

La sécurité, une affaire d'organisation

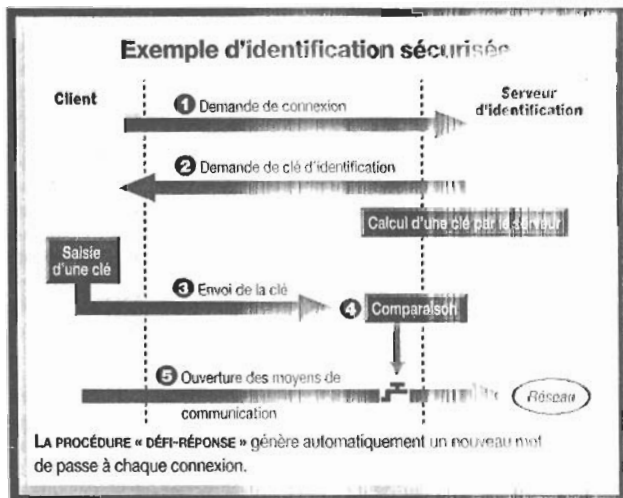
Si les entreprises commencent peu ou prou à prendre conscience des problèmes de sécurité posés par Internet ou Intranet, elles ne savent toujours pas déterminer le degré de protection à mettre en œuvre et les outils appropriés. Ni, a fortiori, comment faire appliquer en leur sein les règles de sécurité.

Avec l'installation de services Internet toujours plus nombreux, les entreprises ouvrent allégrement leur système d'information vers l'extérieur, sans trop se soucier des problèmes de sécurité qui peuvent en découler. Et la situation n'est guère plus brillante dans les sociétés où l'on se contente d'un Intranet ou d'un réseau local « classique », faisant aveuglément confiance au système de mots de passe installé sur les serveurs ; pourtant c'est le plus souvent de l'intérieur même de l'entreprise que proviennent les attaques les plus dommageables. « Il y a des entreprises, les PME notamment, qui se moquent éperdument de la sécurité parce qu'elles ont d'autres priorités, tandis que d'autres, généralement des grands comptes, ont une politique de sécurité très contraignante. Entre les deux, on trouve de nombreuses sociétés qui font les choses à moitié, en se reposant sur quelques produits et consignes », résume Alfonso Castro, chef produit Exchange Server chez Microsoft.

Des procédures imposées aux fournisseurs et aux sous-traitants

● Les plus grandes entreprises, qui ont depuis belle lurette mesuré l'importance des questions de sécurité,

dont celle de l'authentification, imposent ces procédures à leurs fournisseurs et sous-traitants. Mais cela ne suffit pas toujours, nombre de sociétés se contentant pour leur protection d'installer un « firewall » sur leur réseau. Dans d'autres entreprises, à l'inverse, les contraintes de sécurité sont disproportionnées par rapport à l'importance des informations. Un simple annuaire d'entreprise n'exige pas le même niveau de protection que d'autres informations vitales. « Les réseaux et les intranet, ainsi que les accès sur des serveurs confidentiels, les échanges "business to business" et, sur Internet, les télé-services bancaires, l'édition électronique, le commerce électronique... », tels sont selon Pascal Thoniel, président de NIX Research, les domaines où l'authentification revêt le plus d'importance. Pour sa part, Frédéric Engel, responsable marketing chez Activecard, décompose le marché de la sécurité en trois segments. « Il y a d'abord la sécurité interne, pour éviter qu'un collègue usurpe votre identité, mais les échanges avec les fournisseurs, filiales ou sous-traitants, doivent aussi être pris en compte, explique-t-il. C'est la plus grosse part du marché de l'authentification. Vient ensuite le créneau de l'interentreprise, qui nécessite une authentification réciproque (cha-



qu'il échange des informations avec le bon interlocuteur), et celui de l'interopérabilité, les diverses sociétés ne disposant pas forcément de systèmes de sécurité compatibles. Enfin, il y a le marché grand public, le plus porteur pour l'avenir mais aussi le plus compliqué. » Dans les deux premiers cas, les intervenants sont connus, ce qui permet de refuser l'accès à tout individu non répertorié. Sur le marché grand public, en revanche, on a au départ affaire à des inconnus, notam-

ment via serveurs Internet, qu'il faut identifier (ne serait-ce que pour valider des transactions financières dans le cadre d'une application de commerce électronique) tout en leur conférant des droits d'accès correspondant à leur statut.

Suivre la trace des intrusions et déterminer leur origine

● La première fonction de l'authentification est, bien sûr, de permettre l'accès à un système d'information aux personnes autorisées. Mais ce n'est pas la seule. Aucun système de sécurité n'étant fiable à 100 %, de l'avis même des concepteurs de ces solutions, il faut aussi pouvoir suivre la trace des intrusions et déterminer leur origine pour retrouver le coupable. Une fonction que remplissent de nombreux firewalls. Le responsable de la sécurité de l'entreprise devra donc suivre avec attention les alertes remontées par le système de sécurité en cas de tentative d'intrusion, de façon à entendre ce flux entrant ou à le laisser passer en le « pistant ». Cela, en déconnectant les informations vitales du réseau, pour repérer l'origine de l'attaque, sans prendre de risque inutile. Les solutions d'authentification se sont nettement perfectionnées au fil des

La prison pour les intrus

La France est très en avance en matière de répression des atteintes aux systèmes d'information grâce à la loi Godfrain, estime Christiane Féral-Schuhl, du cabinet FG Associés, avocate au barreau de Paris. L'intrusion non autorisée sur un système de traitement automatisé d'informations constitue une infraction sanctionnée lourdement. Il en serait ainsi pour la lecture non autorisée de courrier électronique. « De fait, l'intrusion dans un système d'information est punie d'une peine de un an

de prison et de 100 000 francs d'amende, peine multipliée par deux en cas d'altération ou de suppression de données... Sans compter des peines annexes, telles que la privation de droits civiques, la confiscation des matériels ayant servi à l'intrusion ou la fermeture de l'établissement qui a « couvert » l'acte incriminé. Sauf dans de rares cas, la loi pénale n'est applicable que pour les délits et crimes commis sur le sol français. Mais comment appréhender les contrevenants sur le réseau ? Des organisations

internationales se sont mobilisées sur le sujet. Ainsi du Conseil de l'Europe qui, dès octobre 1995, invitait les Etats à prendre des mesures internes pour conclure des conventions bilatérales et multilatérales, afin de permettre aux autorités chargées d'enquêtes d'intervenir sur les réseaux. C'est aussi le cas de l'Ompi (Organisation mondiale de la propriété intellectuelle), qui regroupe plus de cent pays et propose un traité des droits d'auteur visant à harmoniser les législations de ses Etats membres.

ans. Des tout premiers systèmes, où le mot de passe fourni par l'utilisateur transitait en clair sur le réseau vers un serveur, on est passé à un chiffrement de ce mot de passe, le rendant illisible à l'éventuel pirate écoutant la ligne. Mais toute personne connaissant ce mot de passe peut entrer sur le système. C'est pourquoi on a institué le mode « défi-réponse », qui limite la récupération d'un éventuel mot de passe. Ainsi lors de la connexion d'un poste client à un réseau, le serveur envoie un « défi » (jamais le même), que seul un utilisateur autorisé peut résoudre. Cela grâce à son code confidentiel et à une procédure associant le défi envoyé par le serveur à ce code pour calculer une réponse, ou clé, qui sera renvoyée au serveur puis comparée à ce qu'il attendait, avant d'accepter ou de refuser l'entrée dans le système d'information. L'avantage de ce mode est que le mot de passe ne transite pas sur le système, les seules données échangées (le défi et la réponse) étant différentes à chaque connexion. Ces systèmes à « mot de passe dynamique » s'appuient généralement sur des périphériques physiques comme les « caulettes » proposées par Safedata Systems ou Activecard. L'utilisateur saisit, sur la caulette, son code confidentiel et le défi envoyé par le serveur; elle affiche en retour la réponse à fournir au serveur. Plutôt sûr, ce système présente l'inconvénient d'être assez cher (il faut compter 200 à 400 francs-ht par caulette), ce qui freine son utilisation pour des services de commerce électronique.

Un trousseau de un milliard de clés aléatoires

● Cela a conduit NTX Research à mettre au point la solution Internet Passport/Digipass, basée elle aussi sur un mode défi-réponse mais utilisant une disquette comme support physique d'authentification. Protégée contre la duplication et ne stockant à aucun moment le code confidentiel de l'utilisateur, la disquette contient un « trousseau » d'un milliard de clés aléatoires (ou plus si le client le souhaite) qui, associées au mot de passe de l'utilisateur, vont permettre au poste client d'envoyer au serveur une clé dynamique répondant au défi lancé par le serveur, à partir d'un trousseau comportant un nombre de clés similaires. Cette solution n'utilise pas d'algorithme spécifique pour calculer la ré-

ponse. Elle exploite un mécanisme aléatoire basé sur son trousseau de clés, encore plus compliqué à « casser ». Les cartes à puce, réputées inviolables, constituent un support d'authentification encore plus sûr, mais leur développement est entravé par le coût des lecteurs à raccorder aux postes clients.

Ces solutions se combinent généralement avec les procédures d'authentification offertes par les routeurs, firewalls ou serveurs d'accès distants, qui exploitent soit les protocoles Tacacs+ ou Radius (en mode défi-réponse), soit la norme X509 (un sous-ensemble de la norme X500), qui définit la gestion de certificats numériques, pour offrir une sécurité renforcée.

Les solutions d'authentification fiables ne manquent donc pas. Mais tout le monde s'accorde à reconnaître que la principale faille de tout système de sécurité est l'aspect humain. La mise en place d'une politique de sécurité efficace implique donc une réelle sensibilisation des utilisateurs (voir le témoignage de Patrick Gauvert, p. 44) et une démarche raisonnée de la part du responsable de la sécurité dans l'entreprise. « *Tout d'abord, note Alfonso Castro, il est préférable que responsable du réseau et responsable de la sécurité soient des personnes différentes, le premier ayant pour tâche de tout ouvrir, alors que le second est là pour fermer les accès.* » La sécurisation passe aussi par l'adoption de règles élémentaires : « *Il faut changer régulièrement les mots de passe, ne pas réutiliser les anciens, combiner chiffres et lettres avec au moins cinq caractères, prohiber les mots de passe "faibles" (du style 1234 ou Azerty)* », précise Christophe Domergué, responsable marketing produit Intranetware chez Novell. La liste des précautions à prendre en la matière est longue, et la démarche, peu évidente. Mais, pour une vue complète de la question, on peut se reporter au remarquable livre blanc *How to Develop a Network Security Policy, an Overview of Internetworking Site Security* publié par Sunsoft. La sécurité impose encore que personne, y compris le responsable de la sécurité de l'entreprise, n'ait connaissance du mot de passe d'un utilisateur ni ne puisse lire le contenu des messages qu'il envoie via le courrier électronique. Enfin, note Christophe Talon, président de Safedata Systems, « *on met souvent en balance sécurité et contrainte* ». Ainsi, éviter que trop de sécurité ne

Le rétro-appel permet de localiser l'utilisateur

La protection par nom d'utilisateur et mot de passe ne suffit pas toujours. Le « rétro-appel » (call-back) est encore l'une des meilleures méthodes pour s'assurer que la personne qui se connecte par modem à un réseau d'entreprise a bien le droit de le faire. Durant une première phase, l'utilisateur se connecte à l'équipement modem, s'identifie, et la communication est automatiquement coupée. Dans une deuxième phase, le modem ayant reçu la demande de

connexion rappelle l'utilisateur à un numéro mémorisé dans une table des utilisateurs autorisés. Le prix des modems qui prennent ce processus en charge est élevé, mais ils permettent d'interdire l'accès au réseau avant identification. La plupart des systèmes d'accès distants prennent maintenant en compte cette fonction de rétro-appel, gérée par logiciel, ce qui en diminue le prix, mais réduit la sécurité, l'accès étant tout de même autorisé sur une partie du réseau avant identification.

nuise à la sécurité implique de ne pas surprotéger l'accès à des données essentielles (utiliser un système de type Activecard pour joindre une messagerie électronique, par exemple); il convient d'attribuer le niveau de sé-

curité approprié à un service ou à un site donné. C'est là toute la complexité de la tâche de responsable de la sécurité, qui doit réunir compétences techniques, juridiques et humaines. ■

Suite du dossier page 44

13 Fax

Zetafax • Omtool • RightFax • Cheyenne • FaxMaller • Delrina • Forestrac • Tobit

Rendez-vous au sommet avec l'inventeur de la carte fax intelligente







- Analogiques et numériques
- Mono
- Multi-voies
- Intelligente et programmable
- Routage des fax entrants
- A.P.I. (Dos, Unix, Windows NT, OS/2)
- Agréées DGPT



Toutes les marges et idées sont déposées par Sitel (http://bit.ly/103p3t6)