

# LA SECURITE INFORMATIQUE : UNE EXPLOSION ANNONCEE

■ ***Le marché de la sécurité informatique est en croissance. Au niveau mondial, il est prévu une croissance régulière des logiciels en sécurité de 30% par an, \$3 milliards en 98, \$4 en 99 et \$5 en 2000 (IDC).***

■ Les firewalls sont là pour durer mais leur part totale régresse de par leur intégration dans le réseau, les logiciels autour du chiffrement et les anti-virus demeurent les logiciels majeurs, mais la plus forte croissance revient aux logiciels de gestion et d'administration.

■ Nous proposons en introduction au guide security 2001 un regard plus global de l'actualité de la sécurité, qui ne se limite pas à l'actualité des sociétés et des produits, mais aussi à l'actualité des technologies, des attaques et des évolutions structurelles comme le déplacement d'une partie du business, du logiciel vers le service. 2000 est l'année de confirmation de l'explosion de l'infogérance en sécurité, un marché qui atteindra \$2,3 milliards en 2003 (Frost & Sullivan). C'est aussi l'année de naissance d'IPv6, qui a été choisi pour les mobiles de 3e génération, et l'année de l'explosion des réseaux sans fil avec IEEE 802.11b. Cela génère de nouveaux problèmes de sécurité.

■ L'actualité est complétée par un article de recommandations pour choisir son système de sécurité internet et d'un lexique.

Nous vous souhaitons à tous un bon salon  
Infosec 2001.

Hervé SCHAUER  
*Hervé Schauer Consultants*

# INTRODUCTION

■ ***HSC est un cabinet de consultants offrant une large gamme de prestations à dominante technique dans le domaine de la sécurité informatique.***

■ Si elles exigent le maintien d'une excellence technique/technologique, la diversité et le nombre de nos interventions nous permettent aussi de rester en phase avec les évolutions d'un marché très dynamique. Cabinet indépendant, HSC bénéficie cependant de relations suivies avec de nombreux éditeurs (Bull, Checkpoint, Cisco, Netasq, Nortel et Solsoft.), notamment par le biais des programmes partenaires. Comme tout exercice de ce style, notre choix des événements marquants de l'année ne prétend ni à l'exhaustivité, ni à la neutralité absolue.

■ Nous sommes cependant convaincus que les sujets retenus offriront au lecteur un panorama réaliste et intéressant d'une année riche en changements, et lui permettront de mieux appréhender les évolutions à venir.

# L'ACTUALITE DU MARCHE DE LA SECURITE

## Les faits marquants d'Avril 2000 à Mars 2001 :

### IPv6

■ Le premier fait marquant de l'année 2000-2001 est le démarrage d'IPv6. La phase de migration sera très longue, 10 ans selon les spécialistes, mais IPv6 est né.

La raison principale est l'avènement d'IP sur les mobiles. A Toronto fin Juillet, le MWIF (Mobile Wireless Internet Forum, <http://www.mwif.org>) a en effet officiellement entériné(1) la décision prise conjointement par Osaka et Toronto d'adopter IPv6 pour 3GPP, à savoir l'intégration de TCP/IP sur les mobiles dits de 3ième génération (UMTS). Un document détaillant cette prise de position est disponible à l'adresse suivante :  
[http://www.mwif.org/mtr\\_001.doc](http://www.mwif.org/mtr_001.doc)  
[http://www.mwif.org/press\\_release.html](http://www.mwif.org/press_release.html)

■ Pour beaucoup, ce choix rend inéluctable la migration de l'Internet vers IPv6. Nous allons citer ci-après plusieurs arguments qui étayent cette hypothèse. Tout d'abord, l'Internet sans-fil et les assistants personnels ne sont pas "un nouveau moyen d'accès à l'Internet". Même si actuellement ils ne concernent que des personnes qui utilisent Internet avant-tout sur un écran 1280x1024 au bureau ou à leur domicile, ils le seront cependant à moyen terme, le moyen d'accès à l'Internet du tout un chacun.

■ La fusion de l'Internet sans-fil et de l'assistant personnel ou téléphone constituera sans aucun doute LE standard d'accès à l'Internet. L'utilisation d'un PC pour accéder à Internet, et d'un réseau filaire au bureau ou du câble/ADSL à la maison ne concernera pendant encore longtemps que le quart de la population, alors que le téléphone/PDA approchera les 100 % comme le téléphone filaire ou la télévision aujourd'hui. On ne prend guère de risque en affirmant que ces futurs appareils intégreront très vite l'accès à l'Internet en standard. Pour s'en convaincre, les exemples ne manquent pas :

■ Dans les pays scandinaves, le taux de pénétration de la téléphonie mobile est de 80 % et continue à augmenter.

■ Au Japon, l'offre d'accès à Internet de NTT Docomo, basé sur les téléphones mobiles, a engrangé 5 Millions d'utilisateurs en 12 mois, là où il avait fallu 6 ans à l'accès Internet par PC pour acquérir la même base d'utilisateurs. Parallèlement, même si certaines entreprises ont pu réaliser des profits dans le domaine des butineurs (phone.com avec son système propriétaire WAP), l'avènement de 3GPP rend difficile d'imaginer un coût pour ce type de logiciels, qui seront très probablement intégrés en standard.

■ Un autre aspect à prendre en compte est bien sûr la facilité d'accès des téléphones et PDA au regard des PC, qui contraignent encore trop souvent l'utilisateur final à paramétrer des adresses IP voire à configurer des serveurs DHCP. Un autre facteur, et non des moindres, est l'explosion du marché asiatique. Une zone qui souffre cruellement de la pénurie d'adresses IPv4, ces dernières étant de fait monopolisées par les américains pour leurs propres besoins. L'Asie est donc friande d'adresses IPv6 et il suffit de consulter les registres de l'ICANN (2) pour mesurer l'ampleur de la demande : l'Asie totalise plus de 94000 inscriptions (dont un tiers pour la Chine) contre 28000 pour le continent américain, et 36000 pour l'Europe.  
[http://members.icann.org/pubstats\\_unverified.html](http://members.icann.org/pubstats_unverified.html)

■ Au final les sites de commerce électronique qui voudront tirer parti de la manne conjuguée des utilisateurs de portable et du marché asiatique ne pourront donc le faire qu'en supportant IPv6. Par ailleurs, La Commission Européenne a publié le 13 Mars 2001 sa volonté de pousser au déploiement d'IPv6, dans une communication à destination du Conseil de l'Europe et du Parlement Européen. - Enfin, sur le plan technique et à l'exception des aspects mobilité qui font encore l'objet de nombreuses interrogations, les briques manquantes telles que le DNS IPv6 ou encore DHCPv6 devraient être achevées cette année. - Rien ne semble donc devoir s'opposer à la future suprématie d'IPv6, et tous peuvent d'ores et déjà se préparer au cortège de modifications qui accompagneront ce nouveau standard de l'Internet,

même s'il mettra plus de 5 ans à s'imposer à IPv4.  
- Sur le seul plan de la sécurité, les conséquences seront nombreuses : la présence d'IPsec en standard dans toute pile IP bien sûr, mais aussi un filtrage IP plus complexe qu'en IPv4, ou encore des dénis de services visant les passerelles de migration. L'avènement d'IPv6 sera riche en débats de fond, dont celui entre le tunnel IPsec de bout-en-bout (peer to peer), et le tunnel IPsec via des passerelles de sécurité proposant du contrôle d'accès. IPv6 apporte IPsec mais ce n'est pas une panacée, il apporte aussi son lot de problèmes nouveaux, et notamment dans les mécanismes de migrations IPv4 vers IPv6.

## L'évolution du marché de la sécurité du logiciel vers le service

■ Dans un article en date du 24 juillet, le journal RedHerring, spécialisé dans le domaine mouvant des start-up, fait état d'une évolution du marché de la sécurité, traditionnellement axée autour d'une offre logicielle, vers une offre dont les services constituent le coeur. Un des exemples les plus médiatiques est peut-être Counterpane. Fondée par Bruce Schneier, cette entreprise n'a pas connu le succès retentissant promis aux millions du capital risque, mais son offre connaît cependant un succès certain auprès de nombreuses dot-com

## Le marché du firewall

■ La sécurité est un environnement hautement concurrentiel, et le marché des firewalls ne fait certes pas exception à la règle. Dans cette optique il y a longtemps que les études de marché constituent des armes de prédilection pour un éditeur soucieux d'affirmer sa suprématie sur ses concurrents. Malheureusement, l'énormité des enjeux nuit trop souvent à l'objectivité et à la sérénité des sociétés chargées de réaliser ces études. La confrontation de Cisco et Check Point constitue un exemple récent de cet état de fait.

Ainsi les partenaires Checkpoint ont reçu dans un bulletin mensuel de Checkpoint un article expliquant qu'une étude indépendante par Dataquest/Gartner plaçait Checkpoint en position de leader des VPN IPsec. Ce bulletin faisait écho à la diffusion le mois précédent d'un communiqué de presse de Check Point sur le même sujet.

Le lendemain les partenaires Cisco, qui sont souvent aussi partenaires Checkpoint, recevaient un message dénonçant l'étude de Dataquest.

- Si l'étude Dataquest faisait à mon avis preuve d'une certaine partialité, elle n'est malheureusement que représentative de nombreuses autres études,

réalisées par d'autres sociétés présentes sur ce marché florissant. Pour les raisons citées plus haut, la prudence est donc de mise lors de la lecture de ces études, particulièrement dans le cadre de choix stratégiques en sécurité.

Au-delà de cette guerre d'annonces et de contre annonces, on remarquera que Check Point a délivré l'agrément OPSEC d'Arrowpoint juste après que cette société soit acquise par Cisco.

L'offre d'ArrowPoint concerne la commutation applicative à haut-débit, sur des URLs ou des cookies.

■ Cette escarmouche est à analyser dans le cadre du changement de stratégie de Check Point. Checkpoint a en effet décidé de ne revendre FW-1 que sur des systèmes d'exploitation standards tels que Windows 2000, Linux et FreeBSD, et a stoppé l'intégration de son module de filtrage IP dans les routeurs, commutateurs, modems, et boîtiers spécialisés. Ce changement de politique vient essentiellement d'un conflit de canaux de distribution : un FW-1 acheté via Nokia ne comptait pas dans les ventes de FW-1. S'il est désormais impossible d'acquérir FW-1 via le fournisseur de la plateforme, il faudra toujours l'acquérir auprès de Checkpoint. Certains distributeurs ont utilisé cela pour gonfler leur ventes d'un cotéen disant j'ai vendu des Nokia et de l'autre j'ai vendu des Checkpoint. Avec le nouveau système cela n'est plus possible. Checkpoint et Nokia ont signé leur accord pour 2 ans de Novembre 2000 à Novembre 2002.

Checkpoint semble aussi renoncer à baser sa stratégie sur la fourniture du logiciel de gestion de la sécurité aux fournisseurs de services, après avoir distribué à bas prix son module de filtrage dans tous les équipements. Il ouvre ce marché aux fournisseurs indépendants de logiciels de gestion de la sécurité comme Solsoft et aux leaders tels que Cisco. Checkpoint contraint ainsi tous les fabricants de boîtiers à faire des boîtiers PC à base de FreeBSD et Linux, afin de pouvoir poursuivre le support de FW-1 & VPN-1.

■ Mais cette évolution facilite aussi pour ces fabricants la migration vers un Unix Natif : le coûteux duo FW-1/VPN-1 étant alors remplacé par le performant et gratuit couple Netfilter/FreeSwan, associé à une interface de configuration. Ainsi Nortel Networks (ex-Bay) a déjà remplacé dans ses routeurs le module de filtrage IP de Checkpoint au profit d'un module "maison". Alcatel (ex-Xylan) n'est pas en reste puisque sa prochaine génération de commutateurs disposera elle aussi d'un filtrage développé en interne. Alcatel propose en parallèle à ses nouveaux commutateurs ses boîtiers de chiffrement IPsec issus du rachat de Newbridge qui avait racheté Timestep, qui planifient d'intégrer un filtrage IP complet (issu de ex-Internet Devices). La stratégie Linux d'Alcatel s'illustre également avec les nouveaux PABX d'entreprise Alcatel 4400, avec voix

sur IP & FW intégré, qui sont également des PCs sous Linux.

Dans ce contexte, une des sociétés dont l'avenir est plus complexe à déterminer est Evidian, l'ancien Bullsoft. Malgré un apparent renouveau, cette société de logiciels qui développe notamment Netwall, Access Master, et PortalXpert doit faire face à une concurrence féroce par Cisco et Checkpoint, et l'arrivée de Microsoft sur le marché ne va pas améliorer les choses.

■ Depuis Septembre dernier Microsoft proposait en effet en version beta son firewall Microsoft ISA, en téléchargement. Il s'agit d'un Microsoft proxy server étendu, avec un filtre IP et une interface graphique qui n'a pas impressionné les professionnels de la sécurité. Ce firewall est un logiciel qui fonctionne sous Windows 2000. L'entrée de Microsoft sur le marché des firewalls était prévue, mais risque de surcroît de ne pas passer inaperçue, particulièrement sur les marchés captifs de Microsoft et des PME-PMI. Par ailleurs, Microsoft n'hésite pas à mettre en avant le filtrage de session dont serait capable ISA, un argument au cœur du discours marketing de Check Point, qui semble donc être dans la ligne de mire de la firme de Redmond. Il faut cependant garder à l'esprit que l'évolution vers les firewalls en boîtiers simples à administrer et sécurisés reste la plus pertinente. Les firewalls sur Windows 2000 sont en effet un anachronisme vu le coût d'exploitation. La meilleure plateforme pour un produit de sécurité ne pouvant se contenter d'un boîtier reste Unix, sachant que les boîtiers eux-mêmes sont également des PCs sous Unix. Dans une grande entreprise au sein de laquelle des unités distantes pourraient être tentées par un produit Microsoft, un boîtier gérable de manière centralisée ou en infogérance serait ainsi préférable. Outre les arguments ci-dessus, il est bon de se pencher sur la nature exacte de la société ISCA, citée par Microsoft comme ayant délivré son label à ISA. Cette société n'effectue en effet aucune évaluation de la sécurité des produits, leurs tests qui n'ont à ma connaissance rejeté aucun produit permettant de justifier la délivrance du label sont surtout payants. Il faut donc retenir que le logiciel Microsoft ISA n'a donc pas encore fait l'objet d'une évaluation vis-à-vis des Critères Communs, des critères ITSEC ou d'autres avec une cible d'évaluation d'un niveau de sécurité correct.

## Attaques sur les téléphones mobiles

■ En attendant l'arrivée d'attaques plus évoluées et dangereuses, le SPAM a d'ores et déjà fait son entrée sur les mobiles. Ainsi, de nombreux utilisateurs de l'opérateur de téléphonie mobile Orange, filiale de France Telecom, ont reçu un message publicitaire dans leur boîte vocale. Orange offre en effet un service permettant d'enregistrer un message, puis de le renvoyer vers d'autres boîtes vocales. Ce

service aurait donc été utilisé pour ce SPAM. La méthode pour obtenir les numéros de téléphone n'avait pas été établie, mais pourrait être due à une erreur de conception du système.

Cet incident a fait l'objet d'un article consultable à l'adresse suivante :

<http://www.theregister.co.uk/content/5/12655.html>

■ Cet article est à mettre en perspective avec la reconnaissance par le WAP forum d'une erreur de conception et simultanément, l'annonce de sa correction. Cette faille de sécurité se situerait entre le WTLS et le TLS au niveau de la gateway WAP, donc chez l'opérateur. Si cette information revêt un caractère quelque peu anecdotique, il est néanmoins une première indication du comportement du WAP forum en matière de communication sur d'éventuelles vulnérabilités et défauts...

La sécurité sur les mobiles n'en est encore qu'à ses balbutiements, cet état de fait pouvant en partie être imputé à la course en avant technologique qui anime ce secteur, avec des implémentations GPRS non encore finalisées et d'ores et déjà des annonces de contrats, de projets et de services UMTS.

## Les fournisseurs de services & produits en sécurité épinglés

■ Kitetoo (<http://www.kitetoo.com/>)

a épinglé durant l'année plusieurs fournisseurs de services et produits en sécurité, qui avaient laissé des serveurs WWW accessibles à tous.

Ainsi même Bull a été victime d'un piratage d'un de ses serveurs WWW (1) :

[www.dominio1.bull.fr](http://www.dominio1.bull.fr); situé à Louveciennes.

Le serveur Web sous WNT et Lotus Domino laissait en effet l'accès libre à l'arborescence de la machine, sur laquelle se trouvait une liste de clients et prospects, avec les noms et coordonnées des responsables, la liste de leurs équipements dans chaque département, etc. Ce serveur visiblement Intranet était donc également accessible depuis Internet.

[http://www.kitetoo.com/Pages/Textes/Les\\_Dossiers/Admins/Ze-mega-Kite-Teuf/bull.htm](http://www.kitetoo.com/Pages/Textes/Les_Dossiers/Admins/Ze-mega-Kite-Teuf/bull.htm)

■ Mais Bull est loin d'être le seul à connaître de pareilles mésaventures.

Des serveurs appartenant à KPMG, Arthur Andersen, PriceWaterhouse Coopers ou encore Ernst & Young (2) ont eux aussi vu leurs faiblesses et autres erreurs de configuration révélées au grand jour.

La notoriété, c'est bien connu, a toutes sortes de corollaires, dont certains moins plaisants et plus dangereux qu'on le souhaiterait. Les mésaventures de ces grands noms ont au moins valeur d'exemples. En sécurité, il est difficile mais pas impossible de faire mentir l'adage du cordonnier mal chaussé...

[http://www.kitetoo.com/Pages/Textes/Les\\_Dossiers/Admins/big-five.htm](http://www.kitetoo.com/Pages/Textes/Les_Dossiers/Admins/big-five.htm)

<http://www.zdnet.fr/actu/tech/a0016153.html>

## Canulars

■ La première arme de la guerre économique, c'est l'information. Si le piratage d'un site Web est rarement sans effet sur l'entreprise, force est de reconnaître que des attaques plus subtiles peuvent elles avoir des conséquences dramatiques. Faux communiqués de presse, études de marché commanditées, rumeurs dans les newsgroups...Autant d'outils pouvant être utilisés dans le cadre d'une campagne de déstabilisation. Ainsi Alcatel, qui au cours de l'année 1998, doit à ce type d'attaques d'avoir vu sa capitalisation baisser de 160 à 100 milliards de francs.

■ Il suffit d'ailleurs parfois d'un acte individuel, comme dans le cas d'Emulex, pour faire trébucher sérieusement le cours d'une société. Dans ce cas précis, le FBI a arrêté un étudiant de 23 ans soupçonné d'être à l'origine du faux communiqué de presse responsable, et d'avoir ainsi engrangé près de \$ 250 000.

■ Dans son édition du 15 Octobre 2000, la revue CRYPTO-GRAM, traite d'ailleurs dans son éditorial du même évènement. L'article de Bruce Schneier est intitulé "Semantic Attacks: The Third Wave of Network Attacks". Je recommande chaudement sa lecture, qui permet d'appréhender les attaques à venir et d'y sensibiliser efficacement sa hiérarchie et ses clients. Une partie de l'article traite d'ailleurs de la falsification du passé.

Dans le domaine de la sécurité, il existe d'ailleurs des exemples connus de ce type de phénomènes, certaines figures de la sécurité ayant fait circuler des CV qui présentent une lecture surprenant de l'histoire de ce domaine.

Il apparaît très clairement que la datation devra être pleinement intégrée dans les futurs standards de signature électronique pour couper court à bon nombre de détournements et falsification.

Quant à ces "attaques sémantiques", leur développement ne fait hélas guère de doutes, et s'y préparer nécessite le développement d'une "culture de gestion de crise", actuellement bien plus présente dans les pays anglo-saxons qu'en France.

## Le piratage de sites web par des groupuscules politiques

■ Il n'a pas fallu attendre longtemps pour que les factions et groupuscules de tout ordre utilisent l'Internet, souvent par le biais de piratages de sites Web. Un exemple significatif est la série de piratages effectuée par GForce Pakistan, qui a ainsi imposé son message politique sur 66 sites webs entre le 30 Juin et le 18 Aout, soit plus d'un site par jour.

■ Les copies des sites pirates sont sur attrition,

par exemple pour [www.reservelabs.com](http://www.reservelabs.com) du 18/8/2000 :

<http://www.attrition.org/mirror/attrition/2000/08/18/www.reservelabs.com/>

■ La neutralité (politique/idéologique) d'un site ne constitue en rien une garantie de sécurité vis-à-vis de ce type d'attaques, la liste des sites web ci-dessous montrant que les critères des attaquants sont pour le moins fluctuants, s'ils existent.

■ 2073	Fri 30 Jun	cult hero	(0.6K)
[defaced]	<a href="http://www.cddbcu.gob.mx">www.cddbcu.gob.mx</a>	by GForce Pakistan	
■ 2144	Tue 4 Jul	Munge	(0.8K)
[defaced]	<a href="http://www.setindia.com">www.setindia.com</a>	by GForce Pakistan	
■ 2173	Wed 5 Jul	Munge	(0.6K)
[defaced]	<a href="http://www.networksetc.net">www.networksetc.net</a>	by GForce Pakistan	
■ 2174	Wed 5 Jul	Munge	(0.6K)
[defaced]	<a href="http://www.mckenzieonline.com">www.mckenzieonline.com</a>	by GForce Pakistan	
■ 2215	Fri 7 Jul	/dev/null	(0.6K)
[defaced]	<a href="http://agmoz.com">agmoz.com</a>	by GForce Pakistan	
■ 2219	Fri 7 Jul	/dev/null	(0.7K)
[defaced]	<a href="http://www.bittown.com">www.bittown.com</a>	by GForce Pakistan	
■ 2258	Sun 9 Jul	/dev/null	(0.6K)
[defaced]	<a href="http://www.isical.ac.in">www.isical.ac.in</a>	by GForce Pakistan	
■ 2284	Mon 10 Jul	McIntyre	(0.7K)
[defaced]	<a href="http://cmstst1.fnal.gov">cmstst1.fnal.gov</a>	by GForce Pakistan	
■ 2321	Thu 13 Jul	/dev/null	(0.6K)
[defaced]	<a href="http://www.indiantips.com">www.indiantips.com</a>	by GForce Pakistan	
■ 2326	Thu 13 Jul	/dev/null	(0.6K)
[defaced]	<a href="http://www.interdata.net">www.interdata.net</a>	by GForce Pakistan	
■ 2337	Fri 14 Jul	Munge	(0.7K)
[defaced]	<a href="http://hpcs.fsl.noaa.gov">hpcs.fsl.noaa.gov</a>	by GForce Pakistan	
■ 2339	Fri 14 Jul	Munge	(0.6K)
[defaced]	<a href="http://hobbes.fsl.noaa.gov">hobbes.fsl.noaa.gov</a>	by GForce Pakistan	
■ 2340	Fri 14 Jul	Munge	(0.6K)
[defaced]	<a href="http://calvin.fsl.noaa.gov">calvin.fsl.noaa.gov</a>	by GForce Pakistan	
■ 2341	Fri 14 Jul	/dev/null	(0.7K)
[defaced]	<a href="http://isdevlab.nrel.gov">isdevlab.nrel.gov</a>	by GForce Pakistan	
■ 2345	Sat 15 Jul	Munge	(0.6K)
[defaced]	<a href="http://pluto.rayder.net">pluto.rayder.net</a>	by GForce Pakistan	
■ 2357	Sun 16 Jul	Munge	(0.6K)
[defaced]	<a href="http://geezer.fsl.noaa.gov">geezer.fsl.noaa.gov</a>	by GForce Pakistan	
■ 2358	Sun 16 Jul	/dev/null	(0.7K)
[defaced]	<a href="http://pinkie.fsl.noaa.gov">pinkie.fsl.noaa.gov</a>	by GForce Pakistan	

■ 2359	Sun 16 Jul /dev/null	(0.7K)	■ 2690	Sun 13 Aug security curmud	(0.7K)
[defaced]	<a href="#">acweb.fsl.noaa.gov</a>		[defaced]	<a href="#">www.legalmontecarlo.co.uk</a>	
	by GForce Pakistan			by GForce Pakistan	
■ 2360	Sun 16 Jul /dev/null	(0.7K)	■ 2694	Sun 13 Aug Munge	(0.6K)
[defaced]	<a href="#">laps.fsl.noaa.gov</a>		[defaced]	<a href="#">www.balasainet.com</a>	
	by GForce Pakistan			by GForce Pakistan	
■ 2361	Sun 16 Jul /dev/null	(0.7K)	■ 2695	Sun 13 Aug /dev/null	(0.6K)
[defaced]	<a href="#">precip.fsl.noaa.gov</a>		[defaced]	<a href="#">cpri.bp.nic.in</a>	
	by GForce Pakistan			by GForce Pakistan	
■ 2362	Sun 16 Jul /dev/null	(0.7K)	■ 2696	Sun 13 Aug Munge	(0.6K)
[defaced]	<a href="#">wrf.fsl.noaa.gov</a>		[defaced]	<a href="#">www.itbids.com</a>	
	by GForce Pakistan			by GForce Pakistan	
■ 2363	Sun 16 Jul /dev/null	(0.9K)	■ 2697	Sun 13 Aug /dev/null	(0.6K)
[defaced]	<a href="#">d3d.fsl.noaa.gov</a>		[defaced]	<a href="#">www.saifindia.com</a>	
	by GForce Pakistan			by GForce Pakistan	
■ 2364	Sun 16 Jul /dev/null	(0.7K)	■ 2698	Sun 13 Aug /dev/null	(0.6K)
[defaced]	<a href="#">rocpage.fsl.noaa.gov</a>		[defaced]	<a href="#">www.xisource.com</a>	
	by GForce Pakistan			by GForce Pakistan	
■ 2395	Thu 20 Jul /dev/null	(0.6K)	■ 2699	Sun 13 Aug Munge	(0.6K)
[defaced]	<a href="#">qzwbre.africaonline.co.zw</a>		[defaced]	<a href="#">bcmsu.guj.nic.in</a>	
	by GForce Pakistan			by GForce Pakistan	
■ 2454	Mon 24 Jul /dev/null	(0.7K)	■ 2710	Mon 14 Aug /dev/null	(0.6K)
[defaced]	<a href="#">icehockey.wes.army.mil</a>		[defaced]	<a href="#">www.2ndchanceindia.com</a>	
	by GForce Pakistan			by GForce Pakistan	
■ 2456	Mon 24 Jul /dev/null	(0.7K)	■ 2713	Mon 14 Aug /dev/null	(0.6K)
[defaced]	<a href="#">www.newactionfilms.com</a>		[defaced]	<a href="#">www.micron5.com</a>	
	by GForce Pakistan			by GForce Pakistan	
■ 2500	Wed 2 Aug /dev/null	(0.6K)	■ 2715	Mon 14 Aug /dev/null	(0.6K)
[defaced]	<a href="#">www.thelawyer.co.uk</a>		[defaced]	<a href="#">www.roshnilaces.com</a>	
	by GForce Pakistan			by GForce Pakistan	
■ 2517	Thu 3 Aug Munge	(0.7K)	■ 2716	Mon 14 Aug /dev/null	(0.6K)
[defaced]	<a href="#">www.ubf.co.uk</a>		[defaced]	<a href="#">www.sbardafashion.com</a>	
	by GForce Pakistan			by GForce Pakistan	
■ 2519	Thu 3 Aug Munge		■ 2724	Mon 14 Aug Munge	(0.7K)
	by GForce Pakistan		[defaced]	<a href="#">www.sabyogtravels.com</a>	
■ 2520	Thu 3 Aug Munge	(0.8K)		by GForce Pakistan	
[defaced]	<a href="#">www.systematics-int.co.uk</a>		■ 2729	Tue 15 Aug McIntyre	(0.6K)
	by GForce Pakistan		[defaced]	<a href="#">www.sadhsamaj.com</a>	
■ 2521	Thu 3 Aug Munge	(0.8K)		by GForce Pakistan	
[defaced]	<a href="#">www.opalenergy.co.uk</a>		■ 2732	Tue 15 Aug McIntyre	(0.6K)
	by GForce Pakistan		[defaced]	<a href="#">www.bhansilk.com</a>	
■ 2537	Sat 5 Aug /dev/null	(0.6K)		by GForce Pakistan	
[defaced]	<a href="#">www.satannet.org</a>		■ 2735	Tue 15 Aug McIntyre	(0.6K)
	by GForce Pakistan		[defaced]	<a href="#">www.craftera.com</a>	
■ 2538	Sat 5 Aug /dev/null	(0.6K)		by GForce Pakistan	
[defaced]	<a href="#">www.vanessa-jones.com</a>		■ 2736	Tue 15 Aug McIntyre	(0.6K)
	by GForce Pakistan		[defaced]	<a href="#">www.vinayaksarees.com</a>	
■ 2539	Sat 5 Aug /dev/null	(0.7K)		by GForce Pakistan	
[defaced]	<a href="#">www.vanillaice.com</a>		■ 2738	Tue 15 Aug /dev/null	(0.6K)
	by GForce Pakistan		[defaced]	<a href="#">www.go4booking.com</a>	
■ 2646	Thu 10 Aug Munge	(0.7K)		by GForce Pakistan	
[defaced]	<a href="#">www.zlib.net.cn</a>		■ 2740	Tue 15 Aug /dev/null	(0.6K)
	by GForce Pakistan		[defaced]	<a href="#">www.indiakboobsurat.com</a>	
■ 2654	Thu 10 Aug /dev/null	(0.7K)		by GForce Pakistan	
[defaced]	<a href="#">www.delsoft.com</a>		■ 2741	Tue 15 Aug /dev/null	(0.6K)
	by GForce Pakistan		[defaced]	<a href="#">www.freeindia.com</a>	
■ 2683	Sat 12 Aug /dev/null	(0.6K)		by GForce Pakistan	
[defaced]	<a href="#">www.aidindia.org</a>		■ 2742	Tue 15 Aug /dev/null	(0.6K)
	by GForce Pakistan		[defaced]	<a href="#">www.aribantgroupindia.com</a>	
				by GForce Pakistan	

■ 2743	Tue 15 Aug /dev/null	(0.6K)
[defaced]	<a href="http://www.indialoaninfo.com">www.indialoaninfo.com</a>	
	by GForce Pakistan	
■ 2744	Tue 15 Aug /dev/null	(0.7K)
[defaced]	<a href="http://www.guawatiteaauktion.com">www.guawatiteaauktion.com</a>	
	by GForce Pakistan	
■ 2745	Tue 15 Aug /dev/null	(0.6K)
[defaced]	<a href="http://www.cngbandembroidery.com">www.cngbandembroidery.com</a>	
	by GForce Pakistan	
■ 2757	Wed 16 Aug /dev/null	(0.6K)
[defaced]	<a href="http://feecomp.osmre.gov">feecomp.osmre.gov</a>	
	by GForce Pakistan	
■ 2759	Wed 16 Aug /dev/null	(0.6K)
[defaced]	<a href="http://camelsbump.middlebury.edu">camelsbump.middlebury.edu</a>	
	by GForce Pakistan	
■ 2769	Fri 18 Aug /dev/null	(0.6K)
[defaced]	<a href="http://www.billboardtv.com">www.billboardtv.com</a>	
	by GForce Pakistan	
■ 2770	Fri 18 Aug /dev/null	(0.6K)
[defaced]	<a href="http://www.tvl.cc">www.tvl.cc</a>	
	by GForce Pakistan	
■ 2774	Fri 18 Aug Munge	(0.7K)
[defaced]	<a href="http://lotus.doe.state.in.us">lotus.doe.state.in.us</a>	
	by GForce Pakistan	
■ 2776	Fri 18 Aug Munge	(0.7K)
[defaced]	<a href="http://www.reservelabs.com">www.reservelabs.com</a>	
	by GForce Pakistan	

## La gestion de politique de sécurité

■ Dès 1992 HSC a toujours développé l'idée que :

- La sécurité se déployait plus facilement dans le réseau

- Ce déploiement devait s'effectuer de façon globale et dans une vision proche de l'expression d'un décideur.

Ces concepts ont été ensuite repris en France par Solsoft en 1997 avec Solsoft NP

([www.solsoft.com](http://www.solsoft.com)), puis Evidian dans Netwall ([www.evidian.com](http://www.evidian.com)) en 1999 (Bull à l'époque).

■ La mise en oeuvre fait généralement appel à un langage de haut-niveau pour définir sa politique de sécurité avec une vision globale, et la possibilité de voir graphiquement et topologiquement sa politique de sécurité, plus rarement de l'éditer sur la topologie.

La gestion de politiques (policy management), est de fait une problématique concernant l'ensemble d'une entreprise, connexe tant au monde de la gestion de réseaux qu'à celui de la qualité de service ou encore de la sécurité.

■ En Mai 1999, au IEEE Symposium on Security and Privacy à Berkeley en Californie, Lucent Bell Labs (New Jersey, USA) et le Weizmann Institute ont présenté le résultat de leurs travaux, intitulé : a role-based management toolkit. Ces travaux ont

depuis donné naissance à un prototype appelé Firmato, qui est devenu une spin-off de Lucent, puis qui a fusionné avec une autre spin-off de Lucent appelée Lumeta ([www.lumeta.com](http://www.lumeta.com)), elle-même issue d'Internet

■ Mapping Project et dans laquelle on trouve notamment Bill Cheswick.

■ Les travaux présentés à l'IEEE Symposium (<http://www.bell-labs.com/~yashb/sp99.ps>) apportent une formalisation du modèle entité-relationnel tel qu'utilisé par Solsoft NP.

■ Un compte rendu de la conférence est consultable à l'adresse suivante :

<http://cbacs.nrl.navy.mil/ieee/cipber/old-conf-rep/conf-rep-SP99.html>

■ L'année 2001 a par ailleurs vu la tenue à Bristol du second "Policy Workshop", entièrement consacré à ce domaine. Joseph Pato des laboratoires HP de Cambridge (USA) a ouvert cette édition en rappelant que le développement de la sécurité doit se faire parallèlement à celui des services en lignes, ceci n'étant possible que globalement par le biais de la gestion de politiques de sécurité (security policy-based management).

La première journée a été consacrée à la sécurité. Les participants ont ainsi eu l'occasion de découvrir plusieurs langages de gestion de politique pour la sécurité dans les systèmes d'exploitation ou les applications.

■ Globalement, ces efforts de simplification pour définir globalement une politique de sécurité sur un ensemble de serveurs et d'applications restaient cependant encore éloignées des capacités techniques d'un décideur. John Strassner de Cisco a rappelé les besoins fondamentaux de la gestion de politique dans les réseaux, avec l'exemple d'un réseau bancaire qui doit faire face à un crash boursier, et en conséquence changer rapidement et globalement sa configuration. Le PCIM (Policy Core Information Model) définit au DMTF et repris à l'IETF définit des classes et des entités permettant de structurer sa politique réseau. L'utilisation d'ULM pour la définition ne rend cependant pas l'abstraction des règles / conditions/actions très intuitive. Rick Roeling d'HP a dressé sa vision du marché et démontré que la gestion de politiques était pleinement justifiée sur un plan commercial. De très nombreux fournisseurs de service qui recherchent des outils de gestion d'approvisionnement ou fourniture de leurs services réseau (network provisioning), et divers facteurs soutiennent la demande tels que le manque de ressources humaines compétentes, le développement des services électroniques, de l'infogérance, et le besoin d'abstraction inhérent à la gestion d'un grand réseauhétérogène. Ce workshop était très orienté sécurité, alors qu'à l'IETF la gestion de politique est orientée qualité de service : PCIM est réalisé par des spécialistes de la QoS. PCIM est comme étant de loin le plus abouti des travaux de normalisation, et qu'il

pourrait servir à d'autres domaines hors des réseaux. On notera également l'affirmation par plusieurs orateurs que l'approvisionnement du contrôle d'accès dans les réseaux (network access control provisioning) était la brique de base réclamée par les fournisseurs, et que réseaux d'entreprises et de fournisseurs de services avaient tendance à ne devenir qu'un, tellement ils devenaient imbriqués.

#### Références :

- Web du Policy 2001 Workshop :

<http://www.dse.doc.ic.ac.uk/Events/policy-2001/>

- Associations de fournisseurs

**DMTF** : Distributed Management Task Force (anciennement Desktop Management Task Force) :

<http://www.dmtf.org/>

**SNIA** : Storage Networking Industry Association :

<http://www.snia.org/>

- Normalisation

**IETF** : Internet Engineering Task Force :

<http://www.ietf.org/>

**PCIM** : Policy Core Information Model :

<http://www.ietf.org/rfc/rfc3060.txt>

### Piratage divers

■ Le piratage du forum économique mondial de Davos constitue un archétype de la dichotomie opérée encore trop souvent entre sécurité physique et sécurité logique, ceci au détriment de cette dernière. De surcroît, il ne s'agit pas dans ce cas précis de la simple modification de page Web, mais bel et bien du vol de nombreuses données confidentielles (1400 n° de carte de crédit appartenant aux participants, ainsi que leur n° d'appel téléphonique, ce qui pour des chefs d'entreprise est un problème), tel que la presse s'en est fait l'écho. S'il est emblématique, l'incident de Davos, n'est cependant pas isolé. Cette année encore, de nombreux sites d'organisation à très forte visibilité, telles que l'OPEC, ont été victimes de piratages à l'occasion d'événements spécifiques. À noter que dans ce cas précis, le pirate s'était heureusement contenté d'insérer des commentaires dans le code source des pages HTML.

La page modifiée est consultable

#### à l'adresse suivante :

<http://www.attrition.org/mirror/attrition/2000/09/12/www.opec.org/>

■ Un autre piratage ayant défrayé la chronique est celui, beaucoup plus discret, mais aux conséquences probablement plus importantes, qui a touché 40 entreprises aux USA et un nombre inconnu dans le reste du monde. Cette série de piratage aurait permis à leurs auteurs de s'emparer des données relatives à plus d'un million de comptes.

Le point commun à toutes ces plates-formes attaquées n'est autre que l'utilisation des technologies Microsoft : Windows NT 4.0, IIS 4.0, and SQL 7.0/7.0

Enterprise. Il semble cependant que la plupart des vulnérabilités exploitées disposaient depuis longtemps d'un correctif.

<http://www.microsoft.com/technet/security/bulletin/ms99-025.asp>

<http://www.microsoft.com/technet/security/bulletin/ms00-008.asp>

<http://www.microsoft.com/technet/security/bulletin/ms00-014.asp>

<http://www.nipc.gov/warnings/advisories/1999/99-027.htm>,

<http://www.nipc.gov/cybernotes/cybernotes.htm>

### Les premières attaques pour Palm-Pilot

■ Le premier Cheval de Troie pour Palm-Pilot n'est apparu que fin Août(1).

Compte tenu de la facilité d'échanger des logiciels et d'autres données par infra-rouge, l'apparition de ce type de programmes n'est pas surprenante. La comparaison avec l'évolution des programmes similaires sur la plate-forme PC laisse à penser qu'une généralisation des virus et partant, des antivirus) sur les PDA n'est qu'une question de temps.

Il faut cependant garder à l'esprit que les échanges Palm par infra-rouge nécessitent d'une part validation et d'autre part, proximité de la source et du récepteur. Cette dernière contrainte sera néanmoins levée par l'utilisation de la technologie Bluetooth, améliorant ainsi le confort d'utilisation mais aussi bien entendu la diffusion des codes de toutes origines.

■ Le système d'exploitation du Palm-Pilot n'est pas très sécurisé, les modes de débogages permettent de contourner la sécurité apparentes, mais 3COM a promis que la prochaine version corrigerait ces défauts.

#### Pour en savoir plus :

[http://www.palminfocenter.com/palm/p\\_story.asp?ID=3D1158](http://www.palminfocenter.com/palm/p_story.asp?ID=3D1158)

<http://news.cnet.com/news/0-1006-200-2635223.html>

<http://www.techweb.com/wire/story/TWB20000828S0025>

<http://www.techweb.com/wire/story/TWB20000828S0025>

### Rachats/Fusions

■ Le marché a poursuivi cette année sa concentration, et les opérations de rachat et autres fusions n'ont pas manqué dans les différents secteurs de la sécurité.

Nos voisins d'Outre-manche et d'outre-Atlantique n'ont pas été inactifs, et Baltimore, l'éditeur de composants logiciels permettant de bâtir une infrastructure de clés, a ainsi acheté Content Technologies, leader de l'analyse de contenu. Ce dernier apporte son logiciel phare MIMESweeper, ainsi que son gigantesque

fichier commercial. Baltimore, déjà très agressif, ne manquera certainement pas d'utiliser ces deux atouts pour étendre sa main-mise sur le marché.

Dans le domaine des composants de PKI, HSC recommande par ailleurs de s'intéresser à l'offre des éditeurs non-anglo-saxons tels que ID2 (Suède) et Sagem (France).

■ Un autre rachat de taille est celui d'Axent par Symantec. Ce dernier, connu pour ses utilitaires pour Windows et notamment ses anti-virus, récupère ainsi des produits tels que le firewall Raptor, ou encore les logiciels ESM (gestion) et Netrecon (tests).

■ Ce rachat s'apparente à celui de McAfee reprenant TIS (devenu Network Associates), et positionne Symantec comme le compétiteur de NAI.

De son côté, Nortel Networks devance Cisco, Lucent, ou encore Alcatel, et acquiert Alteon et son offre complémentaire de commutateurs moyenne gamme. Quant à ISS et Check Point, ils semblent pour le moment chercher à maintenir leur position dans leur domaine, sans développer la même gamme que NAI et Symantec.

À noter également le rachat d'Internet Dynamics

(<http://www.interdyn.com/>)

par Redcreek (<http://www.redcreek.com/>).

Ce dernier, qui propose des boîtiers de chiffrement IPsec et fait partie des pionniers dans ce domaine, ne devrait conserver que le logiciel de gestion de politiques de sécurité, et l'adapter à la gestion des tunnels IPsec des boîtiers Redcreek.

■ Le marché français a lui aussi connu son lot d'acquisitions. Dans le désordre, on peut ainsi citer : L'intégrateur Neurocom, qui a mis la main sur la société de conseil en monétique OMI, MSI racheté par Intesis (groupe Finmatica), Axidia par l'américain Scient, GPS Consulting par Net2S, et CF6 par Telindus. Il est d'ailleurs à noter que si les rachats d'Edelweb par ON-X ou d'Intrinsec par Neurones étaient restés dans des montants raisonnables, cela n'est pas le cas dans les opérations récentes. Le rachat de CF6 par Telindus, ou la valorisation par ses investisseurs d'une société de service comme Lexsi, ont atteint des sommets qui laissent perplexe. IB Group a quant à lui fait coup double, avec le rachat de l'intégrateur Boréal et du leader du conseil en sécurité, XP Conseil.

Enfin, dans le cadre du démantèlement du groupe Bull en Bull, Intégris et Evidian, Schlumberger reprends Bull CP8 (Bull Smart Cards).

■ Parallèlement, quelques sociétés étrangères se sont implantées en France cette année. Entrust, le dernier grand du secteur des PKI a ainsi créé sa filiale française, tout comme la société Finlandaise SSH, leader du chiffrement logiciel dans les réseaux, et StoneSoft, qui propose de la haute disponibilité pour FW-1. Moins heureusement, la société marchFIRST

(<http://www.marchfirst.com/>), qui a racheté la société USweb/CKS, qui elle-même avait racheté la société française Sysicom, ne semble pas au mieux financièrement, et l'action s'est effondrée de manière spectaculaire. Cette société est notamment un intégrateur en sécurité, qui a réalisé de nombreux projets sécurité en France, dans les banques, assurance, industrie, secteur public et opérateurs. MarchFIRST compte 10000 employés et dans le cadre des plans de redressement que beaucoup d'entreprises du secteur connaissent en France, les filiales de petite taille comme celles en France soient les premières touchées.

## Le filtrage de contenu

■ L'analyse de contenu constitue un autre marché très porteur. Dans les réseaux, l'analyse de contenu est le complément indispensable ou inévitable au firewall et au serveur de messagerie. En France, les principaux bénéficiaires de ce dynamisme sont les éditeurs classiques d'anti-virus : Trendmicro avec Interscan, Baltimore (anciennement Content Technologies) avec la gamme sweeper, NAI avec la suite McAfee, et Symantec avec Norton anti-virus. À l'heure actuelle, l'analyse de contenu repose en effet principalement sur les anti-virus, qui comprend outre ceux cités ci-dessus, de nombreux (CA, F-Secure, Sophos, Tegal, etc.).

■ La partie en fort développement est l'analyse de contenu dans le réseau. Sur la messagerie, l'analyse de contenu pour lutter contre les contenus malveillants est plus importante que jamais. Avec les messages ne contenant que des URLs qui poussent l'utilisateur à cliquer, l'analyse de contenu doit aussi se déplacer vers les relais HTTP. On pourra d'ailleurs se reporter à la publication par le DoD de son classement des codes malveillants, plus loin dans ce guide.

■ À titre d'exemple, un attaquant peut très facilement envoyer un programme exécutable en imitant un autre à un utilisateur peu expérimenté d'une entreprise, l'utilisateur exécute ce programme en toute bonne foi, ce dernier se connectant par exemple en HTTP au serveur web de l'attaquant, qui peut alors en toute quiétude exécuter des commandes sur un PC au cœur même du réseau de l'entreprise.

■ D'autres filtrages se développent, sur des critères géographiques ou sur le type de contenu, mais ceux-ci sortent du cadre de la sécurité des réseaux.

## Les VPN

- Un VPN est un réseau privé virtuel. En sécurité, un VPN sera composé de tunnel chiffrés. Dans les réseaux TCP/IP le protocole normalisé pour bâtir des VPN ainsi sécurisés est IPsec.
- Les VPN sont un marché en devenir. Malgré un important support marketing, le marché des VPN demeure en effet anecdotique face à celui des FW. Cependant, beaucoup de produits firewalls intègrent le support des VPNs IPsec et sont ainsi utilisés pour gonfler artificiellement le marché des VPN. Beaucoup de FW permettant la construction de tunnels IPsec sont en effet utilisés uniquement en tant que FW, sans utilisation de la fonctionnalité tunnels IPsec.
- Le marché est découpé en trois présentations marketing d'équipements souvent très similaires : le fond de panier sera plutôt un commutateur pour la performance, le filtrage IP est omniprésent, et la possibilité de faire des tunnels IPsec est de base :
  - Les routeurs/commutateurs qui permettent aussi de faire des tunnels IPsec, pour lesquels le leader du marché est Cisco
  - Les firewalls qui intègrent presque tous une fonction de tunnels IPsec, pour lesquels les leaders sont Cisco avec le PIX, Nokia et Checkpoint.Mais dans ce domaine Watchguard et Sonicwall ont trouvé leur place aux USA, Netasq en France. La plus forte croissance est NetScreen qui doit désormais être considéré comme un leader du secteur
- Les boîtiers de chiffrement, qui en général disposent aussi des fonctions de firewall et de routage, et pour lesquels les leaders sont Alcatel, Nortel, Radguard, et Redcreek.

## Actualité en cryptographie

- L'un des événements les plus médiatisés dans le domaine de la cryptographie a sans conteste été le choix pour l'AES (Advanced Encryption Standard) de l'algorithme Rijndael. Il est à noter que si ce dernier est déjà disponible sur la grande majorité des systèmes et même sur une carte à puce, il est cependant pas encore intégré dans les normes, où la manière de l'intégrer n'a pas été décidée. Pour plus de détails, le lecteur curieux pourra entre autres se référer à :  
<http://csrc.nist.gov/encryption/aes/>
- Quelque temps auparavant, une page de la cryptographie se tournait déjà, avec le communiqué de presse de RSA, qui annonçait la mise en domaine public sur l'algorithme à l'origine de son nom, ceci quelques semaines avant l'expiration du brevet correspondant. RSA aura ainsi jusqu'au bout su tirer parti de la notoriété de l'algorithme, qui devait tomber dans le domaine

public quelques semaines plus tard. Cela ouvre de nouvelles perspectives pour la sécurité, car RSA notamment avant son rachat par Security Dynamics réclamait des royalties sur l'usage de l'algorithme.

- PGP avait déjà ouvert la voie en offrant au grand public d'utiliser des moyens de chiffrement forts dans le cadre du courrier électronique grand public. Son créateur Philippe Zimmerman a quitté NAI, l'éditeur de PGP.

- La start-up californienne Starium (<http://www.starium.com/>) annonce quant à elle un boîtier de chiffrement pour le téléphone vocal, utilisant le triple-DES avec une clé de 168 bits, dont l'une des principales particularités sera d'être proposé à un prix inférieur à \$100, à comparer avec les \$3000 et plus auxquels sont proposés ses concurrents.

## Le GSM

- On savait déjà que l'algorithme de chiffrement utilisé par le GSM n'était pas inviolable, mais un problème connu de longue date dans les milieux spécialisés a récemment fait l'objet d'une certaine publicité. Dans la mesure où les téléphones portables n'authentifient pas les stations (ni dans le GSM ni dans aucun autre système), une station intermédiaire peut faire croire au GSM qu'il est dans une zone n'autorisant pas le chiffrement, et ainsi capter en toute discrétion les échanges téléphoniques. À noter cependant que cette faille doit être corrigée dans les évolutions du standard GSM.

- Pour plus de détails, on pourra consulter l'article paru à ce sujet dans

**Zdnet :**

<http://www.zdnet.com/zdnn/stories/news/0,4586,2628754,00.html>

## La valse des salons

- Une des conséquences du passage au premier plan de la sécurité des systèmes et réseaux est que pas moins de 5 salons ont tenté cette année de s'imposer sur ce thème. Si le salon SESI qui devait accompagner Eurosec (<http://www.xpconseil.com/eurosec2001/>) a été annulé, ce dernier semble être devenu incontournable, et demeure ainsi la plus importante conférence en sécurité francophone, avec de très nombreux orateurs et des conférences de qualité.
- Les conférences Netsec pendant le salon du même nom n'ont parfois attirées un public ne dépassant pas 20 personnes. On pouvait aussi visiter la salon de

la Sécurité Informatique  
(<http://www.infosecurity.com.fr/>)  
organisé par l'anglo-saxon Reed  
(<http://www.reed-oip.fr/>)  
qui n'offrait cependant pas de conférences associés.  
Reste à venir Infosec  
(<https://www.clusif.asso.fr/infosec2000/>)  
établi depuis 15 ans, et organisé par MCI,  
qui a eu un grand succès en 2000.

## L'insécurité des développements en ligne

■ Soumises aux impératifs du marketing, confrontées à la pénurie de compétences, les sociétés de développement ont la plupart du temps des difficultés considérables pour intégrer la sécurité dans les projets qui leur sont demandés. Wanadoo a ainsi été victime d'une faille de sécurité dans les logiciels utilisés pour gérer les forums du FAI, forums dont la réalisation et l'hébergement avaient été confiés à une société tierce. Cf :

<http://www.zdnet.fr/actu/inte/a0016211.html>

■ Si dans le cas ci-dessus, les conséquences visibles n'ont rien de dramatique, il n'est malheureusement pas interdit de penser que les développements de projets autrement plus critiques ne font pourtant pas plus de cas de la sécurité.

## Le paiement en ligne

■ Ipin est une technologie de paiement. A la lecture du site web de la société Californienne ([www.ipin.com](http://www.ipin.com)), ce logiciel de gestion de comptes bancaires ne semble pas présenter d'innovations particulières, avec le support des formes classiques d'authentification des individus et de paiement en ligne sécurisés.

Ipin vaut cependant que l'on s'y intéresse pour les sociétés qui investissent dans ce système. Le créateur de la filiale Européenne n'est autre que France Telecom, avec des participations minoritaires de Wanadoo et Ipin.

Après les échecs à répétition de dizaines de systèmes de paiement en ligne, et bien qu'Ipin ne me semble pas un paiement en ligne mais un progiciel de gestion bancaire entouré d'un marketing adéquat, l'initiative semble digne d'intérêt dans la mesure où il s'agit du premier système de paiement en ligne dans lequel un opérateur et non pas une banque investit.

■ Parallèlement, on peut noter la renaissance de la technologie de GTech chez BlueLineInternational, alors que la fusion BNP et Paribas a définitivement

enterré Kline au profit de Cybercomm, dont l'avenir demeure incertain.

## Microsoft victime d'un piratage de son réseau

■ Le géant de Redmond a lui-même été victime d'une intrusion de l'extérieur sur son réseau interne. Le nombre de serveurs internes auxquels les pirates ont eu accès, les documents confidentiels, sources et autres, qui ont été dérobés à cette occasion, ne sont pas connus. Plusieurs sources affirment que le/les intrus seraient restés plus de deux mois au sein du réseau interne de Microsoft, mais il n'existe aucune preuve formelle de ce point. Microsoft qui au vu de la gravité de l'événement, a préféré prendre les devants pour l'annoncer à la presse n'a cependant pas convaincu le CSIS (Center for Strategic & International Studies). Ce laboratoire de recherche politique basé à Washington, a rendu public un rapport intitulé "Cyber-Threats and Information Security" qui met en exergue les risques inhérents à l'utilisation des logiciels de Microsoft suite au piratage dont celui-ci a été victime. Les experts estiment ainsi qu' "il est improbable que l'on puisse passer en revue les millions de lignes de code des programmes de Microsoft pour s'assurer qu'elles n'ont pas été compromises par le ou les pirate(s)".

■ S'il est évident que la sécurité absolue n'existe pas, la mise en première ligne sur Internet de technologies Microsoft n'offre malheureusement pas le plus haut niveau de sécurité. Dans cette optique, HSC préconise depuis longtemps diverses solutions permettant de continuer à utiliser les produits Microsoft : protection des serveurs IIS par des relais Apache sous Unix, confinement des serveurs WNT sur des segments séparés, utilisation de Corba en lieu et place de DCOM....

### Pour en savoir plus :

<http://cmfn.cnn.com/2000/10/27/technology/microsoft/>

## La détection d'intrusion

■ En terme de recherche, la détection d'intrusion est toujours présente, mais en terme de marché, celle-ci n'est plus aussi présente. La conférence RAID (Research and Advances in Intrusion Detection), organisée du 2 au 4 Octobre à Toulouse a ainsi été l'occasion de rencontrer des sociétés et chercheurs présentant des solutions ou approches potentiellement disponibles et de mieux cerner les lacunes des systèmes IDS existants. (Les supports des présentations sont disponibles sur le site web du RAID)

(<http://www.raid-symposium.org/>).

■ Cette troisième édition a permis de découvrir des travaux qui ont conduit à l'implémentation de solutions presque directement utilisables sur Solaris, et d'autres pouvant améliorer l'approche de l'investigation ou de la réaction face à des intrusions. Dans ce même domaine, l'édition d'Octobre 2000 de SANS a par ailleurs vu la démonstration par les australiens de l'utilisation combinée de Shadow et Snort. Ce dernier peut ainsi utiliser la base de règles de Shadow en plus de la sienne, et devient le logiciel d'écoute (sensor) de Shadow, qui continue à faire les analyses a posteriori.

■ Malheureusement, si la recherche progresse, le marché s'essouffle. La majorité des systèmes de détection d'intrusion achetés ne sont en effet pas utilisés, faute d'équipes dédiées et spécialisées capables de faire face à de fausses alarmes encore trop nombreuses. Les logiciels de détection d'intrusion ont d'ailleurs le record des logiciels achetés qui ne servent pas. Les acteurs majeurs dans ce secteur demeurent les mêmes : ISS, Cisco avec ses sondes intégrées dans les routeurs et de nombreux autres comme NAI, ou encore Symantec avec NetRecon racheté d'Axent. Le secteur qui émerge en marge de la détection d'intrusion est la détection d'incident, notamment par l'analyse des journaux. Derrière le succès de Webtrends dans ce domaine, beaucoup de sociétés se développent comme Netforensics pour les routeurs Cisco, ou NetSecureSoftware et Cyrano en France.

## Méthodes

■ La France n'est pas absente de ce domaine avec les méthodes Mehari, Marion, et Melissa. L'année 2000 a vu la traduction en anglais de la méthode EBIOS du SCSSI, **disponible à l'adresse suivante** :  
<http://www.scssi.gov.fr/document/docs/EBIOS/ebios.html>

■ Parallèlement, le Software Engineering Institute de l'Université Carnegie-Mellon, où est également situé le CERT-CC, publie sa méthode d'évaluation des risques informatiques, que l'on pourra **consulter à cette url** :  
<http://www.cert.org/octave/> ou  
<http://www.sei.cmu.edu/publications/documents/99.reports/99tr017/99tr017chap02.html>

■ Le NIST américain a également publié deux documents intéressants pour recueillir des commentaires publics, portant respectivement sur la détection d'intrusion et les principes de sécurité. S'il doit faire l'objet d'une étude approfondie, ce document présente cependant une synthèse intéressante en termes de recommandations, avec 32 principes de base en

sécurité, par exemple isoler les fonctions les unes des autres. Ces documents au format Word sont **disponibles sur** :

<http://csrc.nist.gov/publications/drafts.html>

■ Dans le même domaine, le CIS (Center for Internet Security)  
<http://www.sans.org/cissummary.htm>), organisation américaine à but non lucratif a pour ambition d'élaborer une méthode permettant de qualifier la sécurité d'une entreprise ou d'une entité. Cette méthode devrait servir à mesurer la sécurité de prestataires ou de partenaires pour s'assurer par exemple que lorsqu'un partenaire est relié à un réseau d'entreprise via un VPN alors il correspond à un certain niveau de sécurité et possède telle ou telle note selon les critères du CIS. Les travaux s'inspirent au départ du travail réalisé par VISA pour vérifier la sécurité des 21 000 organisations qui bénéficient du logo de VISA.

Une première version de la méthode est prévue pour mi-2001, et des logiciels automatiques de vérification de la conformité seront aussi développés. Plusieurs organismes et entreprises américaines font déjà partie du CIS, tels que : ATT, Axent, le CERT du DoD, l'ISACA, ISS, Merrill Lynch, la NASA, le Naval Surface Warfare Center, Stanford University, SANS, Stanford University, Virginia Tech University, et bien sûr Visa.

## Normalisation

■ En ce qui concerne les efforts entrepris dans ce domaine, c'est la norme anglaise BS 7799 qui se trouve au centre de l'actualité des derniers mois. Même si cette norme a été mise en procédure rapide pour passer à l'ISO au niveau international, quasiment tous les pays non-anglo-saxon ont refusé cette norme, qui constitue une approche typiquement anglaise des choses, et souffre de nombreux défauts. Elle rentrerait ainsi en conflit avec nombre d'autres travaux déjà existants et reconnus, et ses propositions ne tiendraient pas compte des modèles de développement. Par ailleurs, suivre ses préconisations équivaldrait à figer la sécurité dans le temps, et dans la mesure où elle n'induit pas de démarche opérationnelle, ne permettrait pas de construire une politique de sécurité. Cette affaire reste à suivre dans la mesure où à l'ISO, les anglais ont obtenu par dérogation le n° ISO 17799 au cas où cette norme anglaise serait publiée au niveau international.

## Actualité Judiciaire

■ Dans un jugement rendu le 2 novembre 2000, le tribunal correctionnel de Paris estime que la messagerie Internet est d'une part couverte par la loi

sur les télécommunication, et d'autre part qu'un courrier électronique est une correspondance privée, couverte par la loi sur le secret des correspondances. De surcroît, cette règle reste valable en cas d'utilisation à des fins privées d'un ordinateur destiné à un usage professionnel.

Les prévenus, trois responsables d'un laboratoire de recherches parisien réputé, ont été condamnés pour "violation de correspondances effectuées par voie de télécommunications, par personne chargée d'une mission de service public".

Cette affaire soulève un certain nombre de questions : Même en prévenant ses employés, est-il encore possible d'archiver les messages, ou de réaliser une analyse de contenu contextuelle sur sa passerelle de messagerie ?

J'ai eu l'opportunité de poser la question à un commissaire divisionnaire, conseiller technique sur ces sujets. La prise en compte de la nationalité du salarié permettra ou non de proter plainte. Cependant, si par exemple la passerelle de messagerie est située à Londres, la justice britannique ne collaborant pas, aucune des preuves techniques indispensables ne parviendront au juge français.

#### **Pour en savoir plus :**

Texte du jugement :

<http://www.canevet.com/jurisp/textes/001102.htm>

### **Securité des systèmes d'exploitation**

■ L'institut SANS a publié une étude comparative des méthodes de sécurisation de Solaris : <http://www.sans.org/sol11c.pdf>.

■ Si le PDF n'est pas de bonne qualité, il reste cependant lisible et constitue un document de base utile. Les trois méthodes de sécurisation faisant l'objet du comparatif sont les suivantes :  
- "Securing Solaris Step by Step, un bon document présenté par SANS et auquel des experts reconnus ont participé,  
- Les scripts Titan, qui sont quelque peu anciens, et enfin le script YASSP de Jean Chouanard, réalisé à Xerox Parc, et également soutenu par l'Institut SANS. Pour information HSC a revu, utilise et recommande YASSP : <http://www.yassp.org/>

■ Concernant le système d'exploitation Windows NT, il a également été l'objet d'une autre étude, réalisée par attrition.org, et qui le place en première position des serveurs piratés tels que recensés par attrition.org. Bien sûr cette première place doit être tempérée au vu des parts de marché non négligeables du dit OS, mais ceci ne doit pas faire oublier les causes premières de ce résultat, à savoir les déficiences prononcées de la sécurité sur ce même système.

■ L'actualité de la sécurité des systèmes d'exploitation reste dominée d'un côté par le succès de Linux et sa forte croissance cette année, et de l'autre par la complexité des modèles de sécurité de W2K, dont le déploiement n'a pas atteint les objectifs de Microsoft. Windows XP (Whisler) offre une migration plus facile, depuis les systèmes Microsoft existants, et permettra sans doute plus d'exemples de mise en oeuvre sur des réseaux importants de la sécurité distribuée avec MS\_Kerberos et Active Directory.

■ Un article traitant de la problématique d'authentification dans W2K devrait d'ailleurs être disponible sur le site [www.hsc.fr](http://www.hsc.fr) à la date de publication du présent guide.

### **Signature des codes mobiles**

■ La problématique des codes mobiles est revenu à l'honneur avec la volonté affichée par Microsoft d'incorporer un système de signature de code dans son système d'exploitation Whistler, depuis renommé Windows XP. Si en théorie, cette technologie permettrait de protéger le poste de travail contre des codes malveillants, elle comporte un très grand nombre de défauts. Dans le meilleur des cas, la signature des codes mobiles se limite en effet à garantir l'identité de l'auteur du code mobile. Au contraire une technique comme un bac à sable implémenté dans les machines virtuelles JAVA ou le chroot sous Unix apportent une réelle sécurité de par la conception du système. On peut par ailleurs s'inquiéter du contrôle qu'obtiendrait Microsoft sur les développeurs et éditeurs de par les coûts et les barrières à l'obtention d'une signature certifiée. Dans la même optique, que penser du refus potentiel d'exécution des codes de concurrents suite au contrôle de la signature du code exécutable par le système ? La validité du système a été encore tout récemment remise en question puisque il a été révélé que deux signatures avaient été délivrés par Verisign à un individu qui s'est fait passer pour un employé de Microsoft. Les deux certificats sont donc présentés comme venant de "Microsoft Corporation". Si Microsoft prend bien soin de préciser que le code signé par ces certificats ne sera pas accepté par défaut, il est à craindre que l'affichage du nom "Microsoft corporation" constitue à tort une garantie suffisante pour l'immense majorité des utilisateurs. Cette technologie ne semble donc malheureusement pas différente des autres propositions de Microsoft dans le domaine de la sécurité. Si elles peuvent sembler séduisantes au premier abord, elles n'aboutissent généralement qu'à l'instauration d'un faux sentiment de sécurité (cf les mécanismes cryptographiques de la suite Office), et peuvent souvent constituer des outils de choix pour le contournement des mécanismes de sécurité.

## L'avis microsoft est consultable à :

<http://www.microsoft.com/technet/security/bulletin/MS01-017.asp>

## Avis Verisign :

<http://www.verisign.com/developer/notice/authenticcode/>

## Avis du CERT :

<http://www.cert.org/advisories/CA-2001-04.html>

■ HSC rappelle à titre historique, que lors de son étude de Lotus Notes Domino de Novembre 1998, une des surprises avait été la découverte de l'acceptation par Lotus Notes de tout code externe signé par Lotus, en dur dans le code, sans qu'aucun mécanisme de configuration ne puisse l'interdire et quelle que soit la méthode de réception du code par le logiciel.

## Remise en cause de la signature électronique

■ L'année 2000 a aussi vu une tentative de remise en cause de la loi sur la signature électronique sur la base des possibilités d'usurpation des numéros de téléphone. La technologie RNIS intègre, sauf erreur de notre part, deux n° d'appelant véhiculés en MSISDN. L'un est le numéro présenté, l'autre est le numéro d'origine de l'appel. Le numéro présenté est aisément modifiable avec un simple testeur RNIS. Il est possible ainsi de lancer des appels et faire afficher le numéro d'appel que l'on veut sur le téléphone du correspondant. Cette possibilité d'usurper, en apparence, le n° de l'appellant, a été cité dans un article disponible à l'url :

<http://www.infojuris.com/immunis/veille/preuveelec.html>

■ Il faut garder à l'esprit que cette usurpation de n° RNIS présenté n'est en rien nouvelle, et qu'il n'y a pas en France de cas connus de ce type de manipulations.

## CERTs et Avis de sécurité

■ À l'initiative de Microsoft et Cisco, 18 sociétés américaines dans le domaine des technologies ont créé un nouveau groupe : Information Technology Information Sharing and Analysis Center (IT ISAC), que l'on pourrait à priori assimiler à une sorte de CERT privé. Initialement limité aux sociétés leaders du monde informatique, les porte-paroles de L'IT ISAC envisagent de lier des liens avec d'autres sociétés, d'autres CERTs et certaines agences gouvernementales.

■ Cette annonce permet de mieux comprendre la décision de Microsoft de ne plus publier ses avis de sécurité par messagerie. Cette décision sur laquelle le géant de Redmond est depuis revenu rendait impossible l'accès aux avis de sécurité hors consultation directe du serveur de Microsoft. À l'occasion de la re-publication d'un avis Microsoft dans la liste Bugtraq, Microsoft avait d'ailleurs fait savoir que le Copyright ne permettait pas une telle re-diffusion.