Préface

Qu'est-ce que la sécurité ? A priori, c'est le sentiment, à tort ou à raison, d'être à l'abri de tout danger. Cependant doit-on se limiter à cette définition ? Assurément non. Bien qu'elle présente un postulat de départ satisfaisant, il ne faut pas s'y arrêter. Une autre formulation plus adaptée au contexte des systèmes d'information pourrait être la suivante : protéger l'intégrité, assurer la disponibilité et garantir la confidentialité des biens.

La sécurité informatique a toujours été vue comme le parent pauvre du domaine des technologies de l'information numérique. Elle constitue pour beaucoup une contrainte et un investissement en temps, ressources et argent. Longtemps, les utilisateurs et administrateurs n'ont pas bien vu la nécessité d'entreprendre des actions de sécurisation et les décideurs n'ont pas eu d'idée concrète du retour sur investissement qu'elles impliquaient. Aujourd'hui, les directeurs ont pris le tournant de la sécurité des systèmes d'information. Elle est progressivement devenue une préoccupation majeure s'intégrant dans les définitions de politiques de gestion des risques, motivées par le sentiment latent d'insécurité.

Avec 85 % du marché des systèmes d'exploitation, Windows est aujourd'hui incontournable. Quel que soit le pays, des plus petites entreprises aux multinationales, mais aussi chez les particuliers, le système d'exploitation de Microsoft est présent, dominant le marché. Succès indubitable depuis son parent MS-DOS, il a su s'imposer aussi bien au niveau des postes de travail que des serveurs, grâce à la puissance commerciale et marketing de la firme de Redmond.

Vis-à-vis de la sécurité, Windows a connu une histoire mouvementée, et une réputation d'instabilité chronique a collé aux anciens systèmes Windows 95, 98 et ME (qui n'a jamais rencontré les tristement célèbres « écrans bleus » ?). Par la suite, avec l'arrivée des systèmes

Précision

Puissance commerciale de Microsoft

La firme de Redmond a annoncé un budget de 900 millions de dollars pour la promotion de Windows Vista et Office 2007.

Windows 2000 et XP et la généralisation du noyau NT à tous les postes, de nouveaux défis pour les administrateurs sont apparus avec le développement des réseaux, l'ouverture sur Internet et plus récemment l'apparition d'infrastructures spontanées.

Les défaillances logicielles ne sont plus alors de simples nuisances pour l'utilisateur, mais des failles majeures qui profitent aux virus, chevaux de Troie, spammeurs et autres pirates informatiques. Armes de la cybercriminalité, certaines de ces menaces peuvent aussi, indirectement, conduire à d'importants dommages financiers. Ainsi, bien qu'il soit relativement difficile de les estimer, des sommes de l'ordre de plusieurs milliards de dollars ont été avancées suite à des dommages causés par des programmes malveillants comme le ver Code Red affectant le serveur web IIS de Windows NT 4.0 et 2000. Dès lors, Microsoft a pris la sécurité beaucoup plus au sérieux et a développé de nouveaux moyens de protection pour ses systèmes et applicatifs. Cependant, chacun de ces ajouts était motivé par l'apparition de codes malveillants qui exploitaient des failles du système.

C'est avec la forte croissance du développement des vers comme Blaster, Sasser ou Nimda que Microsoft s'est réellement engagé en définissant une politique de sécurité s'appliquant à tous ses produits. La sécurité a été clairement introduite dans le cycle de vie des logiciels et son suivi a été structuré avec l'apparition des bulletins mensuels. Avec Windows XP Service Pack 2 et Windows 2003, la firme de Redmond a fait un pas dans la bonne direction grâce à l'ajout de fonctionnalités intéressantes comme le pare-feu et le mécanisme de protection de la pile (réduisant les possibilités d'exploitation des débordements de tampon). Après de nombreuses vulnérabilités affectant les fonctionnalités réseau depuis 2003, Windows connaît actuellement un grand nombre de failles de sécurité sur la suite Office, dévoilées pour la plupart dès leur découverte (en *0-day*), ne laissant pas le temps à Microsoft de proposer un correctif. Comme les personnes malveillantes cherchent à atteindre le plus de machines possible, ce nombre important de failles connues est en particulier lié au fait que Windows est le plus déployé des systèmes d'exploitation.

PRÉCISION Utilisateurs des autres sytèmes

Si ce livre traite spécifiquement de Windows, il expose des principes concernant la nécessité de sauvegarder et les attaques réseau qui touchent tous les systèmes d'exploitation (Mac et Unix/Linux).

Ce tableau est pessimiste... Cependant, l'utilisateur de Windows a les moyens de rendre son système d'exploitation robuste contre les menaces existantes. Microsoft a implémenté dans la famille au noyau NT un modèle de sécurité complet, mais complexe. De nombreuses possibilités de sécurisation du système sont proposées, malheureusement elles ne sont la plupart du temps pas toutes employées efficacement. La configuration par défaut de Windows n'est pas encore un parfait exemple de sécurité (on pourra ici citer OpenBSD qui s'en approche). C'est pour-

quoi sa sécurisation nécessite un minimum de sensibilisation pour configurer correctement le système. La difficulté réside ici dans l'exhaustivité de l'application de ces mesures. En effet, si la sécurité est une chaîne, sa solidité est égale à celle du plus faible de ses maillons. Par exemple, utiliser EFS pour chiffrer ses données est une bonne pratique, mais associer cela à un mot de passe faible pour le compte Administrateur compromet grandement les chances d'obtenir un système sûr.

L'apprentissage de la sécurisation d'un système est une tâche comme les autres et, comme lorsqu'on apprend à faire du vélo, il est nécessaire de pratiquer : rien ne remplace l'expérience ! Sachez prendre du recul vis-à-vis des possibilités offertes. Persévérance, sérieux et précision permettent de protéger un système tout en conservant tout son potentiel fonctionnel.

Quelles sont les perspectives pour le système de Microsoft ? Si les annonces concernant la sécurité de Windows Vista ont été nombreuses, la réécriture de grandes parties du système soulève plusieurs questions, en particulier en ce qui concerne l'implémentation de nouvelles fonctionnalités de sécurité (seront-elles exemptes de failles ?). À l'aube de l'année 2007 et de Vista, l'utilisateur de systèmes Windows ne sait pas encore ce que lui réserve l'avenir. Voilà une raison de plus pour s'intéresser de près à la sécurité de son ordinateur.

Un dernier conseil : n'oubliez pas d'être curieux et ouvert. Toutefois, il n'est pas nécessaire d'insister sur ce point : vous vous êtes déjà emparé de ce livre !

Benjamin Arnault
Hervé Schauer Consultants