

2002, L'ANNÉE DE TOUS LES CHALLENGES

On ne peut guère parler de l'année 2001 sans évoquer ce qu'il est désormais convenu d'appeler les événements du 11 septembre. La vague d'incertitude qui en a résulté a en effet affecté l'ensemble des pays développés, renforçant l'attentisme des décideurs et aggravant une situation économique déjà précaire.

Contrairement à ce qui avait été précipitamment déclaré par certains analystes financiers, ce drame n'a pas eu d'effet dopant sur le marché de la sécurité informatique des systèmes et réseaux. En effet, le commerce électronique, qui avait été l'un des principaux moteurs de la sécurité, a malheureusement aussi entraîné cette dernière dans sa chute. La période durant laquelle chaque grande banque était à l'origine de plusieurs Bourses en ligne, et donc d'autant de projets de sécurité, est belle et bien révolue. C'est désormais le règne quasi sans partage des réorganisations, rachats, et autres fusions. La frénésie de réduction des coûts à court terme après les années de largesse ne laisse guère de chance aux prestations en sécurité, généralement considérées comme superflues.

Mon sentiment est que, en ce qui concerne le marché de la sécurité, le 11 septembre a surtout fait prendre conscience de l'importance des plans de continuité. Ainsi que l'a déclaré Jean-Laurent Santoni lors de l'Assemblée Générale du Clusif : "Le problème n'est pas de se demander ce qu'il peut arriver ? Car tout peut arriver, mais plutôt comment continuer l'activité quoiqu'il arrive". Les analyses de risques permettaient d'établir des plans de secours viables, il convient dès lors de réaliser quels sont les vrais enjeux : l'organisation de la sécurité doit évoluer et les responsables d'entreprises doivent intégrer la sécurité informatique dans leurs responsabilités au même titre que les accidents du travail.

L'industrialisation des méthodes de la sécurité s'inscrit dans cette nécessaire évolution, mais rend omniprésente la norme anglaise BS7799, qui devient alors une cible au lieu d'être un des guides de bonnes pratiques en matière de sécurité.

D'un autre côté, les aspects techniques restent sous-évalués et la sécurité des réseaux IP n'est pas toujours suffisamment intégrée à la conception de ces réseaux comme dans la politique de sécurité des entreprises. Les vers Code Red et Nimda résultent de

la monoculture, mais ont souvent mis à jour des lacunes dans la gestion des correctifs de sécurité d'une part et dans la gestion des incidents d'autre part. Très à la mode, les réseaux sans-fils se multiplient sans contrôle, et donc sans sécurité. Ce sont ainsi des milliers de PME qui sont vulnérables, ce que des tests menés à Paris avec l'équipement adéquat suffisent à démontrer. Ces réseaux utilisent des bornes mal réglées, et ne fonctionnent jamais en configuration sécurisée. Dans ces conditions, quelles sont les responsabilités des vendeurs et installateurs de ces équipements ?

Le nouveau protocole de l'Internet en entreprise est aujourd'hui HTTP, autorisé par les firewalls des entreprises. Les risques inhérents à cette situation peuvent être illustrés par deux phénomènes d'importance croissante : le détournement d'HTTP par les utilisateurs dans les entreprises, et la migration de l'EDI vers HTTP. En effet, les employés utilisent de plus en plus l'accès Internet par HTTP des entreprises pour exporter leur messagerie d'entreprise, leur agenda partagé et même leurs fichiers. Cette année certains responsables de sécurité ont ainsi découvert que leur politique de sécurité était contournée par des utilisateurs qui géraient leur messagerie hors de l'entreprise sur des portails dédiés. Quant à la migration du monde EDI/X400 et son explosion à venir avec la formalisation des échanges en XML, elles nous apportent de nouveaux protocoles, tous encapsulés dans HTTP, et pouvant donc contenir des commandes et du code mobile. En conséquence, de nouveaux risques de dénis de service, de falsification, d'usurpation d'identité, apparaîtront probablement dans les prochains mois.

L'année qui a commencé s'annonce donc comme riche de challenges pour le monde de la sécurité. Pour vous aider à mieux appréhender ce domaine en perpétuelle évolution, le guide des acteurs du marché français est complété par le panorama de l'actualité en sécurité, un guide pour choisir un fournisseur de services d'infogérance, un lexique, ainsi que par les listes des associations, revues et manifestations en sécurité.

Nous vous souhaitons à tous un bon salon Infosec 2002.

Hervé Schauer

PANORAMA DE L'ACTUALITÉ EN SÉCURITÉ FÉVRIER 2001 – FÉVRIER 2002

Introduction

Comme tout exercice de style, le choix des événements marquants de l'année ne prétend ni à l'exhaustivité, ni à la neutralité absolue. Les sujets retenus offriront au lecteur un panorama indépendant lui permettant de mieux appréhender les évolutions à venir.

Appliances

L'observateur attentif dans ce domaine aura détecté ce qui s'annonce comme une évolution majeure. En effet, afin de faciliter la gestion des réseaux et de leur sécurité, les fournisseurs de boîtiers commencent à développer des produits intégrant des systèmes de gestion. Ces nouveautés permettent de soutenir l'expansion des réseaux en visant à simplifier la gestion de réseau : gestion des configurations, de la sécurité, de la qualité de service, etc.

Ainsi chez Cisco, le Cisco Intelligence Engine 2100 prend en charge le déploiement des configurations, une phase toujours très délicate pour tout logiciel de gestion de configuration. Les logiciels existants peuvent donc s'appuyer sur ce boîtier au lieu de dialoguer directement avec chaque routeur du réseau.

<http://www.cisco.com/warp/public/779/serupro/operate/csm/nemmsu/ie2100/prodlit/>

Les nouveaux boîtiers VPN de Nokia intègrent une autorité de certification dans le boîtier afin de gérer les certificats des tunnels IPsec. Il n'est donc plus nécessaire de déployer et administrer un serveur pour remplir cette fonction.

<http://www.nokia.com/vpn/management.html>

Il devient ainsi possible d'imaginer que la sécurité du réseau soit assurée à terme par un ensemble de boîtiers distribués, accessibles depuis un butineur après une authentification forte, qui serviront à distribuer la politique de sécurité de l'entreprise dans le réseau, du contrôle d'accès à la gestion des certificats.

Rachats / Fusions / Sociétés

Le recul permet de constater que la crise s'est révélée un terrain fertile pour les rachats et autres fusions. En effet, nombreuses sont les sociétés qui, quand elles n'ont pas fait faillite, ont vu leurs difficultés financières s'aggraver considérablement. Ainsi Cashware, filiale de Thales, a fermé sa filiale CSP5 pour assainir ses finances. Matranet, intégrateur du FW Gauntlet et se battant sur le marché très concurrentiel des appliances et VPN intégrés aux FW, a dû mettre la clé sous la porte de sa filiale aux USA et dit " se recentrer sur la sécurité ".

L'intégrateur Neurocom n'a quant à lui pas réussi à boucler son dernier tour de table et a donc dû se résoudre à mettre en vente sa filiale NetSecureSoftware pour espérer récupérer des fonds. ICS-Sign, le plus discret des tiers certificateurs français a dû se mettre hors circuit. Enfin, Baltimore, affecté par l'absence de décollage du marché des PKI, a mis en œuvre des mesures drastiques de restructuration.

Mais, parallèlement aux annonces des entreprises en difficulté, celles de rachat prolifèrent. EADS-Telecom a ainsi repris les actifs Matranet et compte poursuivre la commercialisation des produits de ce dernier. Thales Secure Solutions ramène dans son panier les sociétés Experlan (Intégration de produits de sécurité), Global Control (Infogérance), ainsi que Neurocom, à l'exception de sa filiale NetSecureSoftware qui doit prendre son indépendance. Devoteam rachète quant à lui XP-Conseil à IB-Group pour renforcer son offre de conseil dans le domaine de la sécurité des systèmes d'information. Depuis l'élimination de Thawte, son principal concurrent, Verisign conforte sa place de leader de la fourniture de certificats. Sa stratégie passe par de nombreuses acquisitions. Dernière en date à tomber dans son giron, la société CyberCash, dont l'offre s'articule principalement autour de logiciels de paiements et de vérification pour les paiements de toute nature, notamment par carte de crédit.

<http://www.bsc.fr/ressources/presentations/efe-pki/mgp00019.html>

Article original :

<http://www.newsbytes.com/news/01/164520.html>

Plus d'info sur la faillite de CyberCash :

<http://www.cybercash.com/>

De son côté, l'opérateur poids lourd des télécommunications d'entreprise Colt a jeté son dévolu sur Apogée Communications et son offre de services et d'intégration en sécurité. Le marché des PKI continue à se structurer, et RSA rachète Securant, qui propose des logiciels de gestion centralisée des authentifications et droits des utilisateurs. (Communiqué de presse de RSA :

<http://www.rsa.com/go/securant/>)

Dans le domaine des firewalls, Sonicwall a racheté Redcreek.

Enfin, ActivCard a récupéré Safe Data Card, ce qui permettra une continuité chez les clients :

<http://www.safedata.com/>

ou

http://www.activcard.com/activ/newsroom/press_releases/070501_us.html

Toutes les sociétés ne cherchent cependant pas des acquéreurs, et nombreux sont les acteurs du marché ayant levé des fonds : Intranode, Netcelo, Solsoft, etc. Notons dans ce contexte le succès d'Openreach, société d'infogérance de tunnels IPsec. Elle a en effet reçu 31 millions de dollars pour assurer son développement dans un secteur où la concurrence entre nouveaux venus et opérateurs historiques se développe (communiqué de presse d'Openreach :

http://www.openreach.com/press/funding_pr.htm).

Noyées dans la masse des innombrables faillites, certaines sociétés bénéficient quand même d'un regain de notoriété lors de leurs tentatives de renaissances, même quand celles-ci échouent. C'est le cas de Radguard, fabricant israélien de boîtiers Ipsec, cité dans un article de NetworkWorldFusion. <http://www.nwfusion.com/news/2001/0418radguard.html>

ADSL

L'ADSL étant désormais largement répandu, les offres sécurité n'ont pas manqué de se développer autour. France Telecom, qui accorde des services d'infogérance de FW avec ses services liaisons louées (Global Intranet, FT Oleane, Equant), intègre désormais des offres d'infogérance de firewalls à ses coffrets ADSL : Oleane Turbo DSL et Wanadoo Netissimo 2. Jusqu'à présent, FT ne fournissait que des filtres simples dans le modem ADSL ; il s'agit désormais d'un service plus complet avec un FW-1 mutualisé chez Oleane et un anti-virus Trendmicro. Cette offre, très tardive sur le marché, devrait cibler les PME-PMI.

<http://www.ununet.fr/actu/article.htm?numero=7868>

SPAM et GSM

L'absence de câble ne met pas les réseaux sans fil GSM à l'abri des inconvénients et dangers des réseaux traditionnels. Ainsi, lors de la convention BlackHat à Amsterdam, Job de Haas, membre d'une société néerlandaise de conseils en sécurité, a fait la démonstration d'un déni de service sur les téléphones Nokia 6210, 3310 et 3330, en envoyant un message SMS mal formé aux téléphones. La marque aurait depuis publié des versions corrigées de son système, mais elles n'ont cependant pu être trouvées sur leur site Internet. Les articles de The Register sur le sujet :

<http://www.theregister.co.uk/content/55/23080.html>

<http://www.theregister.co.uk/content/55/23232.html>

On pourra également consulter la présentation PowerPoint faite à Hal en août 2001 par le même auteur, sur la sécurité SMS et WAP et disponible à l'adresse suivante :

<http://www.itsx.com/bal2001/bal2001-itsx.ppt>

Dans une optique similaire, les messages électronique non sollicités (SPAM) pourraient être interdits dans les réseaux sans fil aux Etats-Unis.

Cela s'appliquerait notamment aux messages SMS.

<http://tbomas.loc.gov/cgi-bin/bdquery/z?d107:br113>:

Il faut en effet garder à l'esprit que le SPAM est une méthode simple de déni de service. À lire également sur le sujet : <http://www.euro.cauce.org/fr/>

De façon plus générale, il apparaît que le développement des accès sans fil à Internet favorise dans de nombreux cas le contournement des politiques de sécurité d'une entreprise. Les méthodes et solutions varient. Voici l'une des possibilités pour ignorer ces systèmes de protection : l'utilisateur décide d'utiliser son téléphone/PDA ou son PDA/ordinateur portable comme système de travail, en étant connecté au Web par un moyen de type GSM auprès d'un opérateur. Il installe sur son PC de bureau un logiciel fourni par son opérateur, soit par un CD-ROM, soit en le téléchargeant sur Internet. Ce logiciel fait dès lors office de passerelle avec le système central de l'opérateur, en utilisant l'accès à Internet disponible à tous dans l'entreprise. De cette façon, l'utilisateur passe outre tous les systèmes de sécurité mis en place par celle-ci pour l'accès à distance (authentification, contrôle d'accès, etc.) et pour l'accès à l'Internet (contrôle d'accès, contrôle de contenu, etc.). Grâce à son accès Internet sans fil auprès du système de son opérateur, il peut accéder à sa messagerie interne à l'entreprise, à son agenda,

et même aux fichiers qui sont sur son PC de bureau. Cet accès sans fil permet d'avoir un système unique, commun à son entreprise et à d'autres accès personnels (messagerie, agenda), accessible en toutes circonstances partout.

Dans un réseau d'entreprise, un tel système constitue une forme de porte dérobée similaire à celles utilisées par les virus et les pirates. Il convient donc de bien apprécier la facilité avec laquelle les gens peuvent " encapsuler " l'ensemble de leurs échanges dans HTTP, et ainsi contourner la sécurité. À la lueur de ces développements, on ne saurait trop recommander aux responsables IT de veiller à conserver la maîtrise de tous les clients dans l'entreprise et d'appliquer un contrôle d'accès et de contenu dans HTTP, avec une mise à jour des requêtes HTTP et leur analyse pour détecter le type de logiciel incriminé. Pour plus de détails, consulter l'article d'Infoworld magazine :

http://idg.net/ic_794599_1794_9-10000.html

Ainsi que les sites de certains fournisseurs de services sans fil :

<http://www.sprintpcs.com/>

<http://www.infowave.com/SProPreview/FaB.htm>

Certificats et PKI

Pour aborder ce vaste domaine, on aura à cœur de revenir sur l'affaire des faux certificats qui, si elle s'estompe des mémoires, reste pourtant symptomatique de certaines lacunes.

Rappel des faits : Verisign (propriétaire de Tawthe France et principal actionnaire de Certplus) a émis deux certificats de signature de code pour Microsoft, certificats qui n'avaient pas été demandés par Microsoft. Les 29 et 30 janvier 2001, un inconnu se faisant passer pour un employé de Microsoft a acheté chez Verisign deux certificats de signature de code de classe 3. Le nom associé à ces certificats est " Microsoft Corporation ". Les certificats de classe 3 sont les plus forts délivrés par Verisign (leur énoncé des pratiques de certification (CPS = Certificate Practice Statement) se trouve sur

http://www.verisign.com/repository/CPS/CPSCH2.HTM#_toc361806951). Une fois en leur possession, l'inconnu peut désormais envoyer du code de toute nature signé avec ses certificats, trompant la grande majorité des utilisateurs qui, croyant ce code réellement supervisé par Microsoft, l'exécuteront sans crainte. Il s'agit donc d'un risque majeur si l'usurpateur utilise effectivement les certificats qu'il a obtenus.

Bien entendu, Verisign a révoqué ces deux certificats. Cependant cette liste de révocation (CRL = Certificate Revocation List) n'est d'aucun secours, car les certificats de signature de code de Verisign n'indiquent aucun moyen de récupérer une liste de révocation (pas de CRL Distribution Point). Microsoft a dès lors suggéré des correctifs de tous ses logiciels depuis 1995 pour intégrer localement, en dur, la liste de révocation de ces deux certificats. En attendant, ils proposent de supprimer le certificat racine de Verisign. L'avis du CERT propose quant à lui de télécharger la CRL sur

<http://crl.verisign.com/Class3SoftwarePublishers.crl> (il faut la sauver sur son disque – l'ouvrir ne sert à rien, cela ne peut pas s'installer en l'ouvrant –, puis click bouton droit dans l'explorateur : installer la CRL).

Malgré cette affaire, le marché des PKI, même s'il n'a pas tenu toutes ses promesses, est loin d'être enterré. De nouveaux acteurs arrivent en effet en France, avec notamment beTRUSTed, tiers de confiance privé de PricewaterhouseCoopers, qui utilise la technologie Entrust, et propose de l'infogérance de PKI, et le suédois Addrush qui propose les mêmes services. La société Cashware, filiale du groupe Thales, prend son envol avec un centre d'opération sur plate-forme Solaris et le support de la plupart des technologies de PKI du marché (Entrust, Baltimore, etc.). À noter que Cashware a également lancé une certification téléTVA pour concurrencer Certplus dans l'infogérance des PKI des établissements délivrant des certificats pour la téléTVA, mais ne concentre pas son activité dans ce domaine. Mais, d'un autre côté, Entrust ferme sa filiale en France, à l'instar d'autres acteurs majeurs de la sécurité, comme F-Secure, et le secteur de Baltimore, qui revend la PKI, est en difficulté, malgré son leadership technologique sur Identrus dans le domaine bancaire.

Le marché offre encore peu de projets de PKI dépassant le stade du prototype : il ne décolle donc pas. Il apparaît donc plus judicieux de se développer sur le service autour de la certification : infogérance, aide en ligne à tous les niveaux, etc., comme le font ou le feront les plates-formes d'intermédiation. Dans ce contexte, les PKI ouvertes, poussées par les pouvoirs publics, représentent encore la grande majorité des projets actuels en France. Un exemple récent : les tribunaux de commerce envisagent de délivrer dans le cadre des frais de création d'entreprise un certificat au créateur.

Pour en savoir plus :

- PWC Betrustrusted : <http://www.betrustrusted.com/>
- Addtrust : <http://www.addtrust.com/>
- Cashware : <http://www.cashware.com/>
- TéléTVA :
<http://www.finances.gouv.fr/DGI/tva/telepro/sommaire.htm>
<http://tva.dgi.minefi.gouv.fr/index.jsp>

La conférence " Mise en œuvre des ICP : retours d'expérience ", organisée par le CLUSIF, a permis à quatre acteurs ayant participé au déploiement d'une infrastructure clé publique (ICP) à différentes étapes clés du projet, de faire part de leur expérience. En premier lieu, Bertrand Sevellec (Integris) a succinctement présenté la part de la composante PKI dans l'architecture Bull eSentry, plate-forme d'accès à des applications depuis un Intranet ou Internet, issue de Bull et utilisée chez Bull dans son exemple. L'architecture eSentry ne requiert qu'une seule et unique authentification, via un serveur WebSSO et l'utilisation de certificats X509. C'est un mécanisme de type Single Sign On (SSO) dans un environnement PKI, présenté au CLUSIF lors de la conférence SSO. L'accent a été placé sur la problématique d'avoir d'une part des applications supportant une ICP, et d'autre part l'infrastructure proprement dite. Une double difficulté qui requiert un investissement important, au sens large. Au-delà des aspects techniques visant à expliciter les interactions entre les différentes entités et applications (sur fond de certificats X.509, de relais HTTP en entrée, d'annuaires LDAP et autres autorités de certification etc.), cette intervention aura rappelé les principes directeurs de la réflexion à mener lors du déploiement d'une telle infrastructure : analyse de l'existant et des besoins, état de l'art des outils disponibles afin d'adopter une démarche réaliste et cohérente, sans oublier la prise en compte des besoins exprimés par les utilisateurs eux-mêmes. Avec une difficulté inattendue : la composante syndicale, intervenant contre la multiplication des mots de passe, et par là même favorable à l'utilisation de supports de stockage type cartes à puce. Ce qui motive la mise en place de ce genre d'infrastructure est essentiellement la nécessaire unification des méthodes d'authentification auprès des applications, ceci en adoptant et conservant la flexibilité requise pour une société aux filiales multiples et à l'organisation mouvante. Quant aux problèmes, les principaux rencontrés se sont avérés directement liés à l'ICP proprement dite, à propos de l'ensemble des procédures à formaliser, par exemple

: quel est l'évènement " déclencheur " d'une demande de certificat, d'un renouvellement... ? Sans oublier le budget ou la planification du projet, qui sont autant de contraintes à considérer. À l'heure actuelle, ce projet réside encore dans une phase embryonnaire. Le seul retour d'expérience concerne donc les difficultés auxquelles les concepteurs de l'architecture ont été confrontés, mais aucun retour concernant l'utilisation effective de cette ICP. Les choix réalisés n'ont donc pu être validés.

Dans un tout autre registre, Dominique Manenc, de la société Certplus, a dressé un panorama du marché des prestataires de services de certification, des rôles que ces derniers pouvaient tenir, ainsi que des pôles économiques susceptibles d'émerger, ventilés suivant les trois grandes catégories suivantes :

- Le pôle Sécurité : pôle concernant principalement la sécurité des échanges, avec notamment la gestion des certificats X.509v3 utilisés lors de sessions SSL/TLS (pour les sites de commerce électronique principalement), ou l'authentification mutuelle lors de la négociation de paramètres de sécurité de tunnel IPSec (dans le cadre de VPN, typiquement).
- Le pôle Signature : pôle constitué des services nécessitant une identification du porteur ainsi qu'un service de non répudiation (à distinguer du mécanisme de " signature " de par sa composante juridique).
- Le pôle Mixte : pôle regroupant les activités comprenant le chiffrement et la signature de courrier électronique, application actuellement la plus en usage.

Au final, il apparaît que la mise en place d'une ICP doit suivre une logique métier, et non une approche purement technologique. Il n'y a pas d'élément probant de retour sur investissement, à moins d'infogérer. Il conviendra de noter que c'est une application comme TéléTVA qui aura sauvé économiquement, à court terme du moins, le marché des fournisseurs de services de confiance. Il ne faut cependant pas négliger les nombreux freins au déploiement d'une telle infrastructure : manque de jurisprudence pour la signature électronique, projets souvent à la croisée des chemins technologique, juridique et marketing, manque de maturité des offres du marché (qu'il s'agisse des produits en termes de compatibilité notamment, ou des acteurs dont l'expérience est essentiellement bâtie autour de projets pilotes).

Malgré tout, les réussites existent, comme le service d'horodatage/estampillage de la Poste, ou l'infrastructure mise en place par le ministère des Finances pour les télépaiements.

La problématique est cependant sensiblement différente de celle à laquelle sont confrontées les entreprises : il ne s'agit pas d'imposer une nouvelle organisation ou de remodeler son système d'information. Reste que les utilisateurs doivent suivre et en faire usage !

Enfin, Jean-Pierre Chabaneix a présenté la mise en place d'un projet pilote d'ICP à la SNCF, en relatant essentiellement son expérience en sa qualité d'utilisateur d'une telle infrastructure. Un usager comblé par l'introduction de systèmes à base de cartes à puce, technologie simplifiant la gestion des mots de passe grâce à une unification des méthodes d'authentification. Une simplification d'autant plus appréciable qu'elle concerne aussi bien l'administrateur que l'utilisateur final.

Le besoin primaire ayant conduit à la mise en place d'une telle infrastructure est simple et correspond à une problématique à laquelle bon nombre d'entreprises sont actuellement confrontées : assurer la confidentialité des données enregistrées sur les postes de travail. Une confidentialité des données à assurer plus particulièrement au niveau des postes nomades, ceci afin de se prémunir contre le vol d'informations par l'introduction de solutions de chiffrement ou d'authentification forte. De plus, des services supplémentaires sont venus se greffer à ceux immédiatement envisagés, ou du moins envisagés à terme, tels que le service de non répudiation, directement associé à un mécanisme de signature électronique. De tels besoins, en considérant la conjoncture actuelle, notamment concernant l'évolution de la législation vis-à-vis de la reconnaissance de la signature électronique, ont mené à l'adoption d'une ICP pour les avantages qu'elle peut présenter. Une telle technologie impose en effet un modèle organisationnel de l'information universel, s'appliquant aussi bien aux hommes qu'aux équipements, qui offre progressivement un véritable panel d'outils et de services.

Un projet pilote d'infrastructure à clé publique a donc été mis en place pour bâtir, à terme, une solution complète et étayée d'un tel système, tout en respectant un certain nombre d'objectifs en terme de performances, d'adaptation à l'environnement technique existant, etc. Les choix technologiques réalisés ont donc été les suivants :

- utilisation du système d'exploitation Windows 2000, nécessitant la migration de l'ensemble du parc informatique (pour la cinquantaine de postes concernés par le projet pilote),

- support amovible de type carte à puce pour les certificats et clés privées,
- extériorisation de la gestion des clés et certificats, via un prestataire de services de certification agréé par le DCSSI.

L'utilisation faite de ce système est tout à fait classique :

- chiffrement des données via EFS,
- session et réseau,
- chiffrement et signature des courriers électroniques via protocole S/MIME.

Ce projet pilote s'est avéré satisfaisant grâce au réalisme consistant à se concentrer sur le déploiement de l'infrastructure en fonction des besoins et surtout des logiciels existants, la procédure inverse (preuve d'un excès d'optimisme et de confiance en cette technologie) conduisant inexorablement à l'échec.

Cette conférence aura permis de rappeler la fragilité économique de l'activité d'infogérance des PKI, l'importance des aides publiques dans leur soutien, ainsi que la difficulté à trouver des applications concrètes et déployées. Pourtant, en décembre 1999, Renault présentait déjà à l'OSSIR sa propre ICP, utilisée avec des applications dédiées par ses revendeurs, et comptant 40 000 utilisateurs authentifiés dans plus de 100 pays, et 200 applets signées. Pourtant, depuis ce premier déploiement en France, les tentatives de présentations d'expérience d'utilisateurs ne trouvent guère que des exemples de projets pilotes.

Filtrage

3COM et Secure Computing ont cette année annoncé un nouveau produit. Celui-ci repose sur l'utilisation dans les cartes Ethernet de 3COM d'un système de filtrage Ethernet intégré qui n'avait jusqu'alors jamais été exploité. Dans le cadre d'un projet financé par la DARPA du département américain de la Défense (DoD), 3COM a étendu ce filtrage à un mini firewall embarqué dans la carte Ethernet, et Secure Computing a présenté à RSA 2001, à San Francisco, un logiciel de gestion du filtrage IP des cartes Ethernet 3COM, permettant de déterminer des règles par PC (ou par utilisateur).

Ces cartes Ethernet supportent 10 règles de filtrage IP sans perte de performances, et en supportent jusqu'à 60. Elles gèrent aussi l'anti-spoofing. À chaque démarrage de l'ordinateur, ce dernier va alors consulter son serveur de contrôle pour mettre à jour sa politique, et ce de manière sécurisée. Un tel produit, indépendant du système d'exploitation, concurrence le filtrage IP que Microsoft a instauré dans Windows XP, mais pourrait proposer une meilleure assurance du contrôle d'accès du PC sur le réseau. Il ne faut cependant pas perdre de vue qu'il suffira à l'utilisateur récalcitrant de changer de carte réseau, et que les ordinateurs portables sont désormais livrés avec des cartes Ethernet 10/100 et Ethernet sans fil (Wi-Fi / IEEE802.11b) en standard qui ne sont pas des 3COM (exemple : Toshiba Tecra). Il convient donc de garder à l'esprit que le contrôle d'accès sur le PC ou dans la carte Ethernet du PC reste complémentaire du contrôle d'accès déployé dans le réseau, qui demeure l'élément fondamental.

- Le communiqué de presse chez 3COM : http://www.3com.com/corpinfo/en_US/pressbox/press_release.jsp?INFO_ID=2002706
- Le communiqué de presse chez Secure Computing : <http://www.securecomputing.com/index.cfm?sKey=318>

Sinistralité informatique

Les assureurs intègrent les risques informatiques dans des polices multirisques. C'est pour cela qu'il qu'il n'est plus possible de les isoler dans les statistiques de sinistres de l'Association française des compagnies d'assurance. Devant l'impossibilité d'avoir des chiffres avec un sens, le CLUSIF n'avait donc pas publié de chiffres depuis 1996. Entre-temps, une enquête sur la sinistralité informatique a été menée par le cabinet CMV Conseil, sous la direction de Pascal Lointier, vice-président du CLUSIF. Celle-ci conclue notamment que, du côté des assureurs, la tendance est d'exclure les virus et les pertes de services essentiels des polices d'assurance. Pourtant, sur l'exemple concret de " Love Letter ", il n'y a eu aucune déclaration de sinistre en France, contre 10 en Allemagne, où il existe beaucoup de polices d'assurance couvrant spécifiquement ce type de risque dans l'informatique. Cela relativise l'importance actuelle du coût des virus pour les assureurs, et montre que la crainte du marché de l'assurance n'est pas encore justifiée.

L'enquête du CLUSIF a été réalisée grâce à cinquante entretiens individuels dans les grands comptes, et auprès de 400 PME de 10 à 1 000 salariés, par téléphone et télécopie. Ce qui frappe est la très faible connectivité des entreprises qui ont répondu : un peu plus de la moitié seulement ont un site Web public et 40 % une messagerie généralisée ! La moitié ont un responsable sécurité identifié. Mon expérience personnelle m'incitait à considérer que la plupart des gens avaient des firewalls et qu'ils étaient généralement mal gérés, mais les chiffres obtenus par le CLUSIF font apparaître qu'un quart des entreprises interrogées déclarent un accès généralisé à l'Internet sans aucun firewall. La conclusion du CLUSIF est que les entreprises craignent plus les risques médiatisés, en décalage avec les risques réels en termes financiers, et que les technologies Internet/Intranet sont peut-être à l'origine d'une fragilité nouvelle. Pour en savoir plus :

<http://www.clusif.asso.fr/>

Le CERT/CC (CERT de l'université Carnegie Mellon, financé par le gouvernement américain) a lui aussi publié ses statistiques 2001. Ces dernières rendent les vers Nimda et Code Red responsables du doublement des incidents déclarés au CERT/CC, les responsables indiquant cependant que les incidents graves ont eux aussi fortement augmentés. La page des statistiques du CERT/CC : http://www.cert.org/stats/cert_stats.html
L'article de ComputerWorld : http://www.computerworld.com/storyba/0,4125,NAV4_7_STO67318,00.html

Espionnage

S'il subsistait encore un doute, le rapport du Parlement européen sur le système d'espionnage Échelon l'a définitivement levé. Il dévoile les dessous de ce système complexe qui a certainement permis aux Etats-Unis de se livrer à un espionnage industriel à grande échelle. Mais ce rapport limite les écoutes d'Échelon à des écoutes satellites. Ce qui contredit d'autres sources non vérifiables faisant état de liens terrestres à la base d'écoutes terrestres, liens situés sur des nœuds de transit de réseaux chez les opérateurs ou très proches des opérateurs installés à Londres, Washington, etc.

- L'article sur le site de *Droit et nouvelles technologies* : http://www.droit-technologie.org/fr/1_2.asp?actu_id=405551740
- Le projet de rapport en PDF : http://www.droit-technologie.org/fr/redirect.asp?type=legislation&legis_id=75&url=legislations/echelon_projet_rapport_final_180501.pdf

Échelon a été dévoilé au grand public, des rumeurs ont fait état de portes dérobées dans le code de Windows et de PGP. C'est maintenant le FBI* qui a reconnu utiliser des vers/cheval de Troie pour récupérer des clés de chiffrement à l'insu des utilisateurs : un programme baptisé " Magic Lantern ". Une technique complémentaire du réseau Échelon puisqu'elle permettrait de récupérer les clés nécessaires au décryptage des données " volées " par celui-ci.

**Restreints à la mort de John Edgar Hoover en 1972, les pouvoirs du FBI ont été notablement augmentés sur décision du secrétaire d'Etat à la justice américain (qui et quand ?).*

Attaques des vers

Une des tendances lourdes de l'année 2001 a été la recrudescence des attaques du code mobile. Sircam, Code Red, Nimda ou encore Goner, pour n'en citer que quelques-uns, sont les vers qui ont pendant quelques temps attirés sur eux les feux de l'actualité.

Sircam est un ver utilisant le logiciel Microsoft Outlook pour envoyer des messages de manière automatique à toutes les personnes présentes dans le carnet d'adresses. Ces mails incluent des fichiers présents sur le disque dur, ce qui signifie l'envoi d'informations des plus anodines aux plus confidentielles. Code Rouge s'introduit quant à lui dans le serveur Web Microsoft IIS et s'active plus tard pour lancer des attaques en déni de service sur d'autres sites.

Mais Nimda est peut-être celui qui a le plus marqué l'année écoulée. En effet, si aucune vulnérabilité nouvelle n'est à la source de ce dernier, l'une de ses originalités réside dans la diversité de ses techniques de propagation entre machines infectées et cibles. En effet, contrairement à un Code Red ou Blue qui concentre ses attaques sur des vulnérabilités propres au serveur Web de Microsoft IIS, Nimda, en se limitant à un mode de transmission de serveur à serveur, accélère considérablement son déploiement en mettant à profit de manière combinée de

nombreuses failles d'IIS, du navigateur Internet Explorer et de Microsoft Outlook, impliquant ainsi les postes des utilisateurs dans l'infection générale. L'auteur de Nimda a opté pour les modes suivants de transmission du ver : de poste client infecté vers le serveur Web IIS, de serveur Web IIS à navigateur Internet Explorer, par courrier électronique, utilisant une faille du logiciel Outlook, par volumes partagés, éventuellement en utilisant une faille de Microsoft Office 2000.

Comme nous allons le voir, les conditions de chaque infection sont loin d'être novatrices, mais cette variété dans les méthodes de propagation garantit la rapidité de la généralisation du ver à tout le réseau. Elle assure aussi la contamination d'une manière ou d'une autre des environnements peu surveillés, rarement à jour, construits essentiellement autour de logiciels de surcroît naturellement vulnérables, et qu'il est enfin difficile de tenir vraiment à jour tant les problèmes sont fréquents.

Les différentes formes d'attaques perpétrées depuis une machine infectée par Nimda ayant été largement décrites dans tous les avis de veille en sécurité des organismes spécialisés, nous ne ferons que rappeler brièvement leurs caractéristiques, à titre d'information. Une machine infectée tentera systématiquement de contaminer une plage d'adresses plus ou moins aléatoire, sans se soucier de la nature de sa cible (client ou serveur, IIS ou autre). Ainsi, le ver peut engendrer malgré tout des situations de déni de service sur des réseaux sans produits vulnérables. Au regard des attaques par déni de service, il est possible de citer l'exemple de Steve Gibson, de Gibson Research Corporation, qui a subi durant le mois de mai une attaque en déni de service réparti¹, par un enfant de 13 ans. On lira ainsi avec profit le compte rendu détaillé rédigé par Steve Gibson sur la façon dont il a découvert, contrôlé et géré cette situation, ainsi que son avis sur la question : <http://grc.com/dos/grcdos.htm>.

¹ Les dénis de service répartis apparaissent également dans deux présentations sur le Web d'HSC : <http://www.bsc.fr/ressources/presentations/sce/06.html> <http://www.bsc.fr/ressources/presentations/dos/mgp00008.html>, cette dernière présentation ne traitant que des dénis de service réseaux.

1. Infection des serveurs basés sur Microsoft IIS ou PWS

Pour s'assurer la prise de contrôle de nombreux serveurs connectés au réseau, Nimda utilise plusieurs failles connues du logiciel IIS, dont les correctifs sont désormais pour la plupart disponibles depuis plusieurs mois maintenant :

- Exécution de commandes par décodage redondant d'une URL mal formée (vulnérabilité connue depuis le 15/05/2001),
- Attaque dite " Web Server Folder Directory Traversal via Unicode in URL ", connue depuis le 10/10/2000.

De plus, Nimda tente d'utiliser les accès dérobés éventuellement laissés par deux vers récents, Code Red et sadmind/IIS. Naturellement, tous les correctifs nécessaires à l'éradication de ces deux failles sont disponibles depuis longtemps. Concrètement, une tentative d'attaque laisse 16 requêtes HTTP sur les journaux du serveur Web. Une fois un serveur infecté, le ver se renomme et se recopie à divers endroits de l'arborescence de stockage, sur les disques locaux, et sur les disques accessibles par partage réseau. Il automatise de plus sa réactivation au redémarrage de la machine. Enfin, il modifie chaque page de contenu Web (.htm, .html, .asp, etc.) et y ajoute une ligne de code Javascript, forçant ainsi le téléchargement de l'exécutable du ver par les navigateurs Web et ouvrant alors la voie au mode d'infection suivant.

2. Infection des postes clients par courrier électronique

Outre les postes clients faisant fonctionner le Microsoft Personal Web Server, sujets aux attaques précédentes, le vecteur de propagation de Nimda le plus " conventionnel " reste le courrier électronique. A l'aide d'un client SMTP autonome permettant la falsification de l'adresse émettrice, une machine infectée envoie le code du ver par e-mail au carnet d'adresses Outlook de l'utilisateur, ainsi qu'à toute adresse électronique trouvée dans les pages Web du cache d'Internet Explorer. Le ver est envoyé sous la forme d'une pièce jointe, généralement un fichier exécutable " readme.exe " dont le type MIME est incorrectement positionné à " audio/x-wav ", et dont une simple prévisualisation (effectuée automatiquement par Internet Explorer) suffira à déclencher l'infection.

3. Infection des postes clients par navigateur Web

Les modifications faites aux pages de contenu Web des serveurs sous IIS entraînent les navigateurs à télécharger et exécuter systématiquement le " readme.eml " offert, une copie de l'exécutable, entraînant le mécanisme de prévisualisation, sans même avoir besoin de double-cliquer, grâce à l'aperçu rapide et l'infection. Ce comportement est conditionné à l'activation de Javascript dans les paramètres du navigateur, ainsi qu'à la vulnérabilité précédente d'Internet Explorer.

4. Infection par partage de volumes sur le réseau

Sur une machine infectée, le ver examine les éventuels volumes accessibles partagés par le protocole NETBIOS sur le réseau local, repère tous les fichiers exécutables et les remplace par sa propre copie. Naturellement, il en profite pour désactiver tout mécanisme de sécurité des partages réseau dans la base de registres de la machine locale, crée un compte " Guest " et lui confie les privilèges d'administration, partage le disque système, etc. Pour découvrir tous les détails sur les circonstances techniques d'une attaque, avoir des statistiques sur la propagation du ver, ainsi que la liste des adresses où vous pourrez trouver les différents correctifs constructeurs pour vos logiciels vulnérables, voyez l'excellente analyse de Nimda par SecurityFocus, à l'adresse

<http://aris.securityfocus.com/alerts/nimda/010919-Analysis-Nimda.pdf>

5. Se protéger de Nimda

L'exploitation des vulnérabilités par Nimda n'avait rien d'innovant ou de particulièrement dévastateur (pas de destruction volontaire de contenu). Les vraies particularités de ce ver demeurent la diversité des moyens d'infection mis en œuvre, la rapidité de sa propagation, et son absence totale de discrétion, comme si le créateur du ver avait voulu montrer la simplicité de mettre à mal une part immense des serveurs Web sur Internet en utilisant des failles connues. En mettant le doigt sur la négligence des administrateurs systèmes et sur l'absence totale de mécanismes élémentaires de sécurité informatique dans les grandes infrastructures, qui affaiblissent leur environnement en privilégiant l'usage de logiciels peu fiables.

Les recommandations suivantes visent à contrer ce type d'attaques :

■ À chaque découverte d'une vulnérabilité dans un produit que vous utilisez, appliquez

immédiatement les correctifs fournis par le constructeur. La diminution du nombre d'attaques d'un ver ne vous garantit pas qu'il ne referra pas surface : il peut être programmé pour agir à nouveau après une période donnée, et des successeurs peuvent apparaître, utilisant les brèches laissées par un ver à succès (tel que Code Red).

■ Privilégiez toujours l'usage de logiciels reconnus pour leur stabilité et leur sécurité. Les vers de cet été, Code Red et Nimda, auront infecté environ 150 000 sites Web, répartis sur 80 000 machines faisant fonctionner IIS. Si vous êtes contraints d'utiliser un logiciel de serveur Web connu pour ses nombreuses lacunes en matière de sécurité, n'hésitez pas à placer un relais inverse devant, avec notamment, l'utilisation du filtrage d'URL.

■ Limitez au maximum la circulation des pièces jointes dans votre système de distribution du courrier électronique, et utilisez un serveur de messagerie moderne, tel Postfix, qui vous permettra de filtrer immédiatement et facilement les messages contaminés dès le risque identifié. Si vous devez utiliser une solution plus conventionnelle d'antivirus, appliquez là encore immédiatement les mises à jour adaptées à votre système.

Les recommandations suivantes doivent permettre de prévenir et, le cas échéant, de lutter efficacement contre ces codes mobiles :

■ Ne pas exposer des systèmes à risque sur son périmètre.

■ Faire une analyse de contenu du trafic sur son périmètre, pour tous les protocoles, typiquement SMTP et HTTP.

■ Ne pas utiliser des systèmes clients exécutant du code automatiquement.

Si cette protection par l'analyse de contenu sur le périmètre reste indispensable, elle restera aussi limitée par la réalité et la technique. La réalité : les logiciels Microsoft autorisent l'exécution automatique de code mobile sans contrôle et cela fait partie de la stratégie de Microsoft. La technique : les logiciels d'analyse de contenu cherchent des signatures et un ver inconnu passera toujours au travers tant que la base de signature n'aura pas été mise à jour.

Du point de vue des experts en sécurité, il apparaît très surprenant que de telles attaques à base de vers ne se soient pas déjà produites en plus grand nombre, et n'aient pas déjà été utilisées pour pénétrer discrètement sur les réseaux privés des entreprises. Une fois une machine du réseau de

l'entreprise cible infectée, l'agresseur a alors tout loisir de l'explorer, d'écouter et de voler les mots de passes, d'utiliser les ressources partagées, etc. À chaque machine piratée, il lui devient de plus en plus facile d'infecter l'ensemble du réseau. Combien de temps alors avant que ses recherches ne mettent à jour des fichiers aussi alléchants que contrat.doc, bilan.xls, marketplan.ppt, etc. ? Le canal le plus ouvert en sortie est généralement la messagerie, parfois l'accès à un serveur WWW, mais dans tous les cas il est facile de renvoyer à l'extérieur les informations obtenues sur le réseau interne.

La protection contre de telles attaques implique un retour à une politique de sécurité globale dans l'entreprise et une protection dans l'entreprise et pas uniquement sur le périmètre :

■ Un contrôle très strict sur le périmètre dans les deux sens : analyse des statistiques des messages en sortie, limitation de la taille des messages, authentification et " journalisation " des accès à l'Internet, analyse de contenu dans le protocole HTTP, etc ; la limitation aux services nécessaires de manière générale, et pas uniquement sur le périmètre. Il faut par exemple éviter d'utiliser DCOM quand cela n'est pas indispensable.

■ Le cloisonnement du réseau : un contrôle d'accès réseau généralisé permettant de limiter les flux au strict nécessaire (un PC ayant besoin d'avoir accès à 10 serveurs ne doit avoir accès qu'à 10 serveurs et pas à 100) ; une " journalisation " des tentatives infructueuses, centralisée à un service sécurité, et une analyse pour détecter la présence d'un code au comportement anormal sur un poste.

■ Un contrôle centralisé dans la mesure du possible des postes clients, de leur configuration, avec un contrôle d'intégrité sur ceux-ci.

En ce domaine comme ailleurs, il n'existe aucune solution parfaite tant il existe d'impératifs et/ou de volontés contradictoires. Cependant, le développement et le déploiement d'une politique globale bien pensée doit permettre de minimiser les risques vis-à-vis de cette prolifération de codes mobiles.

Nimda continue d'infecter des machines, réactivant les envois de courriers électroniques tous les dix jours. Pourtant l'intérêt de la communauté diminue : les journalistes ont beaucoup parlé de l'attaque initiale ; une fois la première vague passée et quelques machines réinstallées, force est de constater que peu d'entreprises remettent en question leur politique de sécurité. Il semble qu'un certain fatalisme vis-à-vis des problèmes de vers Internet se soit installé. Cette attitude est d'autant plus regrettable au vu du caractère nocif de ce type d'attaques, de leur rapidité de diffusion et de leur polymorphisme. Enfin, il est à craindre que ces vers à haute visibilité n'aient été que de simples précurseurs, présageant alors pour les mois à venir de l'apparition de vers aussi efficaces, probablement plus virulents ou destructeurs, et, certainement, aussi ironiques dans leurs vecteurs d'infection.

Normalisation de la sécurité

Domaine en perpétuelle évolution, la sécurité des systèmes et réseaux fait depuis quelques temps déjà l'objet de diverses tentatives de normalisation, pour une bonne part initiées par les pays anglo-saxons. L'un de ces projets, qui connaît déjà une certaine notoriété est celui de la norme anglaise BS7799. Celle-ci est composée de deux parties. La première, BS7799-1, propose des recommandations et a été soumise à l'ISO dans une procédure de " fast track ", pour éviter les commentaires. Elle est passée à une seule voix près, sachant que la Suède n'a voté le " oui " que du bout des lèvres. Quoi qu'il en soit, la conformité à un document de recommandation n'est pas vérifiable. Seule la conformité à la deuxième partie de la norme, soit BS7799-2, l'est vérifiable. Mais cette partie n'a pas été soumise à l'ISO et le BSI britannique indique qu'il n'a pas pour projet de soumettre cette partie à l'ISO. Sans cette deuxième partie, la norme n'est pas vérifiable. Or, au sens normalisé, une norme ISO ne peut exister que si la conformité à celle-ci est vérifiable. En conséquence et jusqu'à nouvel ordre, la BS7799 est une norme ISO bancale. S'il en était besoin, il sera porté à l'attention du lecteur que le Canada a introduit 27 Defect Reports, dont 6 reconnus comme " Technical Major ", ce qui implique que la première partie BS7799-1 devra obligatoirement faire l'objet de révisions conséquentes avant sa publication ISO définitive. Enfin, il faut garder à l'esprit que la BS7799 a été largement conçue par des cabinets de consultants pour des cabinets de consultants, rémunérés pour

valider la conformité d'une entreprise à cette norme. Malheureusement, il est possible d'avoir une sécurité catastrophique et d'être conforme à la BS7799. La réalité est beaucoup plus complexe, et certains acteurs du marché sont perplexes vis-à-vis de ce projet. Malgré un lobbying intensif et continu, ce document britannique n'a aucune reconnaissance légale ou réglementaire en France ou en Europe. Je recommande donc vivement de le considérer avec le recul nécessaire et en tant que document de recommandations et de bonnes pratiques.

L'année 2001 a également vu fleurir les projets de label orientés sécurité, pensés notamment comme un moyen de développer la confiance sur laquelle repose le commerce électronique. L'ACSEL, née de la fusion de l'AFCEE avec l'AFTEL, a ainsi publié un document de neuf recommandations dans ce sens. S'il faut reconnaître un certain mérite à cette idée, la prudence reste de mise. Les outils et techniques actuels ne permettent en effet en aucun cas de garantir un niveau de sécurité d'un site de commerce électronique en rapport avec un label. Ainsi, aucun label reconnu n'a encore vu le jour. Plus de détails sur la question des labels à : <http://www.acsel-net.org/acsel/accueil.htm> Article du *Journal du Net* sur le document : <http://www.journaldunet.com/0106/010621Acsel.shtm>

La Sécurité XML

La norme ebXML est un successeur aux normes actuelles d'EDI. Elle est composée d'une collection de spécifications dans tous les domaines, démultipliant les possibilités d'échanges dématérialisés entre les entreprises par le simple envoi de messages XML sur HTTP ou SMTP sur Internet. La norme est basée sur des composants objets, avec toutes les caractéristiques des objets, y compris avec des répertoires (ou entrepôts) pour découvrir les objets disponibles. Le modèle vient du métamodèle UMM réalisé par UN/CEFACT (Nation Unies). Le standard XMLEDI est construit pour l'intersectorialité, alors que EDIFACT était conçu à chaque fois comme interne à un secteur d'activité.

Le protocole d'échange est SOAP 2.0, la sécurité se limite au chiffrement TLS et à la signature XML, avec des couches de transport HTTP ou SMTP et l'utilisation d'une enveloppe MIME. Ce type de fonctionnalités, actuellement limitées aux logiciels de type SAP, devraient être intégrées dans l'ensemble des logiciels pour PME-PMI dans les années à venir.

On peut ainsi envisager un scénario d'achat entièrement automatique jusqu'au règlement, avec toutes les possibilités d'utilisation de crédit et d'assurance, et ne nécessitant qu'un minimum d'intervention humaine. Il ne faut cependant pas oublier que la dématérialisation des documents commerciaux n'altère en rien les obligations fiscales. Dans cette optique, la signature électronique à toute facture dématérialisée sera rendue obligatoire par une directive européenne dans quelques mois. Pour promouvoir le système, la directive devrait également interdire à une entreprise acceptant des factures dématérialisées de les prendre pour certains clients et de les refuser pour d'autres, à l'intérieur de l'Union européenne. Tout doit être archivé pour respecter les obligations fiscales. Alors que le principe fiscal reposait sur la comparaison des pièces commerciales et comptables chez le client et le fournisseur, la directive va autoriser un archivage unique, sur une plate-forme d'intermédiation, sans que les obligations d'agrément pour celle-ci ne soient encore connues.

Les échanges électroniques par Internet n'en sont qu'à leurs balbutiements. Les notions de vol d'information, par exemple la compréhension des processus d'affaire de son concurrent, de falsification permettant des détournements, et surtout de déni de service, car c'est le plus simple à mettre en œuvre, sont encore inconnues du monde de l'EDI. Pourtant, en migrant sur des technologies XML/SOAP/HTTPS, la sécurité devra être reconnue et prise en compte comme l'élément indispensable au développement des échanges EDI en XML.

IPsec

La conférence IPsec 2001 s'est tenue du 23 au 26 octobre 2001 à Paris et a réuni les principaux acteurs d'IPsec, avec une participation importante des auteurs de drafts et des responsables des groupes de normalisation à l'IETF (92 inscrits au total).

Dès le premier jour, un débat sur les déploiements IPsec et l'avenir a permis de dégager deux opinions divergentes dans ce domaine. Éric Vyncke, de Cisco, a ainsi déclaré qu'IPsec décollait en indiquant qu'il avait connaissance d'un projet majeur toutes les deux semaines. Hervé Schauer a cependant attiré l'attention sur le fait que 25 projets par an n'étaient pas si significatifs, spécialement au regard des 2 500 entreprises et organisations en Europe qui pourraient avoir de tels projets.

Cette conférence a également vu une démonstration d'interopérabilité réalisée par Ghislaine Labouret (Hervé Schauer Consultants). La démonstration regroupait dix périphériques de huit fournisseurs, tous reliés entre eux par 45 tunnels IPsec dans un réseau totalement maillé. Les principaux fournisseurs, comme Nortel, Netscreen et Cisco, étaient présents avec trois IPsec différents : IOS, PIX et VPN3000 ; tout comme les acteurs français : 6Wind, Netasq et Netcelo, et les implémentations libres d'IPsec FreeS/WAN et OpenBSD. Les tunnels fonctionnaient avec l'initiative du tunnel dans les deux sens, soit 90 tests. Tous les tunnels utilisaient IKE et des certificats générés par la PKI IDX-PKI. Moins d'une dizaine de cas n'ont pas fonctionné, même si le paramétrage par défaut a souvent dû être modifié. Ce succès a permis de montrer la maturité technique qu'IPsec avait acquis depuis l'année précédente.

Cependant, certaines des sociétés ayant participé aux précédentes éditions n'étaient pas présentes, certaines pour cause de faillite (Radguard et le revendeur de Redcreek), et des acteurs qui semblaient importants ont refusé de participer, tels que Check Point et Nokia. Les fournisseurs d'infrastructure de clés n'ont quant à eux pas pu réunir les moyens pour participer, à l'exception d'Idealx, avec sa PKI qui est un logiciel libre.

Pour en savoir plus :

- Les transparents de la présentation des démonstrations d'interopérabilité IPsec et IKE sont disponibles sur <http://www.hsc.fr/ipsec/ipsec2001/>
- L'IETF : <http://www.ietf.org/>
- La PKI IDX-PKI d'Idealx disponible en logiciel libre : <http://idx-pki.idealx.org/>

Diverses conférences ont abordé des sujets tels que les nombreux risques apportés par l'utilisation de tunnels IPsec en accès distant par Internet, ou encore l'évolution des travaux sur l'application à IPsec de PCIM (Policy Core Information Model). Le retour d'expérience d'Asdrubal Pichardo de SAP déterminait qu'IPsec est effectivement fonctionnel, mais qu'il affecte la performance et rend difficile la résolution des problèmes réseau, nécessitant des compétences pointues.

Pour terminer la conférence, deux fournisseurs de solutions de sécurité sans fil ont été présentés, Certicom et Bluesocket, ainsi qu'une société de conseil, *@stake*.

Certicom propose des VPN IPsec sur des téléphones mobiles et des PDA. Ron Statler a montré qu'en configurant IKE au plus léger, il était possible d'utiliser IPsec sur de petits périphériques, avec des performances qui restent utilisables pour certaines applications en texte comme la messagerie.

La société Bluesocket propose quant à elle un système de sécurisation des réseaux Ethernet sans fil avec une authentification des utilisateurs dans un butineur. David Crosbie, de Bluesocket, a montré les risques des réseaux 802.11b, en insistant sur le fait que le plus courant d'entre eux est celui de l'utilisateur branchant en toute illégalité une borne sur sa prise Ethernet, sans que les gestionnaires du réseau soient au courant... et sans sécurité. Il a indiqué que l'utilisation du logiciel d'attaque de WEP, disponible sur sourceforge, nécessitait une carte 802.11b Linksys avec une machine Linux. À l'avenir, l'implémentation d'AES avec le système d'authentification de 802.1x permettra de retrouver une sécurité satisfaisante, mais la normalisation de celle-ci n'est pas terminée à l'IEEE. Pour le moment, il a finalement recommandé de considérer les réseaux sans fil comme des réseaux externes qui, outre la sécurité existante des réseaux sans fil, imposent un tunnel IPsec à tous les postes souhaitant se connecter vers un firewall de concentration.

Phil Huggins de *@stake* UK a donné les mêmes suggestions d'architecture que David Crosbie sur Ethernet 802.11b. Il a également traité la sécurité GPRS et a indiqué avoir trouvé sur un système d'écoutes judiciaires un logiciel d'écoute du trafic GTP : *gpdump*. GTP (GPRS Tunnelling Protocol) est le protocole d'"encapsulation" du trafic IP de l'utilisateur dans le réseau IP de l'opérateur entre le SGSN et le GGSN. Plus grave, Phil Huggins a aussi trouvé le logiciel *gpdump* sur des systèmes compromis. En Angleterre ces systèmes d'écoutes judiciaires sont implémentés sur des plates-formes Nokia IPSO. Le logiciel *gpdump* a été développé par un tiers et n'est pas disponible au public. Pour en savoir plus, consulter également la présentation de Stéphane Aubert sur la sécurité GPRS :

<http://www.bsc.fr/ressources/presentations/gprs/>
Ipsec a donc fait preuve d'une certaine maturité, mais ne rencontre pour l'heure qu'un succès encore limité, étant plus souvent utilisé pour construire l'infrastructure réseau des entreprises que pour appliquer une politique de sécurité.

Cybercriminalité

De par leur impact médiatique, les événements du 11 septembre ont été à l'origine de nombreuses initiatives visant à renforcer la lutte contre la cybercriminalité au sens large. Le ministère américain de la Justice a ainsi fait une proposition visant à redéfinir les actes de terrorismes aux Etats-Unis. Dans cette définition, les délits informatiques de piratage de serveur ou de publication de programmes malveillants entrent dans les actes de terrorisme.

Le projet de loi anti-terroriste américain peut être consulté à l'adresse suivante :
http://www.eff.org/Privacy/Surveillance/20010919_at_a_bill.html

Dans cette optique, un article de Duncan Campbell fournit un contrepoint intéressant à l'idée selon laquelle les terroristes utilisent des moyens électroniques très évolués. Il rappelle qu'il suffit à ces terroristes d'utiliser des cybercafés, des comptes hotmail, de simples codes avec des messages en clair pour se fondre dans la masse des échanges électroniques anodins et échapper à la vigilance de la NSA. Cet article peut être consulté à l'adresse ci-dessous : <http://www.guardian.co.uk/waronterror/story/0,1361,558371,00.html>

Cette volonté renforcée de lutte contre la cybercriminalité a trouvé un écho en Europe, et la Convention européenne, par le biais des délégués des ministres du Conseil de l'Europe, a approuvé le projet de convention sur la cybercriminalité. On pourra pour plus de détails consulter l'article de 01net à ce sujet :

<http://www.01net.com/rdn?oid=160278>

En France, le gouvernement a créé l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC), qui semble amené à remplacer la BCRCI et devrait compter à terme trente-cinq personnes.

Dans l'ombre du terrorisme et de la criminalité à grand spectacle, les délits habituels liés aux réseaux perdurent et se développent. Parmi eux, les vers Internet se sont octroyés une place de choix en 2001. Sans revenir sur les faits déjà cités précédemment, évoquons cependant le virus BadTrans, qui recherche les mots de passe de l'utilisateur et les informations sensibles sur son PC pour les renvoyer à des sites, des forums et des adresses électroniques. Les conflits sur les noms de domaines se multiplient également, et ceux qui n'ont pas déposé tous les noms se rapportant à leur marque dans tous les domaines de premier niveau (.com, .biz, .net, .info, .tv, etc.) doivent parfois engager des procédures longues et coûteuses. Les noms de domaines parasités sont aussi parfois utilisés pour des sites Web parodiant le site original. Le cas de l'Organisation mondiale du commerce (www.wto.org, parodié sur www.gatt.org) a ainsi permis à de faux représentants de l'OMC d'être invités à une conférence dont les responsables s'étaient adressés au site www.gatt.org par erreur. Bien sûr, Internet reste également le moyen idéal de propagation des rumeurs les plus diverses, avec parfois des conséquences importantes sur le cours de Bourse d'une entreprise, par exemple. Parallèlement, des affaires de faux sites d'investissement ont porté sur des montants supérieurs à un million de dollars détournés.

L'affaire de la " Yescard " a également défrayé la chronique. Un logiciel permettant de fabriquer une carte bancaire qui dit " oui " (" Yescard ") est en effet librement disponible sur Internet. Il permet de fabriquer des cartes bancaires utilisables dans certains type d'automates de paiement, notamment ceux de la RATP, les cabines téléphoniques France Télécom, les parkings, etc. En effet, pour des transactions portant sur des petits montants, sur certains automates comme les distributeurs de carburant ou de cassette vidéo, l'authentification du porteur est faite en local. Les " Yescard " répondent toujours affirmativement à l'authentification et permettent de payer aux frais du commerçant ou du propriétaire de la carte de même numéro, en cas de collision. La " Yescard " utilise la faiblesse conceptuelle des cartes à puce, qui a fini par être connue malgré les efforts du GIE carte bancaire pour garder le secret. LCI a d'ailleurs fait une démonstration télévisuelle de l'utilisation réussie d'une fausse carte :

http://parodie.com/monetique/brevelci_demo_20072001.htm

De nombreux liens sont disponibles pour qui souhaite explorer plus avant les tenants et les aboutissants de l'affaire.

■ 22/04/01 : Publication du programme, par exemple ici dans fr.misc.cryptologie :

<http://groups.google.com/groups?hl=fr&lr=&safe=off&ic=1&tb=840862e9d4b945ee.1>

■ 23/04/2001 La source d'un programme de " Yescard " circule sur Internet !

http://parodie.com/monetique/breveyescard_23042001.htm

■ 10/06/2001 La " Yescard " expérimentée : ça marche !

http://parodie.com/monetique/edito_10062001.htm

■ 18/07/2001 : Une machine à fabriquer les cartes bancaires

<http://www.mmedium.com/cgi-bin/nouvelles.cgi?id=5662>

■ Article de *Multimedium* (dépêche AFP) reproduit ci-dessous, qui cite *le Monde du Renseignement*.

Apparemment, il n'existe cependant pas de programme similaire pour fabriquer des cartes d'autres types, comme celle des téléphones portables.

Dans une veine similaire, des chercheurs de l'université de Cambridge ont " cassé " le processeur cryptographique DES IBM 4758, le plus répandu sur la planète, utilisé notamment dans les distributeurs de billets. Ils ont envoyé l'information à IBM il y a plus d'un an, mais aucune correction n'a été effectuée par IBM. Le risque est le vol des numéros de carte bancaire et des codes PIN par des malfaiteurs.

Un article sur le sujet :

http://news.bbc.co.uk/1/1/english/sci/tech/newsid_1645000/1645552.stm

Le site Web des chercheurs, avec explications détaillées et FAQ :

<http://www.cl.cam.ac.uk/~rnc1/descrack/>

En France, la possession d'un équipement de décryptage des contenus numériques est interdite depuis bientôt 15 ans, pour protéger les télévisions à péage et lutter contre les décodeurs Canal + pirates. La question de la protection de ces contenus est récemment revenue sur le devant de la scène grâce à un informaticien russe ayant publié la méthode permettant de déjouer le système de protection d'eBooks d'Adobe. Il a été arrêté aux Etats-Unis et attend son procès. Les enjeux économiques croissants de la maîtrise des contenus numériques ont provoqué une débauche de moyens et de législations coercitives.

Face à la médiatisation et aux rumeurs, il convient de travailler à la gestion de son information. Face aux vers et virus, l'antivirus demeure incontournable, et les technologies propices à ces infections sont à éviter. Face à la " Yescard " et aux attaques des contenus numériques, le débat revient inlassablement sur l'obscurité : une sécurité basée sur le secret de sa conception n'est pas pérenne. Une bonne sécurité est celle dont la conception et les algorithmes peuvent être publiés sans affecter le niveau de sécurité du système final.

Les orientations actuelles des législations poussent la sécurité par l'obscurité, par exemple le DMCA aux Etats-Unis. Le lobby des éditeurs de contenus est à la source des législations. La conséquence est que, pour lutter contre les usages frauduleux, les législations en sont venues à interdire aux professionnels de la sécurité de travailler.