SÉCURITÉ INFORMATIQUE

numéro 19 avril 1998

SÉCURITÉ DES SYSTÈMES D'INFORMATION

Spécial
sécurité Windows NT

Windows NT et la sécurité en quelques articles ?

Oui, c'est une sorte de gageure – je dirais même que c'est un fantasme. Traiter de la sécurité d'un système d'exploitation rodé est en soi déjà une tâche «d'un assez beau gabarit», mais quand il s'agit d'un système d'exploitation aussi nouveau, le défi est de taille.

éditorial

C'est pourquoi nous avons décidé, au sein de l'Observatoire de Sécurité des Systèmes d'Information et des Réseaux (OSSIR), de créer un groupe de travail spécialement consacré à Windows NT.

Ce groupe, dont j'assure l'animation avec Michel Miqueu du CNES, a une histoire récente et commence à donner ses premiers fruits, par exemple avec la participation à cette publication et la préparation de divers autres documents ayant trait à la sécurité de Windows NT.

Une autre de nos activités est de compiler (au sens littéraire du terme) et de commenter, si nécessaire, les différents «avis de sécurité» émis par les organismes internationaux habilités (ou pas, d'ailleurs). Nous pouvons également être amenés à vérifier nous-mêmes l'existence de failles de sécurité signalées ou supposées.

Les articles qui vont suivre, tous rédigés par des membres actifs du groupe, évoquent quelques points jugés importants, mais ne peuvent être en aucune façon vus comme exhaustifs, ni même considérés comme un extrait significatif.

Nous vous présenterons d'abord les opérations nécessaires à la configuration avec un minimum de sécurité d'un système nouvellement installé. En effet, un système pris immédiatement après une installation, même suivie du dernier Service Pack disponible (voir l'article sur la mise à jour du système), n'est pas destiné à fonctionner dans un environnement normalement sécurisé. Il faudra ajouter un peu d'huile de coude pour parvenir à une machine opérationnelle et pas trop vulnérable aux utilisateurs ou aux administrateurs maladroits ou malveillants.

Nous avions envisagé d'aborder la question délicate, s'il en est, de la «base de Registres» avec une description des «clés» utiles à connaître et éventuellement à modifier pour contrôler la sécurité de votre Windows NT. Denis Ducamp, de Herve Schauer Consultants, nous avait donné un excellent article sur ce thème. Malgré l'augmentation de la pagination, nous n'avons pas pu le prendre, faute de place. Cependant, cet article est partie intégrante du dossier et peut être retrouvé sur http://www.ossir.org/doc/registres.html.

Nous ne pourrons pas non plus fournir, car d'un volume prohibitif, le détail des failles de sécurité existantes ou potentielles ou résultant de mauvaises configurations ou installations, et leurs parades éventuelles. Pour des informations plus complètes et plus à jour, vous êtes invités à assister à nos réunions. Mieux, si vous avez des choses à dire sur le sujet, vous êtes cordialement invités à venir y participer.

Michel Gaudet
École des Hautes Études en Sciences Sociales
Co-animateur du groupe de travail
Sécurité Windows NT de l'OSSIR.
Courriel : Michel.Gaudet@ehess.fr

Sécurité informatique *fait peau neuve !*

Sécurité informatique a du succès. Malgré les conditions de plus en plus restrictives que nous imposons à l'abonnement, malgré l'épuration «à la hussarde» du fichier des abonnés, nous enregistrons une progression de 15% par an. Aujourd'hui vous êtes plus de 7000 à nous lire. Cette croissance – même maîtrisée –, la diffusion progressive de la connaissance informatique, modifient sensiblement notre lectorat et imposent de nous adapter: nous commençons avec ce numéro spécial NT, exceptionnellement de six pages. C'est que l'enjeu est d'importance: alors que de plus en plus de systèmes NT sont installés, les administrateurs ne savent pas toujours que la configuration par défaut est insuffisante.

À l'écoute de vos critiques et suggestions, il nous a paru souhaitable de renouveler la maquette de *Sécurité informatique*. Nous avons voulu améliorer l'organisation des articles, la clarté d'ensemble et le confort de lecture. Pour cela, il a fallu revenir à un style plus classique, certains diront plus professionnel, d'autres plus austère. C'est un changement dans la forme, non dans l'esprit! Nous désirons maintenir le «cachet grand public» de cette revue, même si ce numéro est exceptionnellement plus technique que d'ordinaire. C'est un pari: être professionnel **et** plaire au plus grand nombre! Le printemps, saison traditionnelle du renouveau, est bien choisi pour relever ce défi. *Sécurité informatique* change de peau, mais garde son âme. La revue restera simple et compréhensible par tous, avec parfois un brin d'humour, comme l'ont voulu à l'origine ses créateurs.

Robert Longeon

CNRS CENTRE NATIONAL DE LA RECHERCHE SCIENTIFIQUE

Configuration d'un serveur et d'une station de travail

La sécurité sous Windows NT

Microsoft propose avec Windows NT Server™ et Windows NT Workstation™ une offre de sécurité de bon niveau construite autour de fonctions couvrant la majeure partie des risques qui pèsent sur un réseau local. Bien que ces produits offrent une intéressante panoplie de mécanismes sécuritaires, deux inconvénients majeurs existent: tout d'abord, les outils standard d'administration disponibles dans Windows NT sont peu adaptés à la gestion de grand réseau, ce qui nécessite une lourde charge d'administration et oblige l'entreprise à respecter une formalisation stricte des règles de gestion pour conserver un niveau de sécurité efficace et cohérent. D'autre part, Microsoft propose une procédure d'installation du système très permissive. Après l'installation du système, pour disposer d'un environnement sécurisé, l'utilisateur doit impérativement activer des fonctions de sécurité, modifier des paramètres du système, restreindre les accès aux ressources et installer les dernières mises à jour.

La politique de sécurité d'un réseau sous Windows NT

La formalisation des règles de sécurité doit être incluse dans un document de portée générale et connu de tous: «La Politique de sécurité du réseau Windows NT». Il doit décrire l'organisation à mettre en place et les services de sécurité offerts aux utilisateurs pour garantir le niveau souhaité. La réalisation de ce document doit être le résultat d'une démarche réalisée selon trois étapes: dans un premier temps, l'identification des menaces pesant sur le système d'information et l'analyse des failles du système (Liste de vulnérabilités Windows NT, exemple: olivier.efri.hr/~crv/security/bugs ou www.dhp.com/~fyodor/sploits).

Puis, l'identification des responsabilités, l'attribution des rôles aux responsables de l'administration de la sécurité et la rédaction des règles décrivant les services mis à la disposition des utilisateurs pour couvrir les risques déduits de l'étape précédente. Enfin, prévoir le déploiement de cette politique, et notamment former les administrateurs à la mise en place des recommandations et sensibiliser les utilisateurs à faire appel aux mécanismes de sécurité offerts.

Installation d'un serveur et d'une station de travail

Nous nous limiterons, dans la suite de cet article, à traiter de la sécurité de l'installation et des recommandations minimales à respecter pour sécuriser le système. L'objectif est d'identifier les règles importantes sur lesquelles vous devez vous pencher lors de l'installation d'une machine afin de combler les lacunes de la procédure d'installation et les failles laissées volontairement ouvertes par Microsoft.

Installer Windows NT sur une partition NTFS

C'est l'une des recommandations les plus importantes, d'autant plus s'il s'agit de l'installation d'un serveur. Elle permet principalement d'attribuer des restrictions aux fichiers de la machine. Néanmoins, ce type de partition ajoute des fonctions de sécurité qui, pour être robustes, doivent être couplées à d'autres mesures de sécurité comme la protection du démarrage et la mise en place de règles d'utilisation des listes de contrôle d'accès (ACL). Rappelons que ces ACL, seulement disponibles en NTFS, permettent de spécifier les droits d'accès des répertoires (pas d'accès, lister, lire, ajouter et lire, modifier, contrôle total, accès spécial répertoire, accès spécial fichiers) et des fichiers (pas d'accès, lire, modifier, contrôle total ou accès spécial) en fonction des utilisateurs ou des groupes d'utilisateurs. Rappelez-vous que les fichiers, bien que protégés, sont vulnérables à tout accès en local (par démarrage sur une disquette système DOS et lecture par des utilitaires disponibles un peu partout, par réinstallation du système et donc réinitialisation des droits, vol du disque dur...).

Protéger les accès locaux aux stations et serveurs

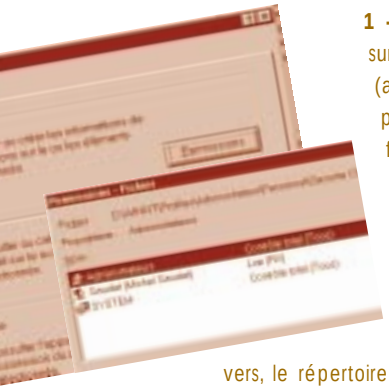
De manière physique (installer les serveurs dans des locaux dont l'accès est protégé) et de manière logicielle (en protégeant la machine contre un démarrage non standard). Ces fonctions ne sont pas offertes dans Windows NT mais sont proposées par les constructeurs sur les micro-ordinateurs: il s'agit des paramètres du Setup (en général accessibles à partir de *Echap* ou *F2* au démarrage du poste). Vous devez restreindre le démarrage de la machine à partir du disque dur et sous Windows NT uniquement, entrer un mot de passe administrateur pour protéger les paramètres du Setup, et, pour les serveurs, entrer un mot de passe de démarrage. Ces mots de passe ne devront pas être connus des utilisateurs.

Quelques URL intéressantes

http://www.ossir.org: charité bien ordonnée…
http://www.microsoft.com/security: évidemment.
http://www.microsoft.com/kb: base de connaissance de Microsoft.
http://olivier.efri.hr/~crv/security/bugs: une liste de bugs commentés.
http://www.dhp.com/~fyodor/sploits: une autre.
http://www.ncsa.com/hotlinks: une autre.
http://www.it.kth.se/~rom/ntsecindex.htm: FAQ (Foire Aux Questions) sécurité NT.
http://www.ntbugtraq.com: les archives de NTBugtraq, liste de diffusion d'avis de sécurité.
http://www.cert.org: la page d'accueil des CERT (centres spécialisés dans la sécurité informatique).
http://ciac.llnl.org: les archives CIAC (organisme officiel américain spécialisé dans la sécurité informatique).
http://www.ntinternal.com: une revue d'informations sur NT et W95 avec utilitaires téléchargeables.
http://www.rootshell.com: une revue de bugs de sécurité tous OS.
http://www.oakland.edu/~emcollie: avec un pointeur sur un document intéressant rédigé pour l'US Navy.
http://www.ntsearch.com: divers pointeurs intéressants.
http://www.jsiinc.com/reghack.htm: diverses infos sur les registres.
http://www.bhs.com: site avec pointeur sur utilitaires divers.
http://www.winntmag.com: un magazine spécialisé sur NT.
http://rcs42.urz.tu-dresden.de/~fh: un site avec plein d'infos sur NT et la sécurité. ■

Installer des permissions sur les fichiers du système

Le principal objectif est de protéger les données de sécurité (SAM) et d'empêcher des modifications non autorisées du système. La combinaison des permissions sur :
– les fichiers,
– les ruches de la base de registre,
– les privilèges de la stratégie de droits,
– les restrictions dans les Politiques Systèmes,
est une réponse satisfaisante mais complexe à mettre en œuvre.



1 - Les permissions sur les fichiers (accessibles par les propriétés des fichiers) doivent être utilisées notamment pour protéger en écriture les fichiers exécutables, les drivers, le répertoire WINNT («Tout le Monde» doit avoir le droit de lire uniquement) et le répertoire REPAIR, qui contient les données de sécurité sauvegardées et qui doit, bien sûr, être protégé contre tout accès non autorisé.

2 - Les ruches de la base de registre (voir l'article consacré aux registres http://www.ossir.org/doc/registres.html) doivent être protégées contre les accès du groupe «Tout le Monde»; seules les permissions suivantes doivent être accordées aux utilisateurs : «Retrouver la valeur», «Énumérer les sous-clés», «Notifier», «Lecture du contrôle». Le détail des permissions à attribuer est précisé dans le *White Paper* «Securing Windows NT Installation» disponible sur le site www.microsoft.com/security/. Attention : rappelez-vous que toute modification du registre peut entraîner une altération du fonctionnement du système. C'est pourquoi réalisez au préalable une sauvegarde de la base de registre.

3 - La stratégie de droits (définie à l'aide du gestionnaire des utilisateurs pour les domaines) devra protéger les accès à la machine en attribuant les privilèges nécessaires aux groupes d'administration et en supprimant les droits inutiles. En particulier, supprimer sur les stations et les serveurs les privilèges attribués au groupe «Tout le monde». Supprimer sur les stations «Ouvrir localement une session» pour les administrateurs de domaine et supprimer «Accès à cet ordinateur *via* le réseau pour les utilisateurs. Pour les serveurs, seules les personnes autorisées à utiliser la console du serveur doivent disposer du privilège «Ouvrir une session localement».

4 - Les Politiques Systèmes (définies à l'aide de l'éditeur de stratégie système) serviront, quant à

elles, à limiter les accès des utilisateurs au système et à restreindre leur environnement de travail aux seules applications dont ils ont besoin. Les fichiers décrivant ces politiques devront être stockés sur les serveurs et être protégés en écriture.

Modifier les valeurs des clés du registre

Le paramétrage par défaut de la base de registre de Windows NT est très permissif, c'est pourquoi des modifications doivent y être apportées (attention, avant de vous lancer dans la base de registre, réalisez une mise à jour des disquettes de réparation d'urgence fournies avec le système). Elles concernent les stations, les serveurs ou les deux.

Sur les stations

• Afficher une bannière d'information légale au démarrage des postes (renseigner les valeurs HKLM\Software\LegalNoticeCaption et HKLM\Software\LegalNoticeText)
• N'autoriser un client à se connecter qu'à des serveurs dont la sécurité des zones de partages a été renforcée (modifier la valeur de la clé HKLM\System\CurrentControlSet\Services\Rdr\Parameters\RequireSecuritySignature = 1)
• Sur les stations d'administration, cacher le dernier identifiant connecté (modifier la valeur de la clé HKLM\Software\Microsoft\WindowsNT\CurrentVersion\Winlogon\DontDisplayLastUserName = 1)
• Restreindre les accès du compte «invité» à la base de registre (modifier la valeur de la clé HKLM\System\CurrentControlSet\Services\LanManServer\Parameters\NullSessionPipes = 1)
• Sur les stations qui nécessitent une authentification réseau (stations d'administration), supprimer la fonction d'authentification local (modifier la valeur de la clé HKLM\Software\Microsoft\WindowsNT\CurrentVersion\Winlogon\CacheLogonsCount = 0).

Sur les serveurs

• Renforcer la sécurité des authentifications sur les zones de partage (modifier la valeur de la clé HKLM\System\CurrentControlSet\Services\LanManServer\Parameters\RequireSecuritySignature = 1)
• Cacher le dernier identifiant connecté (ajouter la clé HKLM\Software\Microsoft\WindowsNT\CurrentVersion\Winlogon\DontDisplayLastUserName = 1)
• Auditer l'utilisation des privilèges de sauvegarde (ajouter la clé HKLM\System\CurrentControlSet\Control\Lsa\FullPrivilegeAuditing = 1)
• Si vous utilisez les connexions RAS entrantes, auditer leur utilisation (modifier la valeur de la clé HKLM\System\CurrentControlSet\Services\RemoteAccess\Parameters\EnabledAudit = 1)
• Forcer l'arrêt du système lorsque les journaux d'audit sont pleins. Modifier la valeur de la clé HKLM\System\CurrentControlSet\Control\Lsa\CrashOnAuditFail = 1)
• Supprimer l'envoi systématique des mots de passe Lan Manager (modifier la valeur de la clé HKLM\System\CurrentControlSet\Control\Lsa\LMCompatibilityLevel = 1)
• Protéger l'intégrité de la procédure de démarrage supprimant les permissions d'écriture sur les clés suivantes : HKLM\Software\Microsoft\Windows\CurrentVersionRun et RunOnce et Uninstall)
• Supprimer la clé HKLM\System\CurrentControlSet\Control\Lsa\NotificationPackages\FPNPWCLNT)

Sur les deux

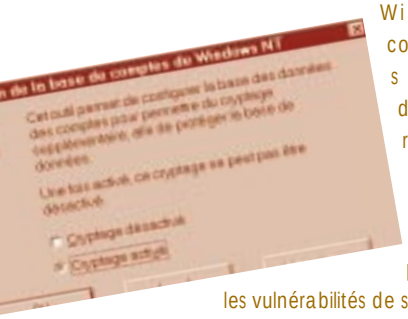
• Définir les groupes autorisés à accéder à distance à la base de registre (ajouter la clé HKLM\System\CurrentControlSet\Control\SecurePipeServers\Winreg\AllowedPaths).
• Protéger les journaux d'audit (système et application) contre des accès anonymes ou utilisateur (ajouter la clé HKLM\System\CurrentControlSet\Services\EventLog\[nom du journal]\RestrictGuestAccess = 1).

Les registres de NT4 relatifs à la sécurité

Vous pouvez trouver cet article de Denis Ducamp (Denis.Ducamp@hsc.fr) sur http://www.ossir.org/doc/registres.html ou sur http://www.hsc.fr/veille/nt/registres.html.
Cet article présente une synthèse de ce qu'il faut savoir sur le sujet. C'est un complément indispensable à ce dossier que nous n'avons pu malheureusement intégrer dans la revue, faute de place. ■

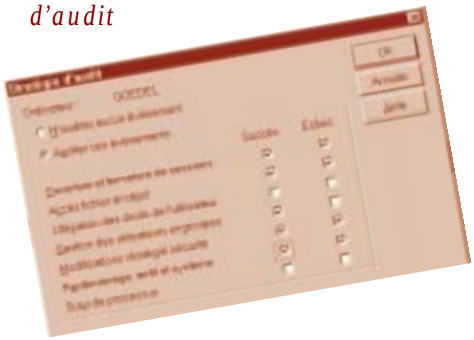
• Supprimer le partage des lecteurs de disquettes et de CD-ROM avec des process systèmes (modifier la valeur de la clé HKLM\Software\Microsoft\WindowsNT\CurrentVersion\Winlogon\AllocateFloppies = 1 et Allocate CDRoms = 1).
• Renforcer la protection de la base d'objets système (modifier la valeur de la clé HKLM\System\CurrentControlSet\Control\Session Manager\ProtectionMode = 1).
• Auditer les modifications de la base de registre (modifier la valeur de la clé HKLM\System\Current ControlSet\Control\Lsa\AuditBaseObjects = 1).
• Renforcer les règles de construction des mots de passe (ajouter la valeur de la clé HKLM\System\CurrentControlSet\Control\Lsa\NotificationPackages = «PASSFILT» et installer le driver correspondant).
• Réinitialiser le fichier cache à chaque arrêt de la machine (modifier la valeur de la clé HKLM\System\CurrentControlSet\Control\SessionManager\MemoryManagement\Clear PageFileShutdown = 1).

Exécuter SYSKEY et installer les Hot fix de sécurité



Windows NT™, comme tous les systèmes d'exploitation réseau, a fait l'objet de nombreuses attaques pour exploiter les vulnérabilités de ses mécanismes de sécurité.
En outre, des logiciels (les Cracker), disponibles sur Internet, permettent de découvrir les mots de passe utilisés par les utilisateurs définis sur le réseau ou sur les stations, malgré l'utilisation par le système d'une fonction de hashing pour chiffrer les mots de passe stockés sur la machine. Pour rendre inopérant ces logiciels et protéger le stockage des mots de passe, exécutez la fonction SYSKEY. Vous pourrez alors générer une clé de chiffrement (d'une longueur de 128 bits) qui sera utilisée pour renforcer l'algorithme de hashing utilisé en standard. Mais attention: l'exécution de cette fonction est irréversible et vous oblige à régénérer une disquette de réparation d'urgence (en exécutant la commande RDISK /s). Si vous ne souhaitez pas stocker la clé maître sur le disque dur, cette fonction vous permet également de limiter l'utilisation d'une station de travail: nécessité de saisir la clé à chaque démarrage du système ou introduction d'une disquette «clé» contenant la clé maître.
Pour les Services packs et les HotFix, voir l'article «La mise à jour de votre Windows NT».

Établissez une stratégie d'audit



À l'aide du gestionnaire des utilisateurs pour les domaines, définissez les événements qui devront être journalisés et qui seront analysés ultérieurement. L'objectif de cette journalisation est de disposer de la double capacité d'identifier une anomalie pouvant être à l'origine d'un sinistre ou d'une attaque et d'expliquer les raisons de la survenance d'un incident.
Les règles de journalisation à définir doivent être définies en fonction des risques que l'on cherche à couvrir. Par exemple, journaliser et analyser les traces générées par des connexions répétées sur les serveurs pour lutter contre les tentatives de pénétration par un compte du réseau.
Des stratégies d'audit devront être définies en fonction des événements recherchés dans les domaines de comptes (domaine responsable de la gestion et de l'authentification des utilisateurs), dans les domaines de ressources (domaines dans lesquels sont stockés et gérés les fichiers utilisateurs) et sur les stations pour lesquelles les accès et les modifications du système doivent être tracés notamment pour expliquer les raisons de la survenance d'un incident.

Établissez une procédure de contrôle de la conformité d'une machine avant son intégration au domaine

Il s'agit dans cette procédure de posséder une *check-list* sur la configuration du système avant la connexion d'une nouvelle machine sur le réseau.
Parmi les questions importantes:
– A-t-on réalisé un test du disque dur?
– A-t-on réalisé un contrôle anti-virus de la machine?
– La structure des répertoires est-elle conforme aux autres installations du réseau?
– Vérifier que la nouvelle station a été identifiée selon des règles de nommage habituelles.
– Vérifier que le Service Pack 3 a été installé et que les Hotfixes de sécurité ont été ajoutés.
– Vérifier que les logiciels d'administration et d'édition de registre ne sont pas présents sur les stations de travail.
– A-t-on protégé les fichiers systèmes?
– A-t-on ajouté et modifié des clés du registre pour combler les lacunes du système?
– A-t-on supprimé les zones de partage sur les stations de travail?
– A-t-on vérifié que les comptes «invité» sont verrouillés et qu'ils sont protégés par un mot de passe?
– A-t-on renommé le compte d'installation ? Le mot de passe de protection de ce compte est-il robuste?
– A-t-on généré les disquettes de réparation d'urgence? Pour les serveurs, ces disquettes sont-elles protégées contre toute divulgation?

Une fois ces tâches réalisées, vous devrez définir une stratégie de compte et les comptes et groupes d'utilisateurs sur les serveurs et les stations.

Conclusion

À la différence des systèmes d'exploitation de réseaux locaux antérieurs, qui imposaient une restriction forte des privilèges d'administration, les procédures d'installation de Windows NT™ sont très permissives, c'est pourquoi nous venons de montrer les principales recommandations techniques qui permettent de sécuriser le système.
Cet effort de sécurisation est d'autant plus important que la volonté forte de Microsoft de développer Windows NT™ sur toute plate-forme PC entraîne le risque de voir se développer une population large de «pirates informatiques» disposant d'une grande connaissance du système. Windows NT™ offre des fonctions de sécurité qui n'étaient jusqu'alors pas disponibles en standard sur les PC. Le passage à Windows NT™ apparaît en conséquence comme une formidable opportunité, mais aussi un grand risque, au cas où les bonnes options ne seraient pas définies à temps: «L'utilisateur n'est pas plus à l'abri après l'installation standard de Windows NT™ qu'il ne l'était avec l'ancien système DOS».

Il en résulte la nécessité lors de la migration vers des réseaux Windows NT™:
– de définir et de mettre en œuvre une véritable politique technique de sécurité,
– de mettre en place une administration de la sécurité structurée et cohérente.

Il est nécessaire de rappeler que certaines fonctions de sécurité de Windows NT™ bien qu'existantes s'avèrent parfois inefficaces du fait de leur complexité de mise en œuvre. C'est le cas par exemple de l'analyse des événements de sécurité. C'est pourquoi il est nécessaire de compléter la panoplie de fonctions par des utilitaires de sécurité disponibles sur le marché et capables de combler les lacunes de Windows NT™.

Jean Olive
Conseil en sécurité d'entreprise (ExenSe)
Courriel : Jeanolive@compuserve.com

Quelques éléments clés de la sécurité dans l'univers Windows NT

SRM. Security Reference Monitor est une partie du «noyau» NT. Il est chargé de protéger les objets systèmes des accès non autorisés et des modifications non permises.
LSA. Local Security Authority, entre autres tâches, gère la politique de sécurité définie par l'administrateur, génère les clés (tokens) d'accès, contrôle la politique d'audit et écrit les messages générés par le SRM.
SAD. Security Account Database est une partie de la base des Registres qui contient les informations de comptes d'utilisateurs et de groupes.
SAM. Security Account Manager contrôle et maintient la SAD. Il assure le service de validation des utilisateurs et fournit le Security Identifier (SID) au LSA qui générera alors les clés (tokens) d'accès.
PDC. Primary Domain Controler est le serveur qui possède l'autorité centrale d'accès à un domaine. Il peut être accompagné par un ou plusieurs BDC (Backup Domain Controler) qui reçoivent régulièrement une copie de la SAD du PDC et peuvent donc fournir le service d'authentification des utilisateurs aux clients (NT Workstations, ou NT Server autonome, ou autres) et remplacer le PDC en cas de défaillance. Ce doit être obligatoirement des systèmes NT. Quand un utilisateur est validé dans un domaine, il a accès aux ressources mises en commun (fichiers, imprimantes, applications, etc.) dans le domaine éventuellement par le PDC mais aussi par tous les serveurs déclarés dans ce domaine.
Il peut exister des relations de confiance établies entre domaines qui sont définies *a priori* à sens unique et qui permettent d'imposer une politique de sécurité donnée entre domaines multiples.
Administrateur. Nom donné par défaut (sur une machine sous NT francisé) au compte permettant de gérer la machine et le domaine. Il est sage de le renommer pour minimiser les risques associés à une attaque par essais de mots de passe. Il faut savoir que même si ce n'est pas très explicite dans la littérature Microsoft, il a, de fait, soit directement, soit indirectement, tous les accès à toutes les ressources d'un système ou d'un domaine. Il est même plus omnipotent que le root UNIX puisque son pouvoir s'étend au-delà du système sur lequel il est déclaré.
Accès physique. Une des précautions les plus élémentaires à prendre pour sécuriser une installation, on ne le répétera jamais assez, est la protection de l'accès physique à une machine; quiconque peut s'installer devant une console a déjà un pied dans le système. Si cette console est celle d'un serveur, c'est la boîte de Pandore ouverte.
Mot de passe. Ne pas traiter un PC sous Windows NT comme sous Windows 95: en particulier, ne jamais laisser un accès sans un mot de passe (même pour une Workstation isolée) quel que soit le compte utilisé – et *a fortiori* évidemment pour les comptes Administrateur. Un mot de passe NT peut avoir jusqu'à 14 caractères, et utiliser pleinement cette protection est une manière simple de minimiser les risques d'intrusions. ■

La menace virale

Les virus informatiques, bien que n'étant pas autant médiatisés qu'il y a quelques années, représentent toujours une menace bien réelle. Nous ne reviendrons pas sur ce sujet traité dans un précédent numéro de votre revue bien aimée, mais on peut dire que la menace des virus macros est sans nul doute la menace la plus importante aujourd'hui. Tout d'abord leur propagation est très rapide du fait de l'échange fréquent de documents par le biais des disquettes ou du courrier électronique, et, de plus, le même virus peut aussi bien fonctionner sur toutes les versions de Windows (3.11, 95 ou NT) que sous OS/2 ou Macintosh. La cible de ces virus la plus répandue est Word et ses documents.
À ce propos, un autre moyen de combattre les macros virus à la main (à rajouter à ceux évoqués dans le dernier numéro): il suffit de presser la touche SHIFT pendant le chargement du document sous Word et de nettoyer les sales bêtes par le menu macro.

Les virus sous Windows NT

Après avoir longtemps pensé que les mécanismes de sécurité sous Windows NT suffiraient à éliminer le risque d'infection virale, il est incontestable aujourd'hui que ce système d'exploitation est tout aussi vulnérable aux virus développés pour DOS et aux virus macros. Seules les fonctions de contrôle d'accès, si elles sont installées, limitent la propagation des virus. Mais elles constituent une faible protection qui n'est en aucun cas suffisante.
Les virus Systèmes se propagent sur un micro-ordinateur avant l'exécution du système d'exploitation installé sur le disque dur et donc avant l'exécution de Windows NT. Le virus s'installe sur la zone système (Secteur de Boot ou table des partitions). En fonction du type de virus, il endommage le système ou s'insère sur le disque de façon transparente. Dans le premier cas, le PC ne pourra plus démarrer sous Windows NT et souvent seule une réinstallation du système permettra de réparer le disque. Dans le deuxième cas, le virus est exécuté à chaque démarrage et peut lancer son attaque en provoquant des dommages identiques à ceux observés sous DOS. Néanmoins, après le démarrage du système, il ne pourra pas rester résident en mémoire (les interruptions DOS nécessaires au fonctionnement du virus ne sont pas comprises par Windows NT) et ne parviendra donc pas à se propager.
Il existe néanmoins un cas où l'infection d'un PC par un virus système demeure indécelable par un logiciel anti-virus: ça se produit si l'on installe Windows NT sur

suite ►

La mise à jour de votre Windows NT

Il est indispensable, pour minimiser les risques associés à la sécurité, d'avoir un système avec les dernières modifications apportées par le constructeur.

Dans le contexte Windows NT, il existe deux catégories de corrections de «bugs»: les corrections globales et cumulatives appelées les Services Packs ou SPX avec X numéro d'ordre et de chronologie, et les corrections au fur et à mesure de la manifestation ou de l'utilisation malveillante des vulnérabilités; on appelle ces dernières des HotFix.
Jusqu'à récemment, les Services Packs incluaient, en plus des corrections, des améliorations du système qui pouvaient aller jusqu'à l'ajout de fonctionnalités ou de services, voire même l'inclusion de commandes nouvelles. À partir du SP4 – pas encore sorti à l'heure de la rédaction de ce papier –, les corrections cumulées et les nouvelles fonctionnalités seront présentées dans des paquetages différents: SP4 pour les corrections et Options Pack (NTOP) pour les nouveautés.

Pour maintenir un système à jour, il faut donc, à partir de l'installation de base, passer le dernier SP (aujourd'hui le SP3), puis, en fonction de la protection que vous estimez nécessaire, passer les HotFix spécifiques correspondant aux vulnérabilités que vous voulez corriger.

Il faut noter que :
1. En cas d'installation de certains logiciels ou de nouveaux services, il peut être nécessaire de réinstaller le dernier SP, car il peut avoir changé des éléments (fichiers .dll par exemple) qui seraient écrasés par la nouvelle installation.
2. Les HotFix sont fournis par Microsoft «sans avoir subi toutes les régressions» autrement dit «sans garanties». Il ne faut donc passer que ceux que vous jugez vraiment nécessaires, même si on a rarement vu des HotFix, passés dans les conditions normales, provoquer des catastrophes.

Reste à savoir où se procurer ces SP et HotFix ? Auprès de Microsoft et/ou à partir de l'URL ftp://ftp.microsoft.com/bussys/winnt/winntpublic/fixes/{frn|usa|…}/nt40/

Remarque très importante : les versions de SP ou HotFix que vous passerez doivent être bien adaptées à la version de NT que vous utilisez : en langue américaine, française ou autre ; en effet, certaines corrections changent des librairies dynamiques (fichiers .dll) qui contiennent des spécificités de localisation. Toute erreur pourrait provoquer des instabilités du système entraînant la nécessité d'une réinstallation complète. Donc, dans le doute, toujours n'installer que des versions pour NT français, US ou serbo-croate suivant le cas.
Pour des infos récentes sur les versions localisées disponibles, voir:
http://www.ntbugtraq.com/mustfix.htm ■

Michel Gaudet

La menace virale suite

une machine déjà infectée par un virus de Boot (virus système stocké dans le Boot de la machine). En effet, lors de l'installation de Windows NT sur un PC déjà infecté, la procédure d'installation copie le secteur de boot du PC (secteur infecté) à un autre endroit sur le disque dur et remplace l'original par un secteur de boot spécifique à Windows NT. La machine contient alors un secteur de boot sain (Windows NT) et une copie du secteur de boot original (secteur infecté) qui n'est pas stocké au début du disque dur. Or les logiciels anti-virus ne recherchent les virus systèmes qu'au début du disque dur (piste 0 du disque); ils ne pourront donc pas détecter la copie du secteur infecté réalisée par Windows NT.

Si, de plus, l'utilisateur choisit d'installer un Dual Boot sur cette machine (fonction offrant le choix du système d'exploitation au démarrage du PC: Windows NT/ DOS /WINDOWS 95) à chaque démarrage sur DOS ou Windows 95, le secteur de boot original (secteur infecté) sera exécuté et le virus deviendra actif. Or, devenant actif, même si le PC est muni de logiciels anti-virus scannant la mémoire, ces logiciels ne peuvent le détecter à coup sûr.

En conséquence, il est fortement recommandé de réaliser un contrôle anti-virus avant l'installation de Windows NT. Dans la mesure du possible, effectuez ce contrôle avec un logiciel anti-virus à jour et selon une procédure de vérification imposant un démarrage de la machine à partir d'une disquette système saine.

Les virus Programmes, quant à eux, fonctionnent sous Windows NT, mais causent souvent des erreurs systèmes qui les empêchent de se propager aussi bien que sous DOS. Néanmoins, on observe depuis peu des virus développés pour fonctionner sous Windows 95 et qui, eux, fonctionnent à merveille sous Windows NT. Seul un examen du disque dur avec un logiciel anti-virus disposant d'une mise à jour récente (moins de deux mois) permet de détecter ces virus.

Un virus dispose des mêmes permissions d'écriture (nécessaire à sa propagation) que l'utilisateur qui l'a exécuté: si l'administrateur protège contre l'écriture les fichiers de programmes, l'utilisateur ne peut pas modifier le code de ces programmes et le virus, déclenché par ce dernier, ne le peut pas non plus.

Les virus macros peuvent perpétrer n'importe quelle action malveillante, de la simple nuisance liée à sa propagation à la destruction de fichiers en passant par la diffusion de virus «classique». La vocation des langages de macros qu'utilisent ces virus est d'automatiser des opérations des logiciels Bureautique. Toutes les fonctions accessibles par ces commandes macros sont donc offertes au virus pour atteindre leur but malveillant.

Les symptômes les plus courants sous Word, caractéristiques de l'infection par un virus macro, sont: les documents enregistrés sont des modèles de document et non des fichiers standard; la commande Macro du menu Outil n'est pas disponible (soit inexistante, soit en grisé, soit elle n'a aucun effet); la présence de macros inexpliquées de type AutoOpen, AutoClose, Auto<...>

La protection contre les virus

Windows NT™ n'offre pas en standard de fonctions spécifiques de protection anti-virus. Néanmoins, certaines de ses fonctions de sécurité pourront être utilisées pour protéger le système contre une propagation virale. Mais l'utilisation de ces fonctions doit être complétée par l'acquisition d'un (voire deux) logiciels anti-virus du marché (comme Viruscan de Mc Afee, Norton Anti-virus de Symantec, F-Prot de Informatique et développement, Dc Solomon Anti-virus de Doctor Solomon, Sweep de Sophos,...).

Le critère principal de sélection d'un logiciel anti-virus ne doit pas être le nombre de virus détectés mais sa compatibilité intégrale avec Windows NT. Le choix devra également prendre en compte sa capacité à pouvoir détecter les virus macros, la fréquence de mise à jour de sa base de signatures (qui doit être égale à deux mois au moins), sa compatibilité avec les autres systèmes que vous utilisez et enfin la qualité du support technique proposé avec l'achat du produit.

L'utilisation d'un logiciel anti-virus ne vous dispense pas d'élaborer une stratégie de protection contre les virus qui doit être constituée d'une combinaison de mesures de prévention, de détection et de protection.

L'objectif de cette stratégie est de construire autour du parc de micro-ordinateurs un espace de confiance disposant des caractéristiques suivantes:

1. Garantie d'innocuité des informations qui y sont véhiculées (contrôle de tous les flux entrant et sortant).
2. Définition et garantie de la cohérence de la protection anti-virus au sein de l'espace de confiance (fonctions anti-virus identiques et à jour sur toutes les machines).
3. Maintien du niveau de sécurité de l'espace de confiance (contrôles anti-virus fréquents et réguliers).

Parmi les moyens anti-virus à employer, voici les plus importants :

Moyens de prévention

• Paramétrez le Setup du PC afin que, lors de la mise sous tension, le BIOS recherche en priorité le système d'exploitation sur le disque dur («Démarrage en priorité sur C:»).

• Utiliser un système de fichier de type NTFS, protéger les exécutables (*.exe, *.dll, *.bat) contre l'écriture et, dans la mesure du possible, évitez d'offrir dans les zones de partages à la fois des droits d'exécution et d'écriture.

• Protéger toutes les disquettes contre l'écriture.

• Utiliser les stations de travail avec un profil Utilisateur.

• Si possible, protéger le normal.dot contre l'écriture et sauvegardez-le.

Moyen de détection

• Assurez-vous que tout support (disquette, CD ROM,...) ou fichier (y compris les documents reçus par pièce jointe) provenant de l'extérieur sont vérifiés **avant leur utilisation** par un logiciel anti-virus **à jour**.

• Réalisez un contrôle anti-virus périodique de votre environnement de travail (utilisation des fonctions de déclenchement de vérification anti-virus programmées).

• Réalisez une vérification du disque dur après toute mise à jour du logiciel anti-virus installé et lors de toute anomalie du système (ralentissement excessif, démarrage anormal, fonctions disparaissant dans les menus de Word,...).

• Réalisez une vérification anti-virus après toute restauration de sauvegarde.

Moyens de protection

• Centralisez la gestion des incidents anti-virus et, en particulier, lors d'une détection virale, avertissez vos collaborateurs et recherchez la source de l'infection.

• Conservez les disquettes de réparation d'urgence et mettez-les à jour régulièrement.

• Procurez-vous des utilitaires de réparation de disque dur compatibles avec Windows NT (par exemple, les Norton Utilities de Symantec).

• Munissez-vous d'un deuxième logiciel anti-virus pour confirmer les détections virales.

• Assurez-vous de la disponibilité du support technique de l'éditeur du logiciel anti-virus et n'hésitez pas à la contacter en cas de toute alerte virale.

Jean Olive
Conseil en sécurité d'entreprise (ExenSe)
Courriel : Jeanolive@compuserve.com

SÉCURITÉ INFORMATIQUE
numéro 19 avril 1998
SÉCURITÉ DES SYSTÈMES D'INFORMATION

Sujets traités : tout ce qui concerne la sécurité d'information. Gratuit.
Périodicité : 5 numéros par an.
Lectorat : toutes les formations CNRS.

Responsable de la publication :
ROBERT LONGEON
Centre national de la recherche scientifique
Service du Fonctionnaire de Défense
c/o IDRIS - BP 167. 91403 Orsay Cedex
Tél. 01 69 35 84 87
Courriel : robert.longeon@cnrs-dir.fr
http://www.cnrs.fr:Infosecu

ISSN 1257-8819
Commission paritaire n° 3105 ADEP

Conseil et coordination : CNRS - MIST - Jacqueline Leclère • Conception et réalisation : La Souris 01 45 21 09 61