

## SOMMAIRE

<b>SPAM</b>	<b>1</b>
<ul style="list-style-type: none"><li>• SurfControl présente les grandes tendances du T1 2006 en matière de spams</li><li>• Watsoft signe un accord de partenariat avec l'éditeur suédois Secured eMail</li><li>• La cyberguerre contre le Spam d'une société israélienne induit des représailles cuisantes</li></ul>	
<b>PATCH</b>	<b>3</b>
<ul style="list-style-type: none"><li>• ISS met en garde contre les risques juridiques liés au déploiement de correctifs d'urgence non officiels</li></ul>	
<b>RÉSEAUX</b>	<b>3</b>
<ul style="list-style-type: none"><li>• ExaProtect accroît la pertinence de sa technologie SIM avec le CSEM</li><li>• La Seine Maritime choisit CheckPhone pour sécuriser ses infrastructures téléphoniques IP</li><li>• Resilience annonce deux nouvelles applications UTM de Check Point</li><li>• Portugal Telecom choisit les appliances UTM Netasq pour sa nouvelle offre de services de sécurité</li></ul>	
<b>VIE PRIVÉE</b>	<b>5</b>
<ul style="list-style-type: none"><li>• Selon la NSA, l'administration Bush retient des logs de façon illégale</li><li>• Inquiétudes sur le plan Wi-fi de la ville de San Francisco</li></ul>	
<b>VIRUS</b>	<b>5</b>
<ul style="list-style-type: none"><li>• F-Secure propose une protection antivirale pour la plate-forme S60 3<sup>ème</sup> édition</li><li>• Selon McAfee SiteAdvisor, la plupart des internautes ne reconnaissent pas les sites distribuant des spywares</li><li>• McAfee propose une protection antivirus pour les ordinateurs Apple à processeurs Intel</li><li>• Un virus diffuse sur internet les plans secrets d'une centrale électrique japonaise</li><li>• La sécurité préventive ? Plus que jamais, une nécessité pour les entreprises</li></ul>	
<b>GESTION DES VULNÉRABILITÉS</b>	<b>9</b>
<ul style="list-style-type: none"><li>• ISS dévoile son prototype SWIPS de prévention des intrusions</li><li>• Cinq ans de prison pour Jeanson Ancheta, le pirate aux 400.000 PC zombies</li></ul>	
<b>BIOMÉTRIE</b>	<b>10</b>
<ul style="list-style-type: none"><li>• Extensity France annonce la disponibilité d'un nouveau module : Anael biométrie</li><li>• Axalto fournit les puces biométriques des cartes d'identités nationales au Qatar</li></ul>	
<b>PIRATAGE</b>	<b>10</b>
<ul style="list-style-type: none"><li>• Des clients du restaurant Courtepaille victimes d'escroquerie à la carte bancaire</li><li>• Un fonctionnaire fédéral américain condamné pour avoir pénétré le PC d'un supérieur</li></ul>	

### SPAM

#### **SurfControl présente les grandes tendances du T1 2006 en matière de spams**

SurfControl, un leader mondial de la protection des contenus sur Internet, présente les résultats de ses dernières recherches sur l'évolution des menaces inhérentes aux e-mails, au cours du premier trimestre 2006 en s'appuyant sur son service ATI (Adaptive Threat Intelligence).

Sur les trois premiers mois, le volume de spams associés aux produits et services a enregistré une croissance continue de 16 % par mois. Cette augmentation s'explique en partie par l'activité particulièrement soutenue en Russie et en Chine, deux zones géographiques où les spams sont souvent plus « génériques » en faisant par exemple la promotion de services de formation, de sites de commerce en ligne ou encore de portails de discussion en ligne. Les attaques de phishing et les autres types d'e-mails malveillants affichent également un taux de croissance à deux chiffres.

En outre, l'éditeur a observé une augmentation significative des spams associés aux produits pharmaceutiques et financiers, ces deux catégories représentant 80 % du volume total de spams. Au cours du seul mois de mars 2006, quelque 1,2 cas de spams graphiques de conseil boursier ont été identifiés. Ce type de spam – qui reste le plus répandu – représente 40 % du volume total de spams financiers. Le spam graphique est un courrier indésirable dont l'intégralité du message est présentée sous forme graphique et qui ne comporte aucun texte « parasite ». Les spammeurs ont intensifié leur usage des services gratuits de redirection afin d'accroître la « note de légitimité » qui leur est attribuée par la technologie de réputation des noms de domaine. Google.com figure à ce titre parmi les redirecteurs les plus couramment utilisés. En Amérique du Sud et dans d'autres régions du monde, les hébergeurs gratuits comme AOL sont utilisés par les spammeurs pour héberger les applications malveillantes (exécutables, keyloggers) les plus répandues. SurfControl a également constaté une utilisation croissante des extensions de domaine de pays lointains comme .as, .cc, .sh ou encore .in. Le fait d'utiliser ces extensions accroît la vulnérabilité potentielle des internautes visés.

<http://www.surfcontrol.com>

## **Watsoft signe un accord de partenariat avec l'éditeur suédois Secured eMail**

Watsoft signe un accord d'exclusivité avec l'éditeur suédois Secured eMail pour la distribution de son logiciel de cryptage de courriers électroniques en France. L'expéditeur du message sécurisé transmet un « secret partagé » au destinataire, qui génère des clés uniques de 256 bits servant à crypter les e-mails à chaque envoi de courrier. Les messages étant transférés directement de l'ordinateur de l'expéditeur à celui du destinataire, ils ne transitent pas par différents serveurs. Il est donc impossible de les intercepter. Secured eMail s'intègre dans Outlook : l'expéditeur rédige son message comme il le fait habituellement et l'envoie en cliquant sur le bouton « Send secure ». Le destinataire n'a pas besoin d'être équipé du logiciel pour pouvoir recevoir le message ; il l'ouvre dans son interface client de messagerie (même Webmail) en téléchargeant le module gratuit Secured eMail Reader, puis en entrant le secret partagé que lui a préalablement transmis l'expéditeur. S'il utilise Outlook, il peut à son tour répondre de manière sécurisée. Fondée en 2003 et implantée à Göteborg en Suède, la société Secured eMail est spécialisée dans la sécurité des communications électroniques.

<http://www.watsoft.com>

<http://www.securedeemail.com>

## **La cyberguerre contre le Spam d'une société israélienne induit des représailles cuisantes**

Le spam a la vie dure. Il continue de compter approximativement pour 70% de tous les messages d'E-mail sur l'Internet, en dépit de la sévérité des lois antispam à travers le monde, des procès vigoureux contre différents expéditeurs de masse. Aussi, relève le New York Times du 21 mai, la prévision célèbre, faite par Bill Gates au Forum Economique Mondial en 2004, que le Spam serait supprimé d'ici 2006, reste-t-elle lettre morte. Le défi posé aux technologues a démontré la difficulté de le relever : Blue Security, une compagnie antispam basée en Israël, a été conduite à arrêter ses services. La compagnie avait donné à ses clients la capacité de pratiquer une « mob justice » une justice collective. Comment ? En surchargeant les expéditeurs de demandes d'être enlevés des listes d'expédition. Un spammer en Russie a exercé aussitôt des représailles d'abord en frappant le site web de l'entreprise et en le mettant hors d'état de fonctionner et ensuite, en menaçant ses clients d'attaques de virus. Blue Security a indiqué qu'elle préférerait arrêter son action plutôt que d'être responsable d'une « cyberguerre ».

<http://www.nytimes.com>

## PATCH

### **ISS met en garde contre les risques juridiques liés au déploiement de correctifs d'urgence non officiels**

Internet Security Systems (ISS), acteur majeur du marché des solutions de sécurité préventive pour les entreprises, met en garde contre les risques juridiques liés au déploiement de correctifs d'urgence non officiels. Ces derniers mois, l'équipe de recherche X-Force a constaté une recrudescence des correctifs officiels proposés aux entreprises pour couvrir des vulnérabilités non encore traitées par l'éditeur de l'application. Elle déconseille fortement aux entreprises de les déployer et propose une solution de protection alternative.

La X-Force identifie les voies d'accès à la disposition des cyberpirates, développe un « patch virtuel » et le met à la disposition de ses clients. La technologie Virtual Patch protège ainsi l'entreprise en détectant et bloquant, durablement et dès le premier jour, toute tentative d'exploitation de la vulnérabilité. Elle élimine, sinon le besoin, au moins l'urgence de tester et mettre en œuvre le correctif de sécurité proposé par le constructeur ou l'éditeur et donne la possibilité de réintégrer la gestion des correctifs de sécurité dans les processus normaux de conduite du changement, profitant par exemple d'une opération de mise à jour applicative pour déployer un correctif dûment testé. En 2005, ISS a réalisé un chiffre d'affaires de 330 M\$. L'éditeur emploie 1.200 personnes et est implanté en Amérique, Asie, Australie, Europe et au Moyen-Orient (35 bureaux dans 20 pays). Son siège social est basé aux Etats-Unis, à Atlanta en Géorgie.

<http://www.iss.net>

## RÉSEAUX

### **ExaProtect accroît la pertinence de sa technologie SIM avec le CSEM**

Les produits SIM (Security Information Management) sont une évolution des outils basiques qui en leur temps collectaient, agrégeaient, reportaient, ou archivaient des événements à partir des outils de sécurité périphériques (IDS, firewalls, etc...) en place dans l'entreprise. Ils aident à réduire la charge des administrateurs IT qui consistait essentiellement à trier les menaces véritables noyées dans le flot des volumes de données de sécurité en tous genres, et des faux positifs, que ces outils périphériques génèrent.

Cependant, ce focus sur les outils de sécurité périphériques ne donne que peu ou pas de visibilité sur les systèmes internes en prise avec le cœur du business et l'information qu'ils contiennent. Ils sont une approche tactique à un problème informatique.

Le concept du CSEM proposé par ExaProtect repose sur l'approche inverse. L'accent est mis sur les actifs stratégiques business et s'étend à l'ensemble du périmètre du système d'information. De cette manière, les données de sécurité sont rassemblées à partir de tous les outils et applications dans lesquels est créée, stockée et transmise, l'information stratégique, et pas seulement à partir des outils périphériques. Il s'agit d'une approche stratégique pour une problématique business.

Les solutions CSEM assurent le monitoring des actifs stratégiques, des activités et des comportements sur les réseaux internes et externes. Elles compilent tous les processus concernés en temps-réel avec les processus de l'entreprise, alertent les administrateurs en cas de déviation, et fournissent une analyse en profondeur des activités déviantes au fur et à mesure qu'elles se présentent. Ceci garantit que les actifs stratégiques sont protégés de tout type de modification non souhaitée et offre une vision complète et auditable de la sécurité du système d'information de l'entreprise.

<http://www.exaprotect.com>

### **La Seine Maritime choisit CheckPhone pour sécuriser ses infrastructures téléphoniques IP**

Dans le cadre de la migration de ses infrastructures de téléphonie vers des technologies IP, le Département de Seine Maritime s'est imposé, dès le début du projet, des contraintes fortes en terme de sécurité afin de

garantir aux dix sites concernés et à leurs 2.500 utilisateurs la disponibilité, l'intégrité, la confidentialité et l'imputabilité (authentification et traçabilité des opérations).

Ainsi, et parallèlement au choix de la solution de téléphonie sur IP, l'organisation sécurité du Département de Seine Maritime souhaitait que la solution de sécurité VoIP assure la haute disponibilité des fonctionnalités et la mise en place d'une architecture sécurisée. Par la suite, des solutions d'interconnexion via Internet seront à l'étude pour raccorder sur le réseau téléphonique les quelques 350 sites restant.

A partir de ces contraintes élevées en terme de sécurité, le Département de Seine Maritime recherchait notamment une solution de protection contre les opérations de détournement de trafic des liens opérateurs (phreaking), et contre le rebond du système de téléphonie vers le reste du système d'information.

Le Département a donc lancé en 2005 un appel d'offre et a finalement sélectionné la solution ETSS de CheckPhone, dont le déploiement sur les dix sites concernés par l'appel d'offre leur garantit ainsi un niveau de sécurité et de traçabilité pour la téléphonie semblable et complémentaire à la politique de sécurité Data.

Par ailleurs, CheckPhone lance la version 2.0 de sa suite ETSS pour élargir son périmètre de protection aux communications téléphoniques sur IP avec la toute nouvelle version 2.0 de sa suite de sécurité téléphonique.

La solution intègre la dimension IP et gère la sécurité des systèmes téléphoniques convergents (traditionnel TDM & IP). La suite logicielle se présente comme un outil idéal d'accompagnement des entreprises qui souhaitent migrer vers les technologies IP sans remettre en question la sécurité de leur système d'information.

Elle propose également une gestion centralisée et unifiée de systèmes hétérogènes grâce à ses connecteurs avec les plates-formes d'administration téléphoniques Alcatel et Aastra Matra. D'autres connecteurs et en particulier un connecteur Siemens, seront également disponibles dans les prochains mois.

Les sondes surveillent les flux téléphoniques TDM (T2/T0), mais également SIP. Elles maîtrisent les flux en temps réel (voix, vidéo, fax, data et applicatifs) et prémunissent l'entreprise contre les risques de piratages, écoutes, spam voix, ...

Enfin, la solution a été conçue pour s'insérer dans une infrastructure de sécurité réseau, en coopérant avec le Firewall de l'entreprise. CheckPhone, fondée en février 2005, est un spécialiste de la sécurité de la téléphonie d'entreprise et la téléphonie sur IP.

<http://www.checkphone.com>

## Resilience annonce deux nouvelles applications UTM de Check Point

Resilience Corporation, fabricant de dispositifs de sécurité, annonce l'intégration des nouvelles applications VPN-1 UTM et VPN-1 Power de Check Point Software Technologies à ses plates-formes d'application. La nouvelle solution unifiée de gestion des menaces de Check Point, allie un pare-feu, un détecteur d'intrusion, une passerelle antivirus, un anti-logiciel espion, un pare-feu d'applications Web ainsi qu'une association de sécurité IPSec et des RPV SSL pour une solution entièrement intégrée. Resilience siège à Mountain View, en Californie, et possède des bureaux de vente partout dans le monde.

<http://www.resilience.com>

<http://www.checkpoint.com>

## Portugal Telecom choisit les appliances UTM Netasq pour sa nouvelle offre de services de sécurité

En signant cet accord avec PT Prime, filiale à 100 % de Portugal Telecom, Netasq confirme son positionnement auprès des plus grands opérateurs européens de télécommunication qui souhaitent mettre en place de nouvelles offres de services sécurisées.

Fondé en 1998, Netasq est l'un des principaux constructeurs européens de solutions de sécurité unifiée destinées aux entreprises de toutes tailles : PME-PMI, Grands Comptes et Administrations. La société conçoit et commercialise des appliances associant la technologie de Prévention d'Intrusion en Temps Réel, l'ASQ (« Active Security Qualification ») aux fonctions de pare-feu réseau et applicatif, VPN IPSec et SSL, filtrage de contenu et sécurisation de la VoIP. Véritable innovateur technologique, Netasq offre ainsi toutes les fonctions

de sécurité indispensables, intégrées dans un seul et même boîtier. PT Prime est une société du Groupe PT, un fournisseur de solutions de communication et information employant les technologies les plus récentes et les méthodes les plus efficaces. Créée en 1999, PT Prime est une filiale à 100% de la société Portugal Telecom SGPS.

<http://www.telecom.pt>

<http://www.netasq.com>

## VIE PRIVÉE

---

### **Selon la NSA, l'administration Bush retient des logs de façon illégale**

Selon le quotidien USA Today, l'Agence pour la Sécurité Nationale (NAS) américaine, sous le couvert de l'administration Bush, aurait depuis 2001 surveillé secrètement les appels téléphoniques de plusieurs millions de citoyens. L'Agence conserverait une gigantesque base de données sur la provenance, la destination, la durée des appels... Elle aurait également analysé ces informations dans le but de détecter des activités terroristes après la catastrophe du 11 septembre. Les opérateurs téléphonique AT&T, Verizon et Bellsouth auraient coopéré sans passer par l'autorisation d'un juge. Des révélations qui ne manquent pas d'être contestées par les intéressés.

<http://www.usatoday.com>

### **Inquiétudes sur le plan Wi-fi de la ville de San Francisco**

Des avocats et les activistes de l'inclusion numérique ont sonné l'alarme à propos du service à large bande large sans fil proposé par la ville de San Francisco. Des auditions se déroulent devant des responsables de la ville. La proposition d'un réseau partout dans la ville, faite par Google Inc. et EarthLink inc., donnerait lieu à une invasion de l'intimité des utilisateurs et n'inclut pas de financement pour que la technologie numérique et l'Internet soit accessible aux personnes aux revenus modestes, selon les critiques qui se sont exprimées. Les compagnies sont toujours en pourparlers pour un contrat final avec la ville, et les activistes visent à changer le projet ou à le faire adopter comme un réseau municipal appartenant à la ville. La ville a passé l'année dernière un appel d'offres pour un réseau sans fil qui atteindrait la majeure partie de la ville pour extérieur et pour un certain usage d'intérieur. La réponse de Google et d'EarthLink est fondée sur un réseau financé par la publicité locale et un service payant plus rapide. Des inquiétudes sur la vie privée des particuliers ont été soulevées depuis l'année dernière par American Civil Liberties Union de Northern California, Electronic Frontier Foundation et le Electronic Privacy Information Center, qui affirment que leurs préoccupations n'ont pas été calmées par le choix de la ville en faveur de Google et d'EarthLink. Le plan de ces deux sociétés a été mal noté sur ces aspects d'«electronic privacy», d'autant que les utilisateurs du service libre Wi-Fi devront donner une adresse e-mail et un signe pour chaque session, ce qui permettrait à Google et à EarthLink de suivre différents utilisateurs dans le temps. Google s'est seulement engagé à garder l'information sur les utilisateurs pour 180 jours ou moins, mais pas EarthLink selon eux.

<http://www.earthlink.net>

## VIRUS

---

### **F-Secure propose une protection antivirale pour la plate-forme S60 3ème édition**

F-Secure Mobile Anti-Virus supporte désormais la plate-forme S60 3ème édition, la dernière génération la plus utilisée dans le monde sur les smartphones. S60 est une plate-forme ouverte pour les développeurs et le système d'exploitation Symbian OS 9.1. Le logiciel supporte 27 langues. Il est tout d'abord disponible pour les nouveaux N-Series Nokia mobile et nouveaux terminaux Nokia E-Series. F-Secure Mobile Anti-Virus sera livré par défaut avec les Nokia N71 et N80. Pour les terminaux Nokia E60, E61

et E70, le client antivirus sera téléchargeable via le catalogue Nokia. Elle sera également disponible pour les réseaux de distribution professionnels et pour le grand public sous forme de boîtes disponibles en italien, Finlandais et Anglais. Fondée en 1988, la société siège à Helsinki (Finlande) et elle possède des filiales dans le monde.

<http://www.f-secure.fr>

## **Selon McAfee SiteAdvisor, la plupart des internautes ne reconnaissent pas les sites distribuant des spywares**

McAfee SiteAdvisor, un pionnier de la sécurisation du Web, teste et classe presque tous les sites visités sur Internet. Il met en garde tous ceux qui pensent qu'un site est sûr s'il «présente bien» et comporte des annonceurs nationaux en page d'accueil. Selon le premier Spyware Quiz conduit par SiteAdvisor, 97 % des utilisateurs d'Internet risquent au prochain clic d'infecter leur PC par des spywares, adwares ou autres programmes indésirables. Bien que la menace du spyware ait été largement exposée dans la presse, à peine 3 % des 14.000 personnes ont parfaitement répondu au questionnaire Spyware Quiz de SiteAdvisor.

Le questionnaire demandait aux internautes d'indiquer les sites sûrs parmi un certain nombre de catégories très populaires. Les pages présentées sont issues des trois millions de sites testés et évalués indépendamment par SiteAdvisor, en fonction de menaces telles que les spywares et les spams. Parmi les résultats les plus inquiétants : dans leur grande majorité (65 %), les internautes auraient contracté de nombreux adwares et/ou spywares ; la présence d'annonceurs nationaux et une présentation claire incitent à faire confiance au site ; même les internautes avertis sont quasiment assurés de consulter un site dangereux au cours d'une trentaine de jours de navigation et de recherches en ligne ; souvent, l'utilisateur ne voit pas les mentions en « petits caractères », qui permettent au site d'installer « légalement » des logiciels indésirables.

Les sites testés représentent des catégories comme les économiseurs d'écran, les smileys (animations ludiques), les jeux gratuits, les paroles de chansons et le partage de fichiers, toutes bien connues pour contenir spywares, adwares et autres programmes indésirables. Le questionnaire a été conçu pour déterminer la capacité des internautes à distinguer visuellement les sites susceptibles d'envoyer des logiciels non sollicités.

Pourcentage d'internautes capables de déterminer la sûreté d'un site de paroles de chansons, 28 %; de partage de fichiers, 59 %; d'économiseurs d'écran, 62 %; de jeux gratuits, 68 %; de smileys, 75 %.

<http://www.mcafee.fr>

## **McAfee propose une protection antivirus pour les ordinateurs Apple à processeurs Intel**

McAfee annonce (enfin) un antivirus pour les ordinateurs Apple à processeurs Intel. Baptisée McAfee VirusScan for Mactel 8.0, la solution fonctionne sous l'émulateur Rosetta d'Apple et protège les ordinateurs Apple contre les virus, chevaux de Troie et autres menaces Macintosh et Windows.

Selon McAfee Avert Labs, les vulnérabilités découvertes pour la plate-forme Macintosh ont augmenté de plus de 228 % depuis 2003, notamment à cause du succès croissant des produits grand public de la marque, comme l'iPod et le service iTunes. Bien que le système d'exploitation Mac OS X reste plus sûr que les plates-formes Windows, la découverte croissante de vulnérabilités critiques impose une approche plus dynamique de la sécurisation, notamment dans les environnements hétérogènes.

McAfee VirusScan for Mactel est conçu pour éliminer ces menaces en détectant, bloquant et nettoyant les e-mails et les pièces jointes infectés. La mise au point de cette solution est une initiative à saluer. En effet, Apple reste dans un univers très fermé. Cette ouverture à la communauté informatique est donc un pas en avant important. La solution s'appuie sur le moteur d'analyse de l'éditeur pour assurer une protection complète des Macintosh au niveau des accès, en arrêtant les virus et autres menaces, y compris celles qui se cachent dans les archives et les fichiers compressés. L'administration est centralisée par McAfee ePolicy Orchestrator 3.5 et 3.6 (ePO), qui gère toutes les solutions de sécurité de McAfee depuis une même interface.

<http://www.mcafee.fr>

<http://www.apple.com>

<http://www.intel.com>

## Un virus diffuse sur internet les plans secrets d'une centrale électrique japonaise

Selon les médias japonais, des données sensibles concernant la sécurité d'une centrale thermoélectrique de la compagnie Chubu Electric Power sont apparues sur internet à la suite d'une infection virale. Le virus aurait diffusé des documents portant sur les mesures de sécurité de la centrale, les noms et les adresses du personnel et d'autres informations critiques via le logiciel de partage de fichiers Share. L'incident s'est produit alors qu'un employé de 40 ans du département sécurité avait installé en mars le programme sur son ordinateur. Un problème similaire est déjà survenu il y a 4 mois dans la même société cette fois avec le logiciel de partage de fichiers Winny. Ce problème est le dernier d'une série de cas similaires survenus récemment au Japon.

<http://www.japantimes.co.jp>

## La sécurité préventive ? Plus que jamais, une nécessité pour les entreprises

Dans le cadre de la première édition des Matinales Sécurité Informatique, une manifestation organisée par la *Lettre Sécurité Informatique*, en partenariat avec l'agence de conseil en communication MP Conseil, trois acteurs de référence (Trend Micro, PointSec, HSC) ont débattu avec un parterre composé de responsables de la sécurité informatique au sein de grandes entreprises. Fil rouge des travaux: la sécurité «préemptive» ou préventive. En ligne de mire: un défi en forme d'interrogation : est-il vraiment possible de détecter suffisamment en amont l'irruption des menaces connues ... et inconnues et y répondre efficacement? Synthèse des propos clés.



Hervé Schauer

Toute la communauté de la sécurité informatique en convient: aujourd'hui, réagir aux événements susceptibles d'affecter le bon fonctionnement des systèmes informatiques ne suffit plus. Pour se prémunir réellement, il faut pouvoir intervenir en amont. Alors, sans verser dans l'informatique-fiction, les entreprises cherchent à savoir s'il est possible, ou non, de déployer des stratégies réellement préventives.

«Déterminer les menaces inconnues d'après les menaces connues est un exercice évidemment difficile mais absolument indispensable si on ne veut plus se limiter à réagir simplement à ce qui survient au jour le jour, résume Renaud Lafay, ingénieur avant-vente chez Trend Micro. En particulier, les menaces inconnues ne contiennent pas de fichiers de signature alors que le taux élevé de faux positif limite l'utilisation des solutions IPS. Pour faire une analogie, la meilleure parade, aujourd'hui encore, est de procéder un peu comme pour la protection d'une maison». Autrement dit, le système d'information à sécuriser doit être assorti d'une série de dispositifs de détection et de surveillance. Objectif: identifier et prendre en compte tout événement anormal. «Les approches de NCIT (Network content inspection technology) que nous prônons, détectent en temps réel la première apparition d'une menace, connue ou non, en utilisant plusieurs méthodes, notamment la corrélation du trafic sur les couches 2 à 7 du SI. L'objectif est, à terme, de fournir à l'entreprise une vue d'ensemble des menaces, au travers d'un point de contrôle unique», précise-t-il encore.

### SÉCURITÉ INFORMATIQUE

est éditée par PUBLI-NEWS S.A.

47, rue Aristide Briand

92300 Levallois-Perret

Tél : 01 41 49 93 60

Fax : 01 47 57 37 25

Email : [i.lancry@publi-news.fr](mailto:i.lancry@publi-news.fr)

Site Internet : [www.publi-news.fr](http://www.publi-news.fr)

Commission paritaire n°0209 I 84348

SIREN : 330 394 834

Tarif : 633 € TTC

(TVA 2,1% pour la France)

Étranger : 619,98 € HT

22 numéros par an

DIRECTEUR DE LA PUBLICATION/

RÉDACTEUR EN CHEF

Ange Galula

RÉDACTEUR EN CHEF ADJOINT

Gilles Prod'homme

RÉDACTION

Karine Ascer

MAQUETTE : Pascal Soulier

Amandine Kacher

Contact : 01.41.49.93.67

Fax rédaction : 01.41.49.93.71

E-mail:

[ange.galula@publi-news.fr](mailto:ange.galula@publi-news.fr)

Copyright : **Sécurité Informatique** ne peut être reproduit ou transmis en totalité ou en partie qu'avec l'accord préalable et écrit de la société éditrice Publi-News.



Mikaël Taillepiéd

## Déterminer le niveau de «risque acceptable»

Reste bien sûr à évaluer le niveau de risque acceptable ou pas, dans la mesure où, une entreprise doit tenir compte des coûts liés à la sécurité informatique. «Dans les approches préventives, le but poursuivi est de bloquer efficacement les attaques les plus dangereuses sans pour autant mettre en cause le fonctionnement des processus opérationnels de l'entreprise, remarque encore R. Lafay. Lorsqu'elle traite avec ses prestataires et ses offreurs de solutions, l'entreprise doit donc d'abord déterminer où elle veut placer le curseur de sa protection informatique, bref, se donner des priorités». Cette exigence s'applique à toute l'infrastructure informatique existante jusqu'aux terminaux nomades, toujours plus nombreux et diversifiés. D'où l'intérêt du point de vue de Mikaël Taillepiéd, directeur général pour la France, l'Espagne et le Portugal de PointSec, éditeur d'origine suédoise spécialisé dans le développement de logiciels de chiffrement pour la protection des données contenues dans les ordinateurs portables, les PDA et autres smartphones : «Nous nous concentrons sur la sécurisation des données et des informations sensibles elles-mêmes. Car aujourd'hui, la protection du capital d'information est cruciale pour une entreprise, spécialement dans les secteurs comme la banque, la finance ou l'assurance».

## Coûts directs à court terme et indirects à long terme

Selon le responsable PointSec les données mobiles peuvent être sécurisées à travers un plan de sécurité en cinq points: police de sécurité, VPN et firewall personnel, antivirus et antimalware, contrôle d'accès et authentification forte, chiffrement des données. Des procédures trop lourdes et dispendieuses ? «Les coûts liés à la perte d'un appareil non protégés sont quantifiables et atteignent rapidement des niveaux importants dans un grand, rétorque M. Taillepiéd. Mais ce que les entreprises mesurent souvent très mal, c'est le niveau de coût en termes d'impact sur leur image. Très vite, il ne s'agit plus de sommes exprimées en euros mais en perte de confiance de la part des clients ou des partenaires. Les conséquences peuvent être parfois très graves pour l'entreprise». Exemple-type: les banques victimes d'attaques phishing et autres intrusions virales qui se voient contraintes de dépenser des millions d'euros en communication (des encarts publicitaires jusqu'aux plates-formes d'appels en passant par la

### Beaucoup de données très sensibles sur les PDA

Appareils hautement technologiques dotés de nombreuses fonctionnalités, les PDA sont souvent utilisés comme des espaces contenant des informations presque trop sensibles. Plus gravement, les informations «perso/pro» sont abondantes. Une meilleure sécurité préventive passe d'abord par une hiérarchisation rationnelle des données à faire figurer... ou pas. Bref, faire main basse sur le PDA d'un manager c'est ouvrir une brèche dangereuse dans son identité technologique, informatique et privée.

**Noms et adresses personnels** : 86 %

**Noms et adresses professionnels** : 81 %

**Agenda professionnel** : 59 %

**Agenda personnel** : 55 %

**Réception et lecture de mails** : 45 %

**Multimédia** : 37 %

**Mots de passe et codes PIN** : 37 %

**Photo personnelles** : 33 %

**Données d'entreprise** : 27 %

**Détails bancaires** : 15 %

Source: PointSec

mise en place de cellules de crise) pour rassurer leurs clients, professionnels ou particuliers. Le lien de fidélité long et coûteux à tisser, peut se rompre à l'occasion de dysfonctionnements informatiques répétés. Le «préemptif» a des incidences bien concrètes sur l'activité même de l'entreprise. Un terme qu'Hervé Schauer, directeur du cabinet de conseil et d'expertise en SSI Hervé Schauer Consultants, reprend pour l'élargir: «Au-delà des effets de modes, l'anglicisme 'préemptif' traduit la volonté des entreprises de mieux intégrer la prévention d'intrusion et en particulier de combiner plus efficacement l'analyse approfondie de la détection d'intrusions avec la capacité de bloquer des pare-feux qu'elles ont déployés. L'action préventive vise en fait à éliminer une situation indésirable potentielle alors que l'action corrective cherche à éliminer une situation

*indésirable détectée*». Voilà pour le principe général à ne pas perdre de vue. A partir de là, au-delà de la «techno» pure, il y a des choix à faire: les PC PDA, téléphone sont-ils ou non sous la maîtrise/responsabilité de l'entreprise, qui administre quoi et selon quelles procédures, quid de la formation des utilisateurs et de l'implication du top management dans la politique de sécurité ? On pourrait multiplier les paramètres à superviser.

## Attention à la porosité de la frontière perso/pro

Dans la foulée, H. Schauer rappelle à juste titre que dans l'administration judiciaire, beaucoup de magistrats utilisent leur PC personnel pour travailler et y déposent, par la force des choses, des informations particulièrement sensibles. On imagine alors les dégâts en cas de perte ou de vol du matériel, sans parler des tentatives de piratage. Qu'on l'appelle «préemptive» ou simplement préventive, la détection/prévention et des attaques et des intrusions n'a pas fini d'alimenter les discussions et les missions de mise à niveau des systèmes d'information.

<http://fr.trendmicro-europe.com>

<http://pointsec.fr>

<http://www.hsc.fr>

Gilles PROD'HOMME

## GESTION DES VULNERABILITES

### ISS dévoile son prototype SWIPS de prévention des intrusions

Internet Security Systems (ISS) a présenté à l'occasion du salon Networld Interop de Las Vegas un prototype opérationnel de sa nouvelle technologie SWIPS (Switch enabled Intrusion Prevention System). Résultat d'un partenariat de recherche et développement avec Extreme Networks. Cet outil intègre des technologies de prévention des intrusions au niveau des commutateurs de dorsale des cœurs de réseau d'entreprises ou des réseaux d'opérateurs. Il bloque aussi les menaces connues ou inconnues lorsque celles-ci ont franchi les défenses extérieures du réseau, réduisant ainsi le risque de propagation à l'échelle de toute une entreprise. Cette technologie inspecte le trafic à vitesse filaire à la recherche de fragments de codes malveillants. Le prototype a démontré sa capacité à analyser le trafic à la vitesse de 100 Gbit/s, à le comparer au débit moyen de traitement d'un système IPS, de 2 à 6 Gbit/s. Ce résultat est obtenu par la réduction du temps de latence de l'analyse IPS. Ainsi, le temps de latence est divisé par 10, à moins de 100 microsecondes. L'intégration des fonctions d'analyse et de routage est réalisée dans les deux sens. Les nouvelles communications sont identifiées au niveau du commutateur et transmises pour analyse à l'IPS, au moyen d'une interface applicative optimisée (API). En retour, la technologie SWIPS participe à l'exécution des tâches de routage.

<http://www.iss.net>

### Cinq ans de prison pour Jeanson Ancheta, le pirate aux 400.000 PC zombies

Selon le FBI, l'Américain Jeanson Ancheta, 21 ans, a été condamné à 57 mois de prison suivis de 3 ans de liberté surveillée pour avoir profité de quelque 400.000 PC zombies rassemblés en réseaux «botnets». Ces machines, initialement infectées par un ver informatique ou un cheval de Troie, et assemblées ensuite en réseaux commandés à distance peuvent être exploitées pour l'expédition massive de pourriels ou le lancement d'attaques paralysant les sites web. Opérant sous le pseudo Botz4Sale, son réseau comptait même des machines localisées dans la division de l'armement de la marine américaine de China Lake ainsi que des machines provenant du département de la Défense. Une véritable humiliation pour les militaires ! Moyennant rémunération, il mettait son système au service d'autres cyber criminels pour propager plus rapidement virus, spams e publicités en masse... Un commerce juteux pour ce jeune homme issu d'une banlieue de Los Angeles. Il a, en effet, reconnu avoir perçu plus de 100.000 \$ en vendant ses services. Malgré la peine la plus lourde jamais prononcée contre un pirate informatique, il devra également s'acquitter d'une amende de 15.000 \$ aux organisations militaires américaines. Son matériel informatique, 60.000 \$ et une BMW lui ont aussi été confisqués.

<http://www.fbi.gov>

## BIOMÉTRIE

---

### **Extensity France annonce la disponibilité d'un nouveau module : Anael biométrie**

Ce lancement fait suite à l'annonce d'un partenariat conclu début 2005 entre Extensity (ex Geac), éditeur de solutions de gestion de performance d'entreprise, et Micro-Host, distributeur exclusif en France du programme de contrôle d'accès physique et logique ARS développé par la société Cameon.

La biométrie, qui repose sur deux catégories de technologies (les techniques d'analyse du comportement et les techniques d'analyse de la morphologie humaine) présente des avantages par rapport au mot de passe ou à la clé matériel. D'une part, rien ne peut être perdu et d'autre part, elle garantit que la personne qui se connecte à distance est bien la bonne personne. ARS, qui est au cœur d'Anael biométrie, est un programme de contrôle d'accès sécurisé, physique ou logique, avec authentification forte par capteurs biométriques. Cette offre est composée d'une interface de contrôle utilisant la biométrie et reliée à un serveur web ou à une application métier, d'un terminal (PC ou PDA) intégrant un capteur d'empreintes digitales et/ou un lecteur de carte à puce, ainsi que d'un serveur ARS qui stocke une partie des informations d'authentification et qui gère le protocole de sécurisation du poste et du terminal client.

Le programme ARS suit les recommandations de la CNIL pour le traitement des informations nominatives : pas de base de données centralisée d'empreintes digitales. L'utilisateur garde la référence de son empreinte digitale sur son média de stockage local : disque dur, disquette, clé USB...

Extensity compte plus de 1.100 collaborateurs répartis dans 42 bureaux à travers le monde.

<http://www.extensity.fr>

### **Axalto fournit les puces biométriques des cartes d'identités nationales au Qatar**

Axalto, fournisseur mondial de cartes à microprocesseur, annonce sa participation au programme de cartes d'identité électroniques au Qatar. L'entreprise livrera des cartes basées sur la technologie match-on card pour l'identification biométrique par empreinte digitale, ainsi que les lecteurs et services associés. Les Qataris utiliseront ces cartes, qui combinent biométrie, technologies avec et sans contact - comme pièce d'identité officielle à compter du premier trimestre 2007. Elle sera délivrée aux citoyens de plus de seize ans ainsi qu'aux résidents étrangers du pays. Outre les données individuelles qui figurent sur les pièces d'identité classiques (nom, date de naissance, adresse, etc.), le microprocesseur stockera également l'empreinte digitale du titulaire. Les données biométriques restent sur la puce et ne quittent jamais la carte, même lorsque celle-ci est en cours de vérification, respectant ainsi la vie privée du titulaire. Les fonctions de sécurité embarquées dans sa carte offriront au titulaire la possibilité d'accéder aux services d'administration électronique et d'effectuer des transactions sécurisées. Grâce à un lecteur de cartes Axalto connecté à leur ordinateur personnel, ils pourront utiliser leur carte d'identité pour déclarer leur employé(e) à domicile, effectuer leur changement d'adresse, obtenir des certificats administratifs, etc. Axalto emploie 4.500 personnes de plus de 65 nationalités différentes. L'entreprise a vendu plus de 3 milliards de cartes à ce jour.

<http://www.axalto.com>

## PIRATAGE

---

### **Des clients du restaurant Courtepaille victimes d'escroquerie à la carte bancaire**

Mardi dernier, la police d'Orléans a révélé qu'une quinzaine de personnes, ayant mangé dans le restaurant de la chaîne Courtepaille situé près d'Orléans dans le Loiret, entre la fin avril et le début mai, auraient été victimes de retraits frauduleux à la carte bancaire. La chaîne de restauration aurait subi le piratage de son

système de transmission bancaire informatique. Les pirates non identifiés auraient accédé aux numéros de cartes bancaires des clients et procédé à des achats et retraits réguliers d'environ 500 €, à partir de la Roumanie ou de l'Espagne. Le nombre total de victimes reste encore inconnu mais la fraude concernerait entre 5 et 10 restaurants sur les 170 que compte le restaurateur en France.

<http://www.courtepaille.com>

## Un fonctionnaire fédéral américain condamné pour avoir pénétré le PC d'un supérieur

Un juge fédéral a condamné un ancien employé à cinq mois de prison ferme et à cinq mois d'assignation à résidence, pour avoir piraté l'ordinateur d'un surveillant au ministère de l'éducation, indique le 18 mai le site web Business Legal Reports. Kenneth Kwak, 34 ans, de Chantilly, en Virginie, avait avoué s'être rendu coupable d'avoir gagné intentionnellement un accès non autorisé à un ordinateur de gouvernement et d'y obtenir de l'information. Dans sa réclamation, Kwak, qui avait travaillé dans un bureau en charge de la sécurité du département des systèmes informatiques de l'éducation, a admis qu'il avait placé l'ordinateur sous surveillance pour y accéder à volonté. Il avait partagé les informations qu'il y avait trouvées avec d'autres personnes du bureau.

<http://blr.com>

### A nos lecteurs

Des informations supplémentaires sur l'actualité des offreurs de solutions de sécurité informatique sont accessibles en ligne. Pour y accéder, connectez-vous sur le site [www.publi-news.fr](http://www.publi-news.fr) puis consultez le fil quotidien d'informations, **PUBLINET**, rubrique **Sécurité**.

## BULLETIN D'ABONNEMENT

A faxer au 01.47.57.37.25

ou à retourner à Publi-News 47, rue Aristide Briand 92300 Levallois Perret – Tél 01.41.49.93.60

- Oui, je m'abonne à **SÉCURITÉ INFORMATIQUE** électronique pour 1 an, 633 € TTC (TVA 2,1% pour la France) - Étranger : 619,98 € HT
- Ci-joint mon règlement par chèque à l'ordre de Publi-News
- Je réglerai à réception de facture
- Je règle par carte bancaire :  Visa
- MasterCard N° \_\_\_\_\_ Date de Validité \_\_\_\_\_

Cachet de l'entreprise :

Signature :

Société .....  
Nom ..... Prénom ..... Fonction .....  
Adresse .....  
Code Postal ..... Ville ..... Pays .....  
Tél ..... Fax ..... e-mail : .....