètre, considéré alors comme fiable. Ces dernières années, plusieurs éditeurs ont amélioré la méthode de filtrage de paquets en ajoutant des fonctions décisionnelles au noyau de filtrage, créant ainsi une nouvelle forme de filtrage de paquets appelée *inspection*

dynamique de protocole. Vous pouvez configurer le filtrage de paquets pour accepter certains types de paquets uniquement et refuser tous les autres, ou inversement.

- **Passerelles d'application**
  Ces passerelles sont utiles lorsque le contenu réel d'une application est très important. Le fait qu'elles soient propres à une application constitue tant un avantage qu'un inconvénient car il est difficile de les adapter aux évolutions technologiques.
- **Passerelles de circuit**
  Ces passerelles sont des tunnels traversant un pare-feu et qui permettent de connecter des processus ou des systèmes spécifiques de part et d'autre de ce tunnel. Les passerelles de circuit sont idéales lorsque la personne utilisant une application peut faire courir un risque plus grand que les informations transmises par l'application elle-même. Les passerelles de circuit diffèrent du filtrage de paquets par leur capacité à se connecter à un modèle d'application « hors plage » qui peut apporter des informations complémentaires.
- **Serveurs proxy**
  Les serveurs proxy sont des outils de sécurité complets, avec fonction de pare-feu et de passerelle d'application, qui gèrent le trafic Internet en provenance et à destination du réseau LAN. Les serveurs proxy proposent également des fonctions de mise en mémoire cache des documents et de contrôle d'accès. Un serveur proxy peut améliorer les performances en mettant en cache et en fournissant directement les données fréquemment demandées. C'est le cas par exemple des pages Web consultées fréquemment. Un serveur proxy peut également filtrer et ignorer les demandes que le propriétaire considère comme non pertinentes, telles que des demandes d'accès non autorisé aux fichiers propriétaires.

Veillez à ce que le client exploite ces fonctions très utiles de sécurité par pare-feu. Placez un réseau de périmètre dans votre topologie réseau à l'endroit où le trafic en provenance de l'extérieur du réseau de l'entreprise doit franchir le périmètre contrôlé par le pare-feu externe. Vous pouvez ajuster le contrôle d'accès pour que le pare-feu réponde aux besoins du client. Vous pouvez également configurer les pare-feu pour qu'ils enregistrent toutes les tentatives d'accès non autorisé.

Pour limiter le nombre de ports nécessairement ouverts sur le pare-feu interne, vous pouvez utiliser un pare-feu de niveau application, comme ISA Server 2000.

Pour plus d'informations sur TCP/IP, reportez-vous à la section Designing a TCP/IP Network (Conception d'un réseau TCP/IP) sur le site :

http://www.microsoft.com/resources/documentation/WindowsServ/2003/all/deployguide/en-us/dnsbb_tcp_overview.asp

Réseaux sans fil

Par défaut, la configuration des réseaux sans fil est telle qu'il est possible d'écouter les signaux émis. Ces réseaux peuvent faire l'objet d'accès externes malveillants du fait du paramétrage par défaut de certains matériels sans fil, de l'accessibilité des réseaux sans fil et des méthodes de cryptage actuelles. Des outils et des options de configuration permettent de protéger les réseaux contre l'écoute malveillante des signaux mais aucune fonction ne protège les ordinateurs contre les pirates et virus entrant via la connexion Internet. Par conséquent, il est extrêmement important d'ajouter un pare-feu pour protéger les ordinateurs contre toute intrusion en provenance d'Internet.

Pour plus d'informations sur la protection d'un réseau sans fil, reportez-vous à la section How to Make Your 802.11b Wireless Home Network More Secure

(Comment améliorer la sécurité de votre réseau domestique sans fil 802.11b) sur le site : http://support.microsoft.com/default.aspx?scid=kb;en-us;309369

Scénarios de sécurité réseau

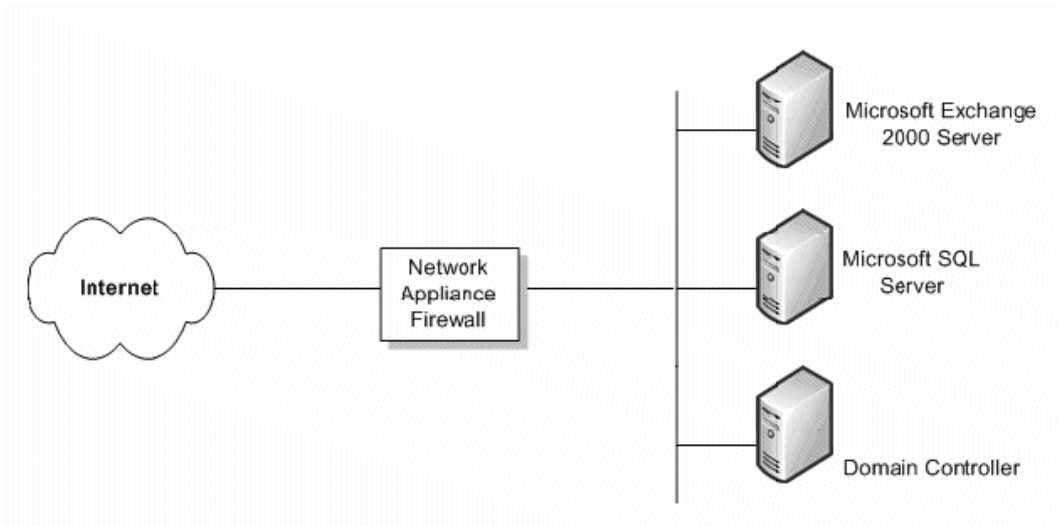
Le niveau de sécurité réseau demandé par la société client dépend de plusieurs facteurs. La définition de ce niveau résulte généralement d'un compromis entre le budget disponible et la nécessité pour l'entreprise de protéger ses données. Il est possible pour une petite société de disposer d'une structure de sécurité très complexe assurant le meilleur niveau de sécurité réseau possible, mais il est rare qu'elle dispose des budgets nécessaires à la mise en place d'un tel niveau de sécurité. Dans cette section, nous allons examiner quatre scénarios assurant différents niveaux de sécurité et fournir des recommandations pour chacun.

Absence de pare-feu

Si votre client dispose d'une connexion Internet non protégée par un pare-feu, il est nécessaire de prendre certaines mesures en ce qui concerne la sécurité réseau. Il existe des pare-feu réseau simples qui assurent un niveau de sécurité suffisant pour bloquer la plupart des pirates.

Un simple pare-feu

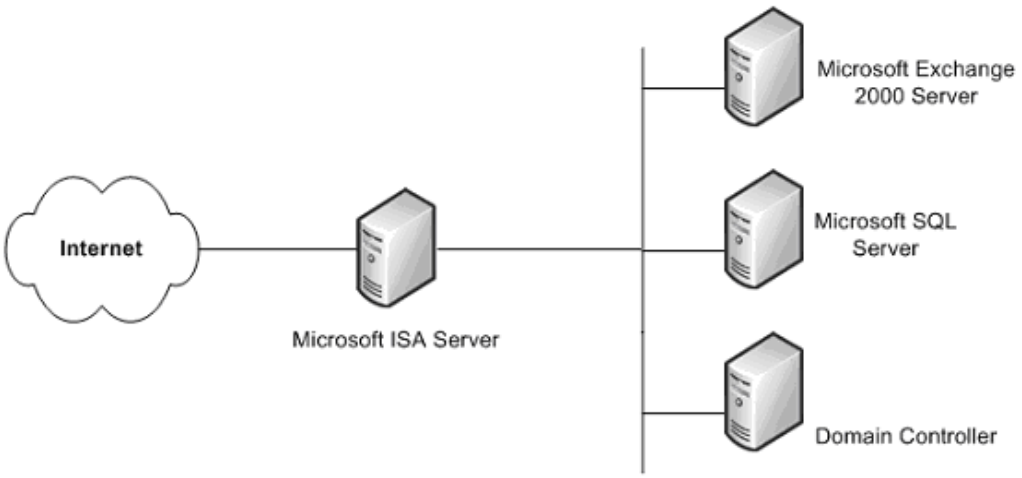
Il est recommandé de vous doter du niveau de sécurité minimum en installant un simple pare-feu entre Internet et les données de votre client. Ce pare-feu n'assure pas tous les niveaux de sécurité avancée et ne doit donc pas être considéré comme un outil de sécurité totale. Mais c'est toujours mieux que rien !



Pare-feu simple

Il reste à espérer que le budget du client permettra d'installer une solution plus sûre pour garantir la protection des données de l'entreprise. ISA Server est une de ces solutions. Malgré les coûts supplémentaires qui en découlent, cet autre serveur assure un niveau de sécurité de bien meilleure qualité qu'un

pare-feu informatique classique, qui n'assure généralement que la traduction d'adresses réseau (NAT) et le filtrage de paquets.



Pare-feu ISA Server

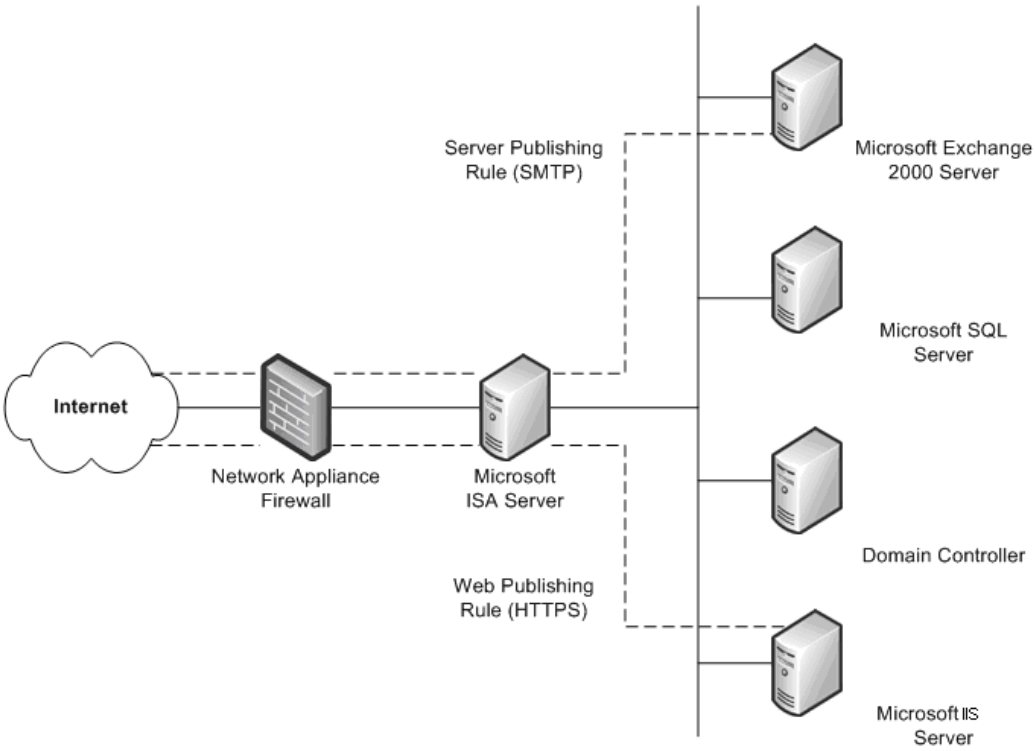
Cette solution de pare-feu unique est plus sûre qu'un dispositif de pare-feu placé au niveau des entrées, et offre des services de sécurité Windows.

Un pare-feu existant

Si le client dispose d'un pare-feu séparant les connexions intranet et Internet, il est possible d'ajouter un autre pare-feu offrant plusieurs méthodes de configuration des ressources internes sur Internet.

Cette méthode s'appelle la publication Web. Elle consiste à déployer un serveur ISA Server devant un serveur Web assurant l'accès aux utilisateurs Internet. En cas de demandes Web entrantes, ISA Server peut simuler un serveur Web, répondant, via son cache, aux demandes de contenu Web émanant des clients. ISA Server transmet les demandes au serveur Web uniquement lorsque les demandes ne peuvent pas être honorées à partir de son cache.

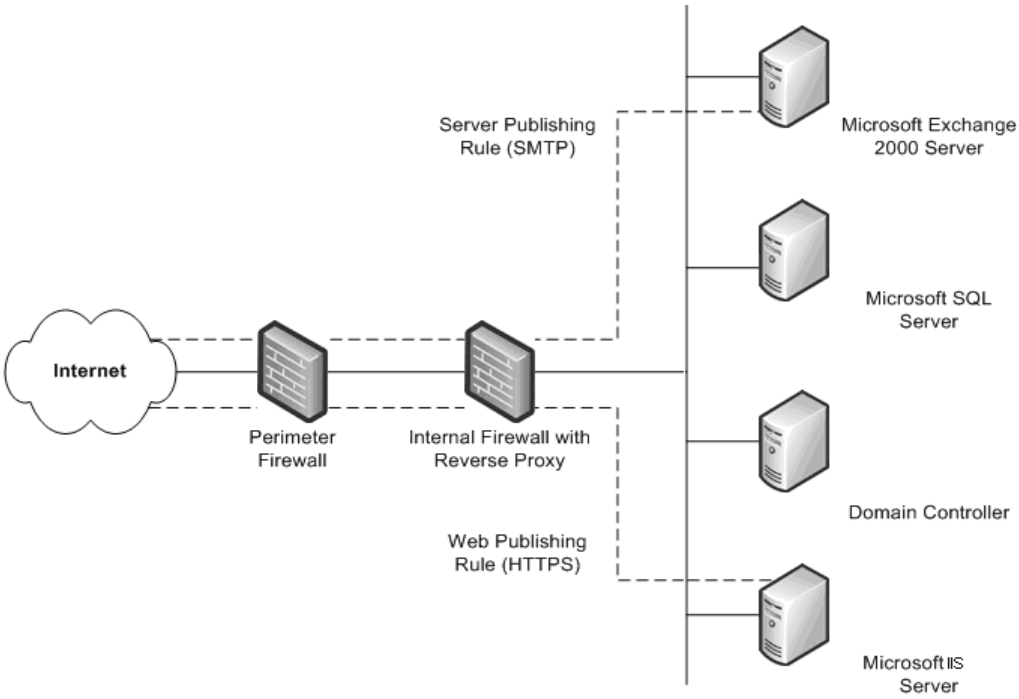
Une autre méthode est la publication sur serveur. ISA Server autorise la publication sur serveurs internes sur Internet sans altérer la sécurité du réseau interne. Vous pouvez configurer des règles de publication Web et des règles de publication sur serveur qui déterminent les demandes à envoyer vers un serveur du réseau local. Vous augmentez ainsi le niveau de sécurité des serveurs internes.



Pare-feu existant avec ISA Server

Deux pare-feu existants

Dans le quatrième scénario, la société dispose de deux pare-feu et d'une zone démilitarisée de réseau de périmètre. L'un de ces serveurs ou les deux proposent des services de proxy inverse pour que les clients Internet n'accèdent pas aux serveurs directement via l'intranet. L'un des pare-feu, généralement le pare-feu interne, intercepte les demandes réseau destinées aux serveurs internes, analyse ces paquets, puis les retransmet pour le compte de l'hôte Internet.



Deux pare-feu existants

Ce scénario est semblable au précédent après installation du second pare-feu. La seule différence provient du fait que le pare-feu interne prenant en charge le proxy inverse n'est pas un serveur ISA Server. Dans ce scénario, travaillez en étroite collaboration avec le responsable de chaque pare-feu pour définir des règles de publication sur serveur parfaitement adaptées à la stratégie de sécurité.

Gestion des correctifs de sécurité

Les systèmes d'exploitation et les applications sont souvent très complexes. Ils peuvent se composer de millions de lignes de code, écrites par plusieurs développeurs. Il est essentiel que les logiciels soient fiables et qu'ils ne compromettent en rien la sécurité ou la stabilité de l'environnement informatique. Pour limiter ces risques, les programmes font l'objet de tests rigoureux avant leur commercialisation. Malgré tout, les pirates cherchent sans relâche à identifier les faiblesses des logiciels. Il est donc impossible de prévoir toutes les attaques à venir.

Pour la plupart des sociétés, la gestion des correctifs fait partie de leur stratégie globale de gestion des configurations et des modifications. Il est essentiel pour toute société, quelles que soient sa nature et sa taille, de disposer d'une solide stratégie de gestion des correctifs, même si la société n'applique pas encore de stratégie de gestion des modifications et des configurations. La plus grande majorité des attaques réussies contre des systèmes informatiques ont visé les systèmes sans aucun correctif de sécurité installé.

Les correctifs de sécurité constituent un sérieux défi pour la plupart des sociétés. Dès qu'une faiblesse logicielle a été détectée, les pirates diffusent généralement rapidement cette information auprès de leur communauté. Dès qu'une faille est identifiée, Microsoft s'attache à diffuser le plus rapidement

possible le correctif de sécurité correspondant. Tant que le correctif n'est pas installé, le niveau de sécurité attendu par le client est sérieusement altéré.

Dans l'environnement Navision, vous devez vous assurer que les clients ont installé les tout derniers correctifs de sécurité dans leur système. Vérifiez également que le client utilise l'une des technologies Microsoft. Il s'agit notamment de :

- **Microsoft Security Notification Service**
  Ce service de notification de sécurité, qui repose sur une liste d'adresses e-mail, avertit les utilisateurs dès qu'une mise à jour est disponible. Ces notifications constituent un élément majeur d'une stratégie de sécurité proactive. Elles sont également disponibles sur le site Web de notification de sécurité TechNet Product Security Notification : http://www.microsoft.com/technet/security/bulletin/notify.mspx
- **Microsoft Automatic Updates**
  Windows peut automatiquement installer des mises à jour de sécurité sur votre ordinateur.
- **Outil de recherche Microsoft Security Bulletin**
  L'outil de recherche Security Bulletin est disponible sur le site Web Security Bulletin Service : http://www.microsoft.com/technet/security/current.aspx. Le client peut déterminer les mises à jour à installer en fonction du système d'exploitation, des applications et des Service Packs exécutés.
- **Analyseur de sécurité Microsoft Baseline Security Analyzer (MBSA)**
  Cet outil graphique est disponible sur le site Web Microsoft Baseline Security Analyzer : http://www.microsoft.com/technet/security/tools/mbsahome.mspx. Cet outil compare l'état actuel d'un ordinateur avec la liste des mises à jour proposées par Microsoft. MBSA effectue également quelques vérifications de sécurité de base pour tester la protection par mot de passe et les paramètres d'expiration, les stratégies concernant les comptes invités et un certain nombre d'autres points. MBSA recherche aussi les vulnérabilités des services Microsoft Internet Information Services (IIS), de SQL Server™ 2000, d'Exchange 5.5, d'Exchange 2000 et d'Exchange Server 2003.
- **Microsoft Software Update Services (SUS)**
  Auparavant appelé Windows Update Corporate Edition, cet outil permet aux sociétés d'héberger sur des ordinateurs locaux toutes les mises à jour et packages de déploiement de sécurité (SRP) disponibles sur le site public de Windows Update. Cet outil utilise une nouvelle version des clients de mise à jour automatique (AU) pour constituer la base d'une puissante stratégie de téléchargement et d'installation automatiques. Le nouvel ensemble de clients AU comprend un client pour Windows 2000 et Windows Server 2003, et peut installer automatiquement les mises à jour téléchargées. Pour plus d'informations sur Microsoft SUS, reportez-vous au site : http://www.microsoft.com/windows2000/windowsupdate/sus/default.asp
- **Feature Pack des services de mises à jour logicielles Microsoft Systems Management Server (SMS)**
  Ce Feature pack contient un certain nombre d'outils conçus pour faciliter la diffusion des mises à jour logicielles au sein d'une entreprise. Ces outils comprennent un outil d'inventaire des mises à jour de sécurité (Security Update Inventory Tool), un outil d'inventaire des mises à jour Microsoft (Microsoft Office Inventory Tool for Updates), l'Assistant de diffusion des mises à jour logicielles (Distribute Software Updates Wizard) et un outil de reporting Web (SMS Web Reporting Tool), ainsi que des modules externes de reporting Web pour les mises à jour logicielles. Pour plus d'informations sur chacun de ces outils, reportez-vous au site : http://www.microsoft.com/smserver/downloads/20/featurepacks/suspack/

Parlez de ces outils à vos clients et encouragez-les à les utiliser. Il est très important que les problèmes de sécurité soient résolus le plus rapidement possible tout en maintenant la stabilité de l'environnement.

Paramètres de sécurité de SQL Server 2000

Comme Navision fonctionne également sous SQL Server 2000, il est important que vous renforciez la sécurité de l'installation SQL Server 2000 du client. Pour ce faire, procédez comme suit :

- Vérifiez que les mises à jour et les Service Packs les plus récents du système d'exploitation et de SQL Server 2000 sont installés. Pour connaître les toutes dernières informations, consultez le site Microsoft Security : http://www.microsoft.com/security/default.asp
- Pour la sécurité au niveau du système de fichiers, vérifiez que toutes les données et que tous les fichiers système SQL Server 2000 sont installés sur des partitions NTFS. Limitez l'accès des fichiers aux utilisateurs ayant des droits Administrateur ou Système par le biais d'autorisations NTFS. Vous empêcherez ainsi les utilisateurs d'accéder à ces fichiers lorsque le service MSSQLSERVER n'est pas exécuté.
- Utilisez un compte de domaine avec peu de privilèges comme NT Authority\Network Service ou le compte LocalSystem (recommandé) pour SQL Server 2000 service (MSSQLSERVER). Ce compte doit disposer de droits d'accès limités au domaine et doit aider à contenir (et non arrêter totalement) une attaque visant le serveur en cas de compromis. Autrement dit, ce compte ne doit disposer que d'autorisations utilisateur local dans le domaine. Si SQL Server 2000 utilise un compte Administrateur de domaine pour exécuter les services, un compromis du serveur aboutira à un compromis de l'ensemble du domaine. Pour modifier ce paramétrage, utilisez SQL Server Enterprise Manager. Les listes de contrôle d'accès (ACL) appliquées aux fichiers, le registre et les droits utilisateur seront modifiés automatiquement.
- La plupart des versions de SQL Server 2000 sont installées avec deux bases de données par défaut : **Northwind** et **pubs**. Il s'agit de deux bases de données exemples qui servent aux tests, à la formation et d'exemples généraux. Ne les déployez pas dans un système de production. Un pirate ayant connaissance de leur existence pourrait tenter une action en s'attaquant aux paramètres et à la configuration par défaut. Si les bases de données **Northwind** et **pubs** sont installées sur l'ordinateur de production SQL Server 2000, supprimez-les.
- L'audit du système SQL Server 2000 est désactivé par défaut. Aucune condition n'est donc auditée. La détection des intrusions est donc plus difficile, ce qui permet aux pirates de rester anonymes. Activez au moins l'audit des connexions ayant échoué.

Pour obtenir les toutes dernières informations de sécurité relatives à SQL Server 2000, reportez-vous au site :
http://www.microsoft.com/sql/techinfo/administration/2000/security/default.asp

A propos de Microsoft Business Solutions

Microsoft Business Solutions, une filiale de Microsoft, propose un large éventail d'applications et de services professionnels intégrés complets qui favorisent les communications entre les PME/PMI, d'une part, et leurs clients, employés, partenaires et fournisseurs, d'autre part. Les applications Microsoft Business Solutions optimisent les processus commerciaux stratégiques dans différents domaines : gestion financière, comptabilité analytique, gestion des ressources humaines, gestion de projets, gestion des relations client, gestion des interventions, gestion logistique, commerce électronique, gestion de la fabrication et des points de vente. Ces applications sont conçues pour apporter de l'aide aux utilisateurs dans la réalisation de leurs objectifs commerciaux. Pour plus d'informations sur Microsoft Business Solutions, visitez le site http://www.microsoft.com/BusinessSolutions/.