

SECURITY

hors l'IT, point de salut?

En-dehors de la protection des données des entreprises, des applications et des infrastructures de réseaux, l'IT s'intègre peu à peu aux pratiques des sociétés de gardiennage traditionnelles et des forces de l'ordre chargées d'orchestrer la sécurité de grands événements sportifs, comme vous le découvrirez dans notre dossier. Par ailleurs, nous ouvrons largement nos colonnes aux avis de professionnels de la question pour parler également d'outsourcing, des tendances, des technologies, etc.

Sommaire

- 2** Tendances: la détection d'intrusion n'est plus ce qu'elle était...
- 4** Suivez le guide avec PricewaterhouseCoopers
- 5** Menace interne: quand l'administrateur IT pète les plombs, gare à la casse!
- 6** Comment les sociétés de gardiennage traditionnelles envisagent-elles l'IT?
- 8** Sécurité des Jeux Olympiques d'Athènes: 250 millions d'euros pour l'infrastructure
- 9** Selon Cisco, les réseaux devraient apprendre le self-defense.
- 10** L'outsourcing de la sécurité: un tour d'horizon.
- 13** Interviews: parole donnée à une douzaine de spécialistes de la sécurité sur les thèmes chauds de l'actualité.
- 19** Trusted Solaris: la prochaine version blindée de l'OS de Sun devrait apparaître l'an prochain.
- 20** Grâce à de nouvelles technologies, Checkpoint veut parer l'érosion de son statut de leader du marché des pare-feux.
- 31** Caller ID: Microsoft part à la pêche aux spams.
- 32** Focus: comment minimiser les chances qu'un spyware s'installe sur votre machine?

Second souffle pour la lutte contre

Face aux critiques, les éditeurs de systèmes de détection des intrusions (IDS) se sont remis en cause. La prévention passe désormais de l'observation passive au blocage actif.

Depuis quelques années, le secteur de la sécurité devient de plus en plus complexe. Pourtant, l'objectif reste toujours le même : protéger son réseau, ses données et ses applications. Mais dès que la parade est trouvée pour un certain type d'attaque, un éditeur spécialisé s'empresse de montrer du doigt une nouvelle faiblesse du réseau qui lui permet de proposer un nouveau médicament.

Pour poursuivre cette métaphore pharmaceutique, les solutions sont aujourd'hui tellement nombreuses que l'on pourrait se demander si dans la liste ne figurent pas quelques placebos! L'année 2003 a, sans conteste, trouvé le sien: la sonde d'intrusions, ou IDS. Ce produit a été conçu pour observer l'activité du réseau et découvrir les éventuelles tentatives d'intrusions d'utilisateurs malveillants ou de programmes préenregistrés sur le réseau. Sauf que bon nombre de sociétés qui se sont équipées d'outils de ce type ont eu, un moment, le sentiment d'être invulnérables, avant de se rendre compte qu'il leur manquait l'armée de spécialistes nécessaire pour les administrer. "Plusieurs de nos clients qui ont acheté des sondes ne les utilisent pas", souligne Nicolas Quint, directeur technique de l'intégrateur Qualiope, spécialisé dans la sécurité. "Un IDS ne vaut pas le coup d'être acheté... La notion même d'IDS est une erreur de l'histoire", affirmait même une étude de Gartner publiée en juin dernier.

Etude qui a provoqué un tollé chez les constructeurs et qui suscite depuis des interrogations de toute part. Notamment parce qu'elle est allée jusqu'à annoncer la disparition pure et simple des sondes d'intrusions d'ici à 2005. Aux États-Unis, la chose a tellement été prise au sérieux que le Pentagone a convoqué en juillet analystes du bureau d'études et éditeurs d'IDS pour s'expliquer.

Mais même si l'on considère que les éditeurs sont de mauvais élèves et que les sondes d'intrusions sont inopérantes, ce qui reste discutable et discuté, l'entreprise peut-elle ignorer que son réseau est vulnérable au-delà du pare-feu ? Non, répondent bien sûr les éditeurs qui entendent répondre aux lacunes des IDS grâce à de nouvelles solutions baptisées IPS (pour Intrusion Prevention System). En modifiant une lettre du premier concept, ces professionnels de la rhétorique tentent sans doute tout simplement de rhabiller leurs produits, mais ils montrent toutefois qu'ils ont désormais compris les exigences des utilisateurs: disposer d'outils opérationnels.

Automatiser le principe de réponse aux alertes

Deuxième enjeu pour les IPS: passer de la détection passive au blocage actif et automatiser le principe de réponse aux alertes. Mais les

les intrusions

responsables sécurité rechignent souvent à cette opération car ils craignent que le trafic légitime soit arrêté ou même que leur réseau soit entièrement paralysé si les IPS se trompent. Les éditeurs, qui se doivent d'être convaincant, disposent alors d'un argument massue : l'importance de la réponse en temps réel, impossible à effectuer manuellement. Chez le fabricant de pare-feu Netasq, on juge que cela est possible dès lors que l'on définit "les types d'attaques contre lesquelles on souhaite se protéger, car il est impossible de toutes les prévoir". Même son de cloche chez le leader des sondes d'intrusions ISS, dont l'IPS combine deux outils : un IDS et un scanner de vulnérabilité de l'autre. Alertes et failles sont ainsi corrélées pour ne réagir que quand le danger est avéré. Si par exemple le ver Slammer entre sur le réseau et qu'il n'y a aucun serveur SQL, ou s'ils sont tous protégés par un correctif logiciel, il n'est pas indispensable de le bloquer. A l'opposé, si une vulnérabilité a été établie, il faut agir en temps réel pour éradiquer le ver.

Agir est d'ailleurs le troisième et dernier enjeu des IPS. Une sonde détectant une requête anormale doit être capable de la bloquer, de mettre un fichier en quarantaine... ce qui veut dire que l'IPS doit apprendre à communiquer avec d'autres produits de sécurité. Chez ISS, on se prévaut de pouvoir reconfigurer des pare-feu Check Point, mais aussi Netscreen, Watchguard ou Cisco. Toutefois, de plus en plus de fournisseurs, comme Symantec ou Netasq, gèrent tous les maillons de la chaîne et proposent des IPS en mode coupure. Ces produits ne deviennent-ils pas alors de simples pare-feu applicatifs ? C'est ce que demandent bon nombre d'analystes du Burton Group ou de Gartner, pour qui l'IPS n'est "qu'un mot pour faire du pare-feu au niveau applicatif et utiliser des signatures dans le filtrage", comme le dit Hervé Schauer, PDG d'Hervé Schauer Consulting.

Si 2003 restera sans conteste comme l'année de l'enterrement en règle de l'IDS, il serait donc un peu prématuré de couronner son successeur. L'IPS devra faire ses preuves et quelques sociétés préféreront sans doute garder encore quelque temps des IDS plus ou moins rhabillés qui ne servent peut-être pas à grand-chose, mais qui n'ont pas encore de remplaçant crédible.

Les pare-feu à l'assaut de la couche applicative

Si un pare-feu ferme un port applicatif, au niveau de la couche transport, il peut empêcher certaines applications de passer et risque de paralyser l'activité de l'entreprise ! Cette simple tautologie a longtemps constitué un véritable casse-tête pour les éditeurs, jusqu'à ce qu'ils découvrent les vertus de la notion de pare-feu applicatif (certains ont mis plus longtemps que d'autres, railleront d'ailleurs les Français Arkoon et Netasq).

Pour arrêter les vers informatiques tels que Code Red, Nimda et autres Slammer, bon nombre d'acteurs s'y sont ralliés en 2003. A l'instar de Check Point avec une nouvelle mouture de son logiciel phare FireWall-1, plusieurs pare-feu se veulent désormais en mesure de bloquer les attaques qui font le plus de dégâts en vérifiant dans les paquets, au niveau applicatif, la cohérence des en-têtes HTTP, H.323, SQL, Soap, CIFS... ou bien en repérant les attaques fragmentées. Sans toutefois aller jusqu'à l'inspection en profondeur des contenus comme le filtrage des codes ActiveX ou Javascript, ou la recherche systématique de chevaux de Troie, chasse gardée des boucliers applicatifs. □



La gamme de consoles de sécurité Proventia d'Internet Security Systems: un exemple parmi d'autres de l'évolution du marché de la détection d'intrusions.

Sécurité:

suivez le guide avec PricewaterhouseCoopers!



Selon la société de consultance PricewaterhouseCoopers, «une bonne sécurisation de l'information est un processus dynamique, pleinement intégré dans d'autres processus d'entreprise.» La sécurisation doit «non seulement offrir une protection contre les risques inhérents (virus, panne de réseau, fuite d'informations confidentielles,...), mais également offrir de nouvelles opportunités de créer de la valeur ajoutée». Et chez PwC, on sait de quoi parle puisque "Information Security: a strategic guide for business", la nouvelle livraison de la série Technology Forecast, traite justement de cette problématique.

Une lecture recommandée

Explicitement dédié aux décideurs des entreprises, ce nouveau volume de près de 300 pages offre un tour d'horizon complet, depuis la définition d'une politique cohérente de sécurité, pour laquelle PwC fournit un tableau de bord, jusqu'aux différentes technologies impliquées (identity management, antivirus, firewall, IDS, etc.) et à un profil de toutes les sociétés actives dans le secteur (en termes d'offres, s'entend, il n'y a pas de classement ou de tests comparatifs). Ce récent volume ne déroge pas aux standards de qualité de la série qui l'ont établie comme une référence incontestable: il fournit une présentation claire des défis et des différentes technologies concernées, dans un langage abordable par tous (enfin presque...), le tout assorti d'un index qui permettra aux ignorants ou aux distraits de percer la signification des acronymes les plus retors. Bien sûr, l'accent porte souvent sur des questions qui concernent avant tout les grandes entreprises internationales, mais l'ouvrage constitue sans conteste un outil suffisamment pédagogique pour justifier sa lecture par les responsables d'entreprise de plus petite taille.

Meilleure intégration de la sécurité

Selon PwC, la mise en œuvre de politiques de sécurité uniformes au sein de l'ensemble de l'entreprise continuera à être handicapée par la

logique des silos où chaque département adopte des solutions ad hoc ponctuelles. Ceci s'applique notamment à des questions telles que le contrôle d'accès et l'identity management. De même, la tendance à l'outsourcing de processus ou d'applications dans le but de réduire les coûts devrait également réduire la capacité des entreprises à déployer des solutions de sécurité uniformes. En parallèle, notons également que lorsque PwC parle de la possibilité de créer de la valeur ajoutée dans le domaine de la sécurité, c'est surtout en référence au contrôle d'accès, aux répertoires d'entreprises, à la gestion des identités et des utilisateurs, domaines pour lesquels l'optimisation des processus se traduira normalement par une compression des coûts et, idéalement, une plus grande efficacité de l'IT au bénéfice des objectifs purement business. Par ailleurs, la nécessité de mettre en œuvre un patching efficace des applications devrait mener à une meilleure intégration avec les outils de gestion et de configuration des actifs IT.

Moins de cuirasse

Sur le plan des infrastructures de sécurité, PwC estime que la protection des réseaux des entreprises sera plus élastique qu'elle ne l'est aujourd'hui. En effet, dans la mesure où de plus en plus d'application exigent l'ouverture de ports sur le firewall, les mesures de surveillance et de défense devront être implémentées de plus en plus profondément au sein des réseaux des entreprises et ne pourront plus fonctionner sur le seul principe de la cuirasse externe incassable. A terme, cela devrait militer pour la poursuite de la croissance des IDS ou de leur proche descendance (parfois baptisée IPS pour Intrusion Prevention System). Dans ce cadre, les consoles de sécurité qui regroupent en une boîte des fonctionnalités aujourd'hui assurées par des technologies distinctes devraient être adoptées plus largement, notamment parce qu'elles pourront à terme fournir une solution de centralisation de la gestion de la sécurité.

ERIC MAHIEU

Gare aux brebis galeuses!

Alors que l'armée américaine renforce les défenses de ses réseaux pour contenir les attaques émanant d'Etats ennemis ou de groupes terroristes, d'aucuns assurent que la menace la plus insidieuse émane de l'intérieur des organisations

Lors du Forum on Information Warfare, qui s'est tenu en décembre à Washington, des chercheurs du FBI et la George Washington University ont mis l'accent sur la "menace interne". Les administrateurs de systèmes, en particulier, sont de plus en plus souvent considérés comme la menace interne potentiellement la plus dangereuse – et une cause de souci pour les militaires – à cause du pouvoir qu'ils exercent sur les réseaux.

Dans sa présentation, le lieutenant-général Kenneth Minihan, l'ancien directeur de la NSA (National Security Agency) a comparé les administrateurs de systèmes d'aujourd'hui avec les spécialistes du cryptage des guerres passées qui dévoilaient les codes ennemis. Il a affirmé que ces administrateurs devraient faire l'objet de plus d'attention de la part des militaires et qu'ils devraient être mieux payés.

Le FBI et les chercheurs de la George Washington University ont étudié les cas d'usage criminel d'ordinateurs, y compris en interviewant des prisonniers. «L'administrateur responsable de l'élaboration des systèmes informatiques a une extraordinaire capacité à causer des dommages», a ainsi affirmé Jerrold Post, professeur de psychiatrie et de psychologie politique au sein de l'université

George Washington. Post a remarqué que les internes qui commettent des crimes informatiques, tels que la fraude, l'extorsion, le sabotage et l'espionnage, le font pour une diversité de motivations, qui comprennent la vengeance et l'enrichissement personnel. Il a affirmé qu'il est critique de comprendre la psychologie des administrateurs IT en général pour identifier les signes d'un danger possible.

«Les introvertis figurent largement parmi les spécialistes IT; ils intériorisent le stress et ne s'expriment qu'en ligne», a-t-il expliqué. Une enquête menée à propos des "des déviants" IT a révélé qu'ils partagent typiquement certains traits de personnalité (voir encadré).

Post a déclaré qu'une analyse poussée de l'histoire de travail d'administrateurs IT coupables d'avoir saboté le réseau de leur employeur ou d'avoir causé d'autres dommages révèle qu'ils commettent souvent des infractions moins graves auparavant comme, par exemple, refuser de réaliser leur backup. Une intervention précoce du management pourrait empêcher que le problème grandisse, parce que les individus introvertis ne cherchent habituellement pas d'aide.

Le FBI a également mené sa propre étude des individus coupables de crimes informatiques, sans nécessairement se focaliser sur les administrateurs IT, en interviewant ceux qui sont détenus en prison, a expliqué John Jarvis, un spécialiste du comportement. «Le cybercrime est principalement un phénomène interne. Un quart seulement peut être considéré comme émanant de l'extérieur.» □

Profil psychologique vraisemblable en cas de menace interne

(Source: George Washington University Political Psychology Program)

- Introverti; vit "en ligne".
- Historique de frustrations significatives vis-à-vis de la famille, du cercle de relations ou des collègues
- Divorce ou problèmes de couple
- Tendance à éprouver de la colère vis-à-vis de l'autorité
- Arrogance, tendance à l'esbroufe masquant un égo fragile
- Attachement extrême à l'infrastructure IT

Sécurité informatique

l'improbable mariage?

Nombre d'experts issus de ces mondes distincts permettent aux entreprises de construire une politique de sécurité globale visant à garantir au mieux la continuité des activités. Et si ces deux sphères n'étaient pas si étanches l'une par rapport à l'autre? Petite revue de leurs connexions présentes et futures...

On peut comprendre que les acteurs spécialisés dans la garantie de l'intégrité physique des personnes, bâtiments et infrastructures, comme le gardiennage ou encore la sécurité électronique, préfèrent clairement ne pas élargir leur champ d'action aux problématiques de sécurité informatique, considérant que ces métiers sont tout à fait distincts, même si liés fortement par la notion de protection. Et vice versa: on imagine difficilement un consultant en sécurité informatique conseiller à la fois son client sur le firewall le plus adéquat, la politique de sécurité la plus adaptée, et mettre en place un système de protection incendie! Et pourtant...

Quand les parallèles se rejoindront

Un acteur tel que Telindus, dont le métier historique concernait l'équipement réseau stricto sensu, a innové au fil des ans en lançant des départements dédiés à la sécurité, mais aussi à la voix et à la vidéo (via la vidéo surveillance digitale, et non plus analogique). Avantage concurrentiel: un seul prestataire peut prendre en charge la sécurité informatique et la surveillance vidéo d'un même client. Yves Vekemans, Business Innovation Manager Security, pointe du doigt une connexion récente entre les deux mondes de la sécurité d'entreprise: «Chaque année, nous organisons un Security Day entièrement consacré à la sécurité réseau. L'année dernière, en raison des événements du 11 septembre 2001, nous l'avons transformé en Security & Safety Day, auquel a pris part notre équipe de vidéo surveillance».

Cette date commence à avoir des répercussions au niveau de l'organisation du personnel, comme l'explique encore Frédéric Dupont, Business Innovation Manager Convergence chez Telindus: «Auparavant, dans chaque entreprise, il y avait un responsable de la sécurité physique et un autre de la sécurité informatique, distincts, avec des profils différents. De plus en plus, on tend vers un concept global de sécurité, et donc vers la mise en place d'un security officer qui portera la double responsabilité». Vu la tendance à la digitalisation de la surveillance, l'IT devrait prendre une part de plus en plus conséquente dans le large domaine de la sécurité. L'inverse est vrai également, puisqu'il n'y a aucun intérêt à avoir un réseau extrêmement bien protégé au niveau informatique alors que n'importe qui peut rentrer dans le bâtiment et se connecter à ce même réseau!

Le processus de convergence des deux mondes est en cours, mais loin de la maturité. En outre, l'évolution doit encore suivre au niveau des solutions, afin que le monitoring de la sécurité dans un réseau et celui dans un bâtiment puissent être faits par une même personne. Du côté des prestataires de sécurité physique, Stéphane Bocqué, national marketing manager de Group 4 Falck, résume: «Les ponts existent et sont très vivants. Au bout du compte, il y a deux spécia-

et sécurité physique

lisations différentes mais totalement complémentaires qui, par la force des choses et la manière dont la technologie évolue, doivent communiquer et fonctionner ensemble». Exemple de complémentarité basique: le stockage sécurisé de back-ups physiques à côté des back-ups informatiques.

Main dans la main

Rappeler que l'informatique a investi tous les secteurs de notre société est une lapalissade. Le profil des ingénieurs et techniciens des entreprises de sécurité physique s'est donc transformé en profondeur: les compétences en matière d'applications informatiques de gestion et d'utilisation de réseau sont devenues incontournables afin de garantir des solutions performantes.

Les systèmes de vidéo surveillance n'échappent pas à l'évolution générale et sont eux aussi sous-tendus par une application informatique... qui risque elle-même d'être piratée, qu'elle soit gérée off line ou via Internet.

C'est au responsable de la sécurité informatique à gérer ce risque, bien sûr, mais celui-ci est lié au prestataire en sécurité physique de son client, comme en témoigne encore Stéphane Bocqué : «La plupart de nos systèmes, spécifiquement dans les grandes entreprises, ne s'appuient plus sur des réseaux et câblages propres, mais utilisent la bande passante concédée par le client. Il y a donc communication entre celui qui installe les systèmes de contrôle d'accès et le gestionnaire du réseau, ne fût-ce que parce qu'il y a cette utilisation. En outre, aujourd'hui, la plupart des applications de sécurité fonctionnent sur les normes IP». Le fait de travailler sur des systèmes et protocoles ouverts, voire universels, permet de créer des interfaces et produits qui s'inscrivent dans la logique de réseau de l'entreprise, et donc dans sa politique de sécurité informatique.

Group 4 Falck a par exemple lancé il y a quelques mois «eView», solution de vidéo surveillance totale par le Net, constituée d'un terminal IP doté d'un disque dur, le tout installé chez le client, qui stocke donc physiquement les images. La sécurité informatique de l'application est assurée par ce dernier. Du côté de Group 4 Falck, seules les personnes qui ont un droit d'accès (protégé bien sûr par mot de passe) peuvent consulter les images à distance, mais ne peuvent les enregistrer. Toute transaction effectuée par Group 4 Falck par rapport à un système décentralisé est de plus totalement contrôlée et traçable. La sécurité globale est in fine assurée par le truchement des deux métiers.

Access denied?

Les frontières semblent aussi s'effriter quand on observe les systèmes de contrôle des droits d'accès. Celui du

Pentagone a été mis en place par Group 4 Falck. Il se «limite» à l'accès physique sur site du porteur d'une carte magnétique qui peut être utilisée avec code, lecture à distance et/ou puce programmable. La carte mise à disposition reste la propriété de Group 4 Falck et est liée à une personne et à des horaires dans ses systèmes.

Elle peut être directement corrélée à l'obtention de droits d'accès informatiques, ce qui présente l'avantage d'une solution centralisée: «Tout comme ces cartes peuvent être utilisées pour l'accès aux machines de vending, elles peuvent l'être pour n'importe quelle application, dont l'accès à un PC» ponctue Stéphane Bocqué, avant de préciser que «Group 4 Falck laisse la possibilité au client de programmer lui-même la puce pour des applications qui lui sont propres. Nous n'allons pas mettre au point nous-mêmes la solution software adéquate». Il suffit donc que le client installe un reader sur chaque PC et que l'accès soit contrôlé par les softwares et la technologie qui se situent à l'arrière-plan.

Une technologie d'identity management que Telindus connaît bien, comme en témoigne Vincent Genart, business consultant en sécurité: «Nous menons à terme bon nombre de grands projets de systèmes d'informations qui gèrent l'identification, l'authentification et l'autorisation des détenteurs d'un badge ou d'une carte». Plus la peine, lors des modifications concernant les droits d'un employé, d'intervenir dans plusieurs systèmes: une carte, un système d'information unique, et le tour est joué. Une belle preuve, toute simple, de complémentarité.

OLIVIA AREND

Vigilance physique et informatique Quand la faille vient des hommes

La sécurité de l'entreprise est aussi une problématique de management de l'humain. On a beau mettre en place une armada de solutions pour contrer les agressions et protéger les maillons faibles, si la prudence la plus élémentaire (et la moins coûteuse!) n'est pas assurée en interne, la porte est grande ouverte aux catastrophes.

A tous les niveaux de l'entreprise, la sécurité doit donc être intégrée aux bonnes pratiques de travail, grâce à une «security policy» comprenant à la fois les règles établies par l'entreprise en matière de sécurité informatique (ce qui est assez commun), et celles définies en matière de sécurité physique (qui est appelée à se digitaliser le au moins en partie). Un document complet qui existe encore peu, dans les faits.

Or une forte proportion des incidents liés à la sécurité provient de l'intérieur même de la société, et bien souvent sans intention malicieuse de la part du «fautif». On n'envie pas toujours les cas les plus absurdes, et pourtant fréquents. Le personnel administratif n'est pas forcément au fait que certains hackers se font passer pour des responsables informatiques pour leur demander un mot de passe afin de régler un problème soit-disant urgent. L'anti-virus le plus à jour et le plus performant des firewalls n'y pourront rien!

Et puis, un peu de discipline: alors que rares sont les personnes qui laisseraient traîner leur badge, que celui qui n'a jamais oublié (ou failli oublier) de faire son log-off en quittant son bureau lève le doigt...

Mission à Athènes

Cet été, Athènes accueillera les Jeux olympiques. Comme le rappelait Ioannis Spanudakis, Managing Director d'ATHENS 2004, lors de l'événement "Competing for the Future" organisé en ce mois de février par Siemens ICN. La sécurité constitue une priorité absolue aux yeux des autorités grecques..

Celles-ci n'ont donc pas lésiné sur les moyens pour se doter d'une infrastructure de pointe, fournie par un consortium international qui regroupe la société américaine SCIC et Siemens-ICN.

Ioannis Spanudakis n'a pas vraiment eu besoin de forcer la dose pour illustrer le caractère global de l'événement. Il lui a suffi d'aligner quelques chiffres. L'organisation des Jeux a nécessité un investissement global de 6,5 milliards d'euros, ceci pour accueillir 10.500 athlètes, plus de 3.500 officiels, juges et arbitres, 22.500 journalistes accrédités et, last but not least, des centaines de milliers de spectateurs (plus de cinq millions de tickets vendus). Enfin, l'audience télévisée devrait dépasser cinq milliards d'individus.

C4i: un projet de 250 millions

Pour M. Spanudakis, le fournisseur se devait d'être d'envergure internationale tout en disposant d'une présence significative en Grèce (support et besoin de formation obligent). En outre, il devait s'agir de systèmes déjà éprouvés auparavant dans des circonstances comparables, et adaptables aux besoins des services concernés. Il n'était pas question que les services de sécurité soient contraints de revoir toute leur procédure de fonctionnement de A à Z pour s'adapter à l'infrastructure.

Un peu plus de 700 millions d'euros sont réservés aux seules dépenses de sécurité. Dans cette enveloppe, 250 millions (hors TVA) sont investis dans le projet C4i (inspiré du concept du Pentagone pour Command, Control, Communication, Coordination, le "i" désignant l'intégration du tout). L'objectif est de fournir l'infrastructure de commandement qui permettra aux décideurs de piloter l'action des 41.000 membres des forces de l'ordre et des services liés: la police, mais aussi l'armée et le ministère de la Défense, les services de renseignement, les garde-côtes, le corps des pompiers, le servi-

ce ambulance, le secrétariat général de la protection civile ou encore le service de la gestion du trafic routier.

Quatre sous-systèmes

Cette infrastructure se décompose en quatre sous-systèmes. En premier lieu, on compte plus d'une centaine de centres de commandements répartis aux sièges des différents services de sécurité et au sein des stades, mais aussi dans les hôtels ou à bord des sept navires qui hébergeront les athlètes et les officiels; il y a également des postes de commandement mobiles. Deuxièmement, on trouve un réseau de données qui permettra l'échange des informations en temps réel entre tous les services concernés et jusqu'aux équipes de terrain. S'y intègrent différents systèmes de gestion des incidents et des logiciels spécialisés comme un module de gestion des ressources qui permet, entre autres, de visualiser directement sur une carte les moyens disponibles pour faire face à un incident. En troisième lieu, le plus gros composant de l'infrastructure est constitué par le réseau TETRA qui permettra à 22.000 utilisateurs de communiquer via un réseau radio protégé par cryptage. Ce réseau permettra en outre de suivre en temps réel les déplacements de chacun des 4.000 véhicules qui serviront au transport des athlètes et des officiels. En dernier lieu, l'infrastructure intègre également tous les systèmes de sécurité physique qui comprennent les équipements de surveillance placés sur tout le pourtour du village olympique, les images prises par un réseau de 190 caméras fixes disposées dans des lieux jugés stratégiques d'Athènes, les caméras embarquées à bord d'un dirigeable et des hélicoptères des forces de l'ordre. Ces moyens comprennent même des systèmes de détection sous-marine, puisque des navires ancrés dans le port du Pirée serviront de lieu d'hébergement pour une partie des membres de la communauté olympique.

ERIC MAHIEU

Pro-activité: le maître-mot chez Cisco

Un ver tel que Slammer a mis l'an dernier moins d'un quart d'heure pour se propager à l'échelle du globe. Comment réagir dans un délai aussi court?

Dès lors, pour Peter Saenen, System Engineer spécialisé en sécurité chez Cisco, "la position de ces sociétés qui disaient 'si quelque chose arrive à Singapour, on a encore six heures pour réagir ici en Europe', ça, c'est du passé. Dans le domaine de l'antivirus, on travaille surtout de manière réactive en mettant à jour les signatures anti-virus du système, mais si le virus peut se propager en dix minutes, cela ne tient plus la route."

Cisco met donc aujourd'hui en avant le concept de "self-defending network". Les réseaux d'entreprise sont de plus en plus ouverts sur l'extérieur, de plus en plus de travailleurs sont équipés de laptops ou d'autres terminaux mobiles... Pour Peter Saenen, là réside le danger majeur aujourd'hui: "qui est cet utilisateur qui veut se connecter, où a-t-il été? Depuis combien a-t-il fait l'update de son antivirus?" Pour protéger le réseau face à une infection, il faut d'abord répondre à ces questions. Aujourd'hui, explique Peter Saenen, un utilisateur qui arrive dans son bureau se connecte sur le réseau et reçoit une adresse IP: "si j'ai un bon Security Officer, le PC commence par contacter le serveur de sécurité qui va faire un scan antivirus, etc. Le seul souci qu'on a dans cette vision-là, c'est qu'au moment où on reçoit une adresse IP, c'est déjà foutu! En fait, on fait déjà partie du réseau et si on a été infecté par un virus, celui-ci peut commencer à se propager."

Mode quarantaine

Chez Cisco, la solution est donc de vérifier de quelle machine il s'agit (identity-based networking) et son état avant l'octroi de l'adresse IP. "Est-ce que l'antivirus est à jour? Est-ce que la machine a le bon OS, avec le bon patch?" Si la machine ne présente pas toutes les garanties, elle sera placée en mode quarantaine: elle recevra une connexion, mais dans un WLAN bien spécifique, séparé des autres connexions du réseau. Quand tous les updates de sécurité auront été faits, la machine pourra se logger sur le réseau normal. Cet accès conditionné est possible

grâce au Cisco Trust Agent. Il ne s'agit pas d'un produit en tant que tel, mais d'une technologie pour laquelle Cisco octroie des licences, à l'heure actuelle à des partenaires tels que Symantec, TrendMicro et Network Associates. Ceux-ci intègrent au sein de leur propre système cet agent, capable de dialoguer avec un réseau Cisco.

Bloquer les flux suspects

Cisco propose également une technologie baptisée Security Agent. A l'origine, celle-ci a été développée par la société Okena, rachetée l'an dernier. Ici aussi, l'idée est de travailler d'une manière différente de l'antivirus traditionnel dont l'efficacité dépend largement de la fraîcheur de sa base de données. La solution imaginée par Okena pour protéger les machines clientes (desktop et serveurs), c'est de surveiller les flux à l'intérieur d'un système. En effet, il n'y a qu'un nombre limité de moyens "licites" d'obtenir des droits au sein d'un système. Si une application commence à réclamer des droits de manière irrégulière, il y a de grandes chances qu'il s'agisse du symptôme de l'activité d'un virus qui tente de prendre le contrôle d'une machine. Dans ce cas, le Security Agent va bloquer cette activité suspecte et donc empêcher l'infection. Selon Peter Saenen, cette technologie lui a permis de bloquer un ver tel que MyDoom sur sa propre machine. Le prochain pas, selon lui, sera de l'adapter pour les réseaux. A l'heure actuelle, cela ne fonctionne pas encore de manière tout à fait effective, notamment parce qu'il demeure un problème de "faux positifs", c'est-à-dire la possibilité de bloquer certaines applications "légitimes" parce que le système de sécurité les interprète comme des signes de trafic suspect. □



Pour Peter Saenen, System Engineer, chez Cisco, "on sait aujourd'hui faire pas mal de choses pour protéger les réseaux". Côté desktops et laptops, c'est autre chose...

Outsourcing et

Si la sécurité informatique apparaît comme une préoccupation importante dans le contexte d'économie connectée aujourd'hui, les entreprises doivent-elles pour autant consentir elles-mêmes des investissements en ce domaine?

contradictoires dans les termes?

Selon les promoteurs d'une solution d'outsourcing de la sécurité, il est plus rentable et plus efficace de faire appel à un prestataire spécialisé. Mais même si l'entreprise choisit une solution d'outsourcing, elle ne pourra pas cesser pour autant de mener sa propre réflexion sur la sécurité... en interne.

Confier la responsabilité de la sécurité informatique de l'entreprise à un fournisseur externe n'est-il pas contradictoire dans les termes avec l'idée même de sécurité? A ce propos, on peut noter que dans la plupart des entreprises, les fonctions traditionnelles de gardiennage sont largement assurées par des prestataires externes sans qu'on y trouve à redire. A priori, on voit donc mal ce qui prohiberait le recours à un prestataire de services spécialisé dans le domaine de la sécurité IT. Bien sûr, beaucoup considèrent aujourd'hui que l'actif sacré d'une entreprise, intouchable par des externes, ce sont ses données mais, deuxième argument, si on parle énormément de hacking et d'attaques sur les réseaux des entreprises aujourd'hui, les agressions externes seraient, selon des organismes tels que le FBI, minoritaires par rapport aux méfaits (sabotage, vol d'informations, etc.) causés par des membres (ou ex-membres) du personnel des entreprises, que ce soit pour des motifs de vengeance personnelle ou d'appât du gain.

Par ailleurs, le mode de fonctionnement de l'économie aujourd'hui suppose qu'une entreprise doit partager une partie de ses informations avec des partenaires externes et ceci n'est pas sans risque comme vient de le prouver la récente diffusion sur Internet du code-source de différentes versions de l'OS Windows de Microsoft (l'enquête suit son cours, comme on dit, mais la fuite serait bel et bien liée à un partenaire). Enfin, la possibilité de plus en plus large offerte aux employés d'une entreprise d'accéder aux applications de la société alors qu'ils sont en déplacement (mobilité) ou qu'ils travaillent à partir de chez eux (télétravail) introduisent de nouvelles failles potentielles dans la cuirasse, donc réclament de nouvelles manières d'aborder la sécurité. Dans ces conditions, faire appel à un spécialiste externe ne peut pas rimer avec une augmentation du danger.

De quoi parle-t-on?

Quand on parle d'outsourcing de la sécurité, il faut encore s'entendre sur ce dont on parle exactement. En effet, comme le rappelle Wim Temmerman, Country Manager d'Internet Security Systems Belux, il faut insister sur la distinction qu'il faut établir entre l'outsourcing de la sécurité en tant que telle et l'outsourcing de toute la fonction IT, auquel cas la sécurité en fait également partie sans nécessairement en constituer l'essentiel. Selon Wim Temmerman, il n'est d'ailleurs pas rare de voir des spécialistes de l'outsour-

sécurité:

cing en général (les IBM, EDS, etc.) travailler an tandem avec de véritables spécialistes de la sécurité.

Quel que soit le périmètre de l'outsourcing, le document de référence, c'est le contrat de service qui bétonne les fameux SLA (service level agreement) qui fixent le type et le niveau de services que le fournisseur s'engage à atteindre pour le compte de son client. Quoiqu'il arrive par la suite, c'est à lui qu'on se réfèrera en cas de litige ou d'incident. Il est donc absolument stratégique de définir aussi précisément que possible ces clauses SLA. Personne ne s'y trompe puisque la négociation d'un tel contrat prend des mois, voire des années, en particulier lorsqu'il s'agit d'un client de grande taille qui dispose fatalement d'une infrastructure complexe. En cas d'outsourcing en cascade, le prestataire principal faisant lui-même appel à des partenaires, par exemple spécialisés en sécurité, ceux-ci seront tenus par leurs propres SLA vis-à-vis du prestataire principal pour assurer par exemple la gestion des incidents.

Bien sûr, dans le domaine de la sécurité, c'est avant tout la rapidité de la réaction qui compte (un ver tel que Slammer a mis moins d'un quart d'heure pour se diffuser à l'échelle de la planète) et, dans ce contexte, on peut éventuellement voir le SLA comme un parapluie déployé à l'intention des fournisseurs de services. Il n'est pas sûr en effet que ces fournisseurs pourront trouver pour l'ensemble de leurs clients une parade appropriée à ce type de menaces dans des échelles de temps aussi courtes et le SLA peut alors devenir un alibi commode que le fournisseur peut invoquer pour tenter de se dédouaner.

Dès lors, un des points essentiels de ce type de services, au-delà de la gestion des informations et des alertes générées par les firewalls, sondes IDS, etc., c'est d'assurer un suivi régulier de l'infrastructure à protéger. On découvre chaque jour de nouvelles vulnérabilités dans les OS et dans les applications. Patcher ces vulnérabilités est devenu un métier en soi puisque chaque entreprise utilise au minimum des dizaines d'applications différentes, quand ce n'est pas des centaines. Dans la mesure où beaucoup de virus exploitent des vulnérabilités connues depuis plusieurs mois, un prestataire spécialisé peut sans nul doute rendre de grands services dans ce domaine. Bien sûr, patcher les systèmes nécessitera toujours l'intervention du personnel IT de l'entreprise ou d'un fournisseur "généraliste" pour tester la performance des systèmes patchés et leur compatibilité éventuelle avec les autres applications de l'entreprise.

Les arguments pour

En-dehors de cela, quels arguments avancer en faveur de l'outsourcing? Il y a d'abord l'argument du coût, qui n'est pas spécifique au domaine de la sécurité. Aucune entreprise ne peut se prétendre sécurisée si elle ne dispose pas sept jours sur sept et 24 heures sur 24 d'une personne qui puisse réagir rapidement à toute nouvelle menace éventuelle. Hackers et virus n'ont en général pas la politesse élémentaire de lancer leurs attaques pendant les heures du bureau. Par conséquent, si une entreprise choisit de maintenir en interne une équipe dédiée à la sécurité, elle devra au minimum mobiliser une équipe de cinq personnes pour assurer une couverture permanente (cinq personnes, car il faut bien sûr compter avec

Managed Security Providers: la crise d'identité?



Selon Martin Dipper, les MSP promettent trop de choses à trop de clients...

Pour Martin Dipper, Vice-President Partner Programs chez Infonet Services Corporation, spécialiste de la gestion de réseaux qui fournit notamment à ses clients des services de firewalling et de gestion des incidents, le marché MSP est confronté à une crise d'identité. "Les Ubizen et autres vont avoir de sérieux problèmes parce qu'ils essaient de faire trop de choses pour trop de multinationales et ils vont perdre le contrôle de leurs coûts et de leur business model. Plus personne ne sait exactement ce qu'ils font. Beaucoup d'ex-compagnies produits, telles que Symantec, essaient aussi d'entrer dans le marché des services. Bien sûr, Symantec a

une base très forte, notamment de bons produits, mais une nouvelle fois, nous pensons qu'il y a un problème: Symantec va avoir beaucoup de difficultés à y parvenir parce qu'avoir une culture de services, ce n'est pas la même chose qu'avoir une culture produits. C'est une autre mentalité: une fois que vous allez vers les services, vous devez tous les jours avoir des contacts avec les clients dans différentes régions du globe. Quand on vend un produit, on le vend et puis, on s'en va. C'est assez différent."

Même le rachat par Symantec de Riptech, un spécialiste MSP, ne garantit pas le succès, selon Martin Dipper, parce qu'il faudra du temps pour diffuser au niveau global l'expérience d'un acteur qui travaillait essentiellement au niveau local (aux Etats-Unis): "quand on demande à des fournisseurs de produits s'ils sont globaux, ils vous répondent 'oui, nous avons un bureau à Boston, un autre à Bruxelles et un troisième à Tokyo'. Etre global, ce n'est pas cela. Etre global, cela veut dire que vous avez une présence dans 50 ou 55 pays. Cela veut dire aussi que vous avez une procédure pour prendre des commandes, livrer et supporter dans chacun de ces pays et que vous pouvez étendre votre présence dans les pays voisins à partir de ceux où vous êtes implantés. Il faut dix ou quinze ans pour établir une compagnie vraiment globale."



Pour Wim Temmerman, Country Manager BeLux d'Internet Security Systems, l'intérêt essentiel d'une solution d'outsourcing, c'est que le client peut se concentrer sur son core business.

les vacances, les maladies, les formations, etc.). A l'évidence, toutes les entreprises ne peuvent pas se permettre de se payer ce type de personnel spécialisé, mais l'outsourcing est-il vraiment destiné aux PME? On peut en douter et l'émergence des consoles sécurité multi-fonctions semble d'ailleurs attester que les fournisseurs de solutions de sécurité ne le pensent pas non plus.

Si la sécurité ne figure pas parmi les priorités de l'entreprise, faire appel à un spécialiste permet à celle-ci de focaliser ses moyens et

cela signifie qu'un gestionnaire ne peut jamais prévoir exactement à quel niveau de dépenses il devra se situer demain pour assurer sa protection. Faire appel à un MSP qui s'engage à remplir certaines missions pour un montant forfaitaire mensuel permet à l'entreprise de mieux maîtriser l'évolution de son budget et d'éviter de surcroît des investissements importants pour se maintenir à niveau: dans cette configuration en effet, c'est le MSP qui doit consentir les investissements nécessaires en technologies et en personnel (s'il ne les fait pas, il s'expose bien sûr à ne plus pouvoir satisfaire aux conditions de son SLA).

Penser sécurité... même en interne!

Cela étant, l'outsourcing ne dispense pas l'entreprise de disposer d'une politique et de procédures de sécurité et de la répercuter vis-à-vis de ses employés. La désignation d'un responsable, hors de la sphère IT et proche de la direction est également hautement conseillée: il faut nécessairement désigner un responsable de rang élevé parce qu'il devra pouvoir faire entendre sa voix auprès de la direction pour faire passer le "message" sécurité, pas toujours populaire en particulier lorsqu'il suppose d'investir, et parce qu'il devra disposer de l'autorité nécessaire pour imposer les mesures qui s'imposent à des ensembles d'utilisateurs disparates à travers l'entreprise dont les besoins seront parfois contradictoires avec les nécessités sécuritaires. Relevons ici un paradoxe: selon l'Information Security Guide récemment publié par PricewaterhouseCoopers, le recours à l'outsourcing de certaines fonctions IT peut lui-même devenir un problème en termes de sécurité puisqu'il devient à ce moment-là plus difficile de déployer une politique et une solution de sécurité uniformes dans l'ensemble de l'entreprise.

Tous les spécialistes de la sécurité le répètent comme un mantra: la sécurité est une question de culture et d'état d'esprit (celle d'une paranoïa raisonnée, si l'on veut) avant d'être une question de produits. L'intérêt de se doter d'une politique de sécurité n'est pas seulement de disposer d'un outil permettant à tout un chacun de savoir ce qu'il peut ou ne peut pas faire ou comment réagir en cas de problème, mais aussi d'établir une hiérarchie entre les risques que l'en-

Aucune entreprise ne peut se prétendre sécurisée si elle ne dispose pas sept jours sur sept et 24 heures sur 24 d'une personne qui puisse réagir rapidement à toute nouvelle menace éventuelle. Hackers et virus n'ont en général pas la politesse élémentaire de lancer leurs attaques pendant les heures du bureau.

son attention sur son métier de base tout en permettant au patron de l'entreprise de "pouvoir dormir la nuit", pour reprendre l'expression de Wim Temmerman qui considère que cet aspect est sans doute le plus important à prendre en compte. Autre argument: le contrôle des budgets. Si les menaces et les technologies évoluent,

l'entreprise est prête à assumer et ceux qu'il est hors de question d'envisager. Dans la foulée, l'entreprise peut orienter au mieux ses investissements pour protéger les parties jugées les plus critiques de son infrastructure ou de son information... et considérer que l'outsourcing constitue la meilleure garantie de se protéger. □

L'avis des spécialistes

Nous avons demandé à plusieurs acteurs de la sécurité belges qu'elles étaient leurs craintes et leurs espoirs pour 2004, et quel souvenir ils gardaient de 2003. Encore plus de worms et de spams, une plus grande prise de conscience des managers, plus d'intégration, les dangers du télétravail... Voici un florilège des réponses que nous avons reçues.

SkillTeam

Nouvelles technologies

Lancée en 1991, SkillTeam est spécialisée dans la création et la mise en place de solutions intégrées pour l'ICT et les projets e-business. Pierre Dugnoille, Managing Director:

Pourriez-vous établir un top 3 des failles de sécurité à l'heure actuelle?

1. Le manque de compréhension de ce qu'est la sécurité. Plus que la mise en place d'un firewall, c'est un "on-going process".
2. C'est insuffisant de simplement sécuriser une société des attaques venant de l'extérieur.
3. L'e-mail, bien que de plus en plus indispensable, devient une menace importante pour le business et la productivité à cause du malware et du spam.

Quelles seront, pour vous, les grandes tendances de la sécurité en 2004?

L'intégration des nouvelles technologies dans les solutions existantes. De plus en plus de "blackbox" appliances, qui unissent plusieurs technologies. Un certain nombre d'acteurs de la sécurité et du networking intègrent aujourd'hui des solutions de haute technologie dans leurs portfolios. Une plus grande attention à la gestion centrale des différentes solutions de sécurité, aussi bien à l'intérieur de la même famille de produits

que depuis différents produits séparés.



Selon vous, quelle est l'erreur la plus courante lorsque l'on parle de sécurité?

La sécurité n'est pas une infrastructure "set and forget" mais un mind-set et un investissement continu. La gestion des patches et des updates et le "business desktop management" sont au moins aussi importants que l'idée traditionnelle de périmètre de sécurité.

On parle souvent des menaces internes aux entreprises. Jusqu'à quel point faut-il surveiller ses employés?

L'utilisation personnelle croissante de l'internet, de l'e-mail et de l'instant messaging a un effet négatif sur la productivité et la bande passante disponible. Sans parler de l'important risque en matière de sécurité: divulgation de données confidentielles, porte ouverte aux virus, échange de messages à caractère pornographique ou raciste. C'est logique que les sociétés veuillent implémenter une politique de sécurité stricte. Certaines l'ont d'ailleurs déjà fait: elles autorisent l'usage personnel, mais stipulent que l'employé est strictement contrôlé.

La sécurité, l'affaire de tous

Telindus couvre toutes les technologies modernes de télécommunications. Yves Vekemans, Customer Services Manager:

Le top 3 des failles de sécurité?

1. L'absence de politique de sécurité basée sur les gens, les processus et la technologie sur laquelle on pourrait se baser pour réaliser des projets de sécurité concrets.
2. Le manque d'outils pour améliorer la sécurité et la productivité des travailleurs (anti-virus, anti-spam, url-filtering, personal firewalls...).
3. Le manque d'outils pour rendre la sécurité interne efficace.

Les grandes tendances de la sécurité en 2004?

En vrac: l'intrusion des systèmes d'Identity Management et l'impact de l'eID-card. Les rapports de sécurité, indispensables une bonne gestion de sécurité avec une security policy fournie. L'amélioration en continu de l'ethical hacking, reconnu comme instrument de sécurité indispensable. La sécurisation du

réseau interne. L'introduction des outils de productivité internet comme les anti-spam, l'url-filtering, les anti-spyware, le secure instant messaging, les personal firewalls, etc. L'emploi de Forensic Labs pour, après les problèmes, examiner ce qui n'a pas fonctionné.

Enfin, la mobilisation générale des utilisateurs et ses effets sur la sécurité.

Quel est l'événement qui vous a le plus marqué en 2003 sur le plan de la sécurité?

La sécurité n'est plus l'affaire de quelques techniciens, elle est discutée à tous les niveaux et concerne tout le monde.

Selon vous, quelle est l'erreur la plus courante lorsque l'on parle de sécurité?

Avoir une discussion technologique sans avoir d'abord pensé aux risques pour le business.



Check Point

Nokia ne construit pas que des GSM, loin s'en faut. La société finlandaise s'est également spécialisée dans une série d'autres technologies, notamment celles vouées à la sécurité des réseaux. La solution Check Point, par exemple, sécurise communications internet et contrôle d'accès. Elle repose sur une combinaison Firewall/VPN. En Belgique, les produits Nokia sont distribués par Noxs, société que l'on connaissait encore il y a peu sous le nom de Comsol. Guy Seeuws, Channel Manager:

Le top 3 des failles de sécurité?

Pour moi, les trois failles actuelles les plus importantes sont: 1. le spam; 2. le Wi-Fi; 3. les collaborateurs internes.

Les grandes tendances de la sécurité en 2004?

Les solutions mobiles sécurisées end to end.

Quel est l'événement qui vous a le plus marqué en 2003 sur le plan de la sécurité?

L'élargissement de la sécurité du monde financier au monde industriel.

Selon vous, quelle est l'erreur la plus courante lorsque l'on parle de sécurité?

La sécurité est une culture et non un produit.

Craignez-vous une émergence des problèmes de sécurité sur les plates-formes mobiles?

Oui, et il s'agit d'un défi dont peu de sociétés se préoccupent encore.

On parle souvent des menaces internes aux entreprises. Jusqu'à quel point faut-il surveiller ses employés?

En suivant et en maintenant une « security policy » bien balisée.

Quels sont selon vous les problèmes de communication liés à la sécurité?

Les problèmes arrivent lorsque, à l'intérieur de l'entreprise même, la communication est floue.



Des problèmes, mais aussi des solutions

L'un des leitmotifs de Saphico, fondée en 1995, est de tout faire pour rester au "top" en matière de technologie, histoire de pouvoir répondre à toutes les demandes de ses clients. La société fournit des solutions complètes qui lui permettent d'avancer quelques arguments chocs tels que «Vous ne recevrez plus jamais aucun virus par e-mail». Philippe De Groote, General Manager:

Le top 3 des failles de sécurité?

Il y a actuellement de très bonnes solutions pour tous les problèmes de sécurité.

1. Le wireless, les virus ou le hacking, mais aussi ce qui est moins connu comme le spyware ou les hacking tools.
2. Autre phénomène très courant: les PME sont mal informées. En fait, elles le sont souvent par de petits acteurs qui ne connaissent les problèmes qu'en petite partie.

3. La grande tendance du moment: le déplacement des Client less VPN et de la détection d'intrusion vers le firewall et l'anti-virus.



Quel est l'événement qui vous a le plus marqué en 2003 sur le plan de la sécurité?

L'événement le plus marquant est bugbaer et ses variantes qui ont vu de nombreuses PME se rendre compte qu'elles étaient très vulnérables. Ce qui leur a donné l'impulsion pour mieux se protéger au niveau de leur firewall.

Craignez-vous une émergence des problèmes de sécurité sur les plates-formes mobiles?

Les plates-formes mobiles ne font qu'élargir le problème et le rendent plus compliqué en raison des accès plus nombreux, puisque la société doit rester ouverte à ses road warriors. Ce qui rend la sécurité plus difficile, mais cela ne la rend pas pour autant insurmontable.

Authentification

Vasco, société américaine fondée en 1997, est spécialisée dans l'authentification. Elle compte deux antennes en Europe: une en France et l'autre en Belgique, à Wemmel, aux portes de Bruxelles. Vasco compte parmi ses clients 200 institutions financières internationales, 1.000 «blue-chip corporations» et les gouvernements de plus de 60 pays.

Vasco développe des produits d'Identity Authentification pour l'e-business et l'e-commerce, sous forme matérielle (avec ses produits de la gamme Digipass) et logicielle (à destination des PC et des téléphones et autres appareils portables). La cible de Vasco: les applications qui utilisent des mots de passe fixes comme élément de sécurité.

Jochem Binst, Director of Corporate Communications:

Le top 3 des failles de sécurité?

1. Le danger sans cesse plus important de l'utilisation de mots de passe statiques, qui permettent aux transactions de tomber dans les mains de n'importe qui. Les tentatives de fraude par phishing (e-mails bidons demandant des renseignements personnels) en sont la première conséquence.

2. Le travail à domicile non sécurisé
3. Les virus

Les grandes tendances de la sécurité en 2004?

L'introduction des nouveaux standards de cartes de crédit EMV. Il n'y aura plus de cartes avec bande magnétique, mais des smart cards qui autorisent deux facteurs d'authentification.

Quel est l'événement qui vous a le plus marqué en 2003 sur le plan de la sécurité?

L'application de l'algorithme AES dans les jetons Digipass.

Selon vous, quelle est l'erreur la plus courante lorsque l'on parle de sécurité?

La sécurité est pour les sociétés bien plus qu'un mal nécessaire. Toutes les sociétés qui font des affaires via Internet doivent se rendre compte que la sécurité peut augmenter leur chiffre d'affaires, vu que les clients acquièrent une plus grande confiance dans le medium internet si la sécurité est efficace.

Entreprises, à vos patches!

Wim Temmerman, Country Manager Belux d'Internet Security Systems:

Le top 3 des failles de sécurité?

1. L'incapacité des entreprises à garder leurs systèmes de sécurité à jour grâce à des upgrades et des patchings réguliers.
2. Avec le temps, les sociétés ont eu recours à des technologies très différentes. Cet amalgame n'est pas simple à gérer.
3. Le travail à distance: on travaille de partout, avec ou sans câbles. Mais les desktops sont trop peu sécurisés.

Les grandes tendances de la sécurité en 2004?

L'apparition de menaces hybrides qui utilisent les faiblesses des systèmes. Cette tendance est de plus en plus forte, MS Blast, SoBig.F et MyDoom sont là pour en témoigner. Les nouvelles attaques suivent de plus en plus près la découverte des failles, ce qui rend peu efficace les moyens de défense traditionnels. Appliquer manuellement

tous les patches et faire tous les upgrades du système antivirus seront toujours indispensables. Beaucoup d'entreprises demeurent par ailleurs prisonnières d'une approche réactive, "patch-when-attacked", inefficace, et continuent à penser la sécurité en termes de produits et de techniques alors qu'elle doit surtout être envisagée dans le rôle d'un "business enabler". Il existe désormais des solutions proactives à coût abordable, grâce à la combinaison de la puissance d'une technologie de "vulnerability assessment", d'une solution de détection d'intrusion et d'une intelligence à jour en matière de sécurité.



Quel est l'événement qui vous a le plus marqué en 2003 sur le plan de la sécurité?

Je ne veux pas distinguer un événement particulier mais insister sur la complexification constante des menaces hybrides et sur la difficulté des entreprises à aligner leur niveau de protection.

Peapod

Spam, souci croissant

Peapod distribue en Europe des solutions e-software et e-service. La société équipe les réseaux internet et d'entreprise et les environnements e-business avec des solutions de gestion de la sécurité complètes. Mohan de Silva, Managing Director:

Le top 3 des failles de sécurité?

1. Les dangers du "mobile code" (soft qui se lance à distance) qui proviennent de la grande quantité de spam.
2. Les serveurs e-mail insuffisamment sécurisés.
3. Les Outlook Web Access servers.

Les grandes tendances de la sécurité en 2004?

Nos clients ont une demande de plus en plus grande pour une protection efficace contre le spam.

Selon vous, quelle est l'erreur la plus courante lorsque l'on parle de sécurité?

On consacre la plus grande attention aux connexions internet entrantes mais pas assez au fait que toute l'information peut sans problème (involontairement) sortir

via le firewall, tous les ports sont souvent ouverts.



Craignez-vous une émergence des problèmes de sécurité sur les plates-formes mobiles?

A nos yeux, il y a sur le marché des solutions de protection avancées pour les appareils mobiles comme les Palm, Pocket PC et laptops. Mais pas pour les nouveaux GSM qui permettent de télécharger des applications (comme des jeux par exemple).

On parle souvent des menaces internes aux entreprises. Jusqu'à quel point faut-il surveiller ses employés?

En établissant une politique de sécurité au sein de l'entreprise et en l'implémentant et en la gérant au moyen de différentes solutions de protection qui dirigent l'utilisateur « sur la bonne voie », comme par exemple l'URL filtering et le contrôle de l'emploi/du contenu des e-mails et attachements, de l'accès aux serveurs, de l'accès à Internet, de l'accès depuis l'extérieur au réseau de l'entreprise...

La technologie n'est pas tout

Ubizen est l'un des "grands" de la sécurité en Belgique. Bart Vansievenant, VP Corporate & Field Marketing:

Le top 3 des failles de sécurité?

1. Les technologies de protection traditionnelles comme les firewalls et les systèmes antivirus ne sont plus assez efficaces.
2. Les sociétés limitent encore trop leur protection à ce qui se trouve dans le périmètre de leur réseau. Mais ce périmètre n'existe plus. Chaque desktop, laptop, PDA est devenu partie intégrante de la limite extérieure de l'entreprise. La connexion centrale à Internet peut être sécurisée jusqu'à l'absurde, si un virus de type worm entre dans le réseau de la société via un PC portable, il infectera le reste du réseau interne en un rien de temps. Rien n'est plus dangereux qu'un faux sentiment de sécurité.
3. Dans la plupart des sociétés, la sécurité est souvent traitée de la même manière que les autres projets IT. Mais la sécurité n'est pas un projet, c'est un processus. Ce n'est pas suffisant de dessiner une seule fois une architecture de sécurité et de l'implémenter ensuite. En matière de sécurité, vous

n'êtes jamais prêt, cela demande une formation permanente.



Les grandes tendances de la sécurité en 2004?

La sous-traitance: au moyen d'un contrat avec une société spécialisée, une société s'assure que les opérations de sécurité quotidiennes seront opérées de manière optimale. Le déplacement du périmètre de sécurité "classique" vers des technologies de sécurisation plus fines. Enfin, une protection centralisée et intégrée.

Selon vous, quelle est l'erreur la plus courante lorsque l'on parle de sécurité?

La conviction que la protection est une affaire purement technologique. En réalité, il s'agit d'une combinaison d'aspects organisationnels, légaux et techniques. Vous pouvez techniquement implémenter la politique de passwords la plus stricte, si les utilisateurs ne sont pas 'security aware' et communiquent leur password par téléphone à quiconque se prétend être du service informatique, cela ne servira à rien.

Failles mal gérées

On ne présente plus Symantec, acteur de poids dans le secteur de la sécurité. Patrick Dalvinck, Regional Director Benelux:

Le top 3 des failles de sécurité?

1. Les vulnérabilités, les failles et la manière de les gérer. D'après l'Internet Security Threat Report de Symantec, 64% des attaques concernaient des failles nées dans l'année précédant l'attaque. Beaucoup de sociétés ne sont toujours pas au courant de ces failles ou ne disposent pas des moyens de les patcher.
2. La complexité et la vitesse des "blended threats" (60% des attaques au premier semestre 2003 selon l'ISTR). Les entreprises se retrouvent souvent face à des menaces combinées.
3. La confusion. Les sociétés travaillent souvent avec différentes solutions, provenant d'horizons différents. Cela engendre une grande quantité de données qui peuvent être difficilement corrélées, les gestionnaires de système peuvent difficilement en tirer une vue d'ensemble.

Les grandes tendances de la sécurité en 2004?

Nous apercevons surtout une tendance à l'acceptation de solutions intégrées, une solution intégrée pour le client, une appliance intégrée et une réponse intégrée.

Nous nous attendons également à ce que les sociétés aient de plus en plus recours à l'outsourcing, notamment pour le périmètre de sécurité.

Quel est l'événement qui vous a le plus marqué en 2003 sur le plan de la sécurité?

Nous avons eu affaire l'été passé à quelques blended threats dangereuses. Nous parlons surtout d'une période marquante, plus que d'une histoire marquante. En août (Welchia, Blaster en Sobig.f), les sociétés et les consommateurs ont été confrontés de manière récurrente à ces menaces. Les jours qui ont suivi, on a vu avec MyDoom et NetSky, la vague de blended threats a suivi de manière fulgurante.



Trop de bricoleurs

Emmera, société belge fondée en 1999, est spécialisée dans le conseil et la mise en place de solutions informatiques intégrant la sécurité. Maxime Rapaille, Network & Security Consultant:

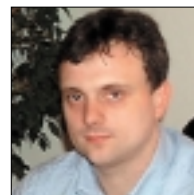
Le top 3 des failles de sécurité?

1. Le manque d'information ou la mauvaise information des utilisateurs et du management. En effet, partout où le management manque d'information, la sécurité manque de moyen... Les risques sont énormes.
2. Les réseaux sans fils non sécurisés et leurs PC clients.
3. Les utilisateurs domestiques et travailleurs à distance.

Les grandes tendances de la sécurité en 2004?

Au niveau des risques: des virus et des worms encore plus actifs et plus virulents, la montée en puissance du spam, les réseaux sans fils non sécurisés, dont le nombre explose. Les PME ne sont pas assez informées, ni assez prises en compte par les spécialistes. Elles doivent faire confiance à des bricoleurs de la sécurité, qui placent des firewalls comme on place une serrure de sécurité sur une porte en

carton. Au niveau des produits et solutions: les produits antispam, les appliances combinées, les produits orientés PME.



Jusqu'à quel point faut-il surveiller ses employés?

Je pense qu'il faut d'abord les informer. Ensuite mettre en place assez de barrières pour éviter qu'ils ne s'égarer là où ils ne doivent pas aller, et ne pas les soumettre à la tentation. Enfin, il faut surveiller l'ensemble du réseau et détecter les anomalies.

7. Quels sont selon vous les problèmes de communication liés à la sécurité?

La sécurité a trop souvent mauvaise presse. Trop d'acteurs ont préféré faire peur aux gens pour promouvoir leur business. Ensuite, l'image qu'ont certains que la sécurité est un service de luxe, et donc cher. Il y a aussi le faux sentiment de sécurité induit par le message donné par des 'installateurs de firewall' qui préfèrent leurrer leur client que d'avouer leur incompétence.

Faux sentiment de sécurité

DCB distribue des produits liés à la sécurité internet. La société met l'accent sur le service et son savoir-faire. Wim Clinckspoor, Directeur Technique:

Le top 3 des failles de sécurité?

1. Le faux sentiment de sécurité. Alors que les logiciels antivirus et les fabricants d'OS et d'applications ont les plus grandes difficultés à rendre disponibles à temps les updates nécessaires et autres patches.
2. Le sentiment de sécurité qui entoure l'utilisation d'un VPN, alors que c'est un accès facile au réseau. Par exemple: les travailleurs à domicile avec un tunnel VPN vers le réseau de la société. Même si le VPN est sûr, le PC du travailleur à domicile ne l'est pas forcément. Un hacker peut utiliser son PC comme relais pour atteindre le réseau de l'entreprise.
3. Le manque de connaissance des intégrateurs dans le domaine de la sécurité. Les firewalls sont la plupart du temps configurés pour que tout fonctionne, alors que le raisonnement devrait être inverse.

Les grandes tendances de la sécurité en 2004?

Tout d'abord, les virus seront de plus en plus agressifs, une meilleure sécurité est donc indispensable, mais il ne faut plus seulement compter que sur les fabricants d'antivirus pour les updates. Ensuite, de plus en plus de virus et de hackers vont utiliser les problèmes de sécurité des OS, un management des patches fonctionnant correctement est donc également indispensable. Par ailleurs, la sécurité sera de plus en plus le travail de sociétés spécifiques qui emploieront du personnel spécialisé dans un domaine précis de la sécurité. Enfin, on commence à se demander si les attaques ne doivent pas être majoritairement stoppées dès les firewalls des ISP.

Quel est l'événement qui vous a le plus marqué en 2003 sur le plan de la sécurité?

La diffusion de quelques virus agressifs comme Nachi, Sobig et l'absence de protection de beaucoup de sociétés.



Un avenir au soleil assuré pour Trusted Solaris

Sun va continuer à offrir la version Trusted Solaris de son système d'exploitation en tant que produit séparé, a déclaré un responsable de la compagnie qui a tenté de dissiper toute confusion que Sun aurait pu créer aux yeux du marché.

Des représentants de Sun ont récemment répété, à diverses reprises, que des fonctionnalités liées à la sécurité de Trusted Solaris avaient été ajoutées à sa distribution Solaris standard. Trusted Solaris est une version "blindée" de l'O.S. de Sun, utilisée au sein de l'armée, des gouvernements et de certaines entreprises.

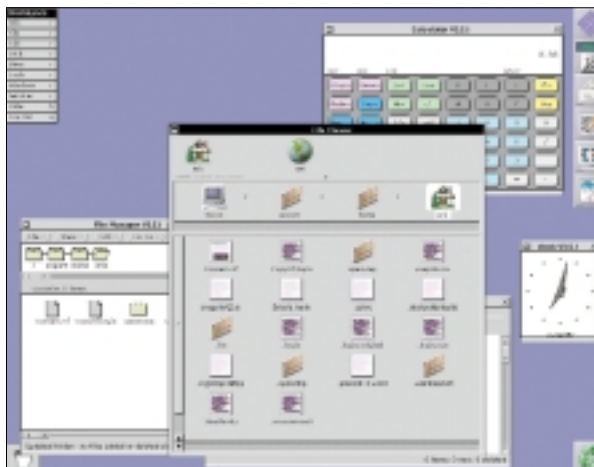
Selon Ravi Iyer, Group manager of security systems marketing chez Sun, les deux lignes de produit continueront cependant à exister de façon séparée. "Il y a une perception incorrecte à propos du fait que ces deux produits auraient été fusionnés. Ce n'est pas le cas, mais nous avons emprunté certaines fonctionnalités de Trusted Solaris pour les intégrer à Solaris", a-t-il affirmé.

Solaris inclut par exemple le process rights management, une fonctionnalité de Trusted Solaris qui empêche les applications d'accéder aux ressources qui ne sont pas essentielles à la tâche qu'elles remplissent. Cette fonctionnalité permet de minimiser les dommages causés par les attaques de type buffer overflow (dépassement de tampon), une forme assez commune de technique d'attaque contre les ordinateurs, selon Sun. Mais d'autres fonctionnalités de sécurité ne seront pas intégrées. Trusted Solaris laisse par exemple les utilisateurs accorder des labels à toutes les applications et tous les fichiers sur un serveur et en contrôler l'accès sur base du niveau d'autorisation de chaque employé. Ces fonctionnalités réclament trop de performance ou de suivi administratif pour être intégrées à un OS à vocation généraliste, a expliqué Ravi Iyer. D'autres fonctionnalités telles que le contrôle d'accès discrétionnaire et les fonctions de réseaux et d'impression sécurisés ne sont pas non plus destinées aux distributions standards de Solaris. Les clients paient un extra pour la sécurité renforcée de Trusted Solaris, de même que pour obtenir certaines certifications de sécurité, a remarqué Iyer.

Par ailleurs, Sun a pour objectif de réduire le temps nécessaire au lancement de nouvelles versions de Trusted Solaris. Dans le passé, il s'écoulait en moyenne un an entre le moment où apparaissait une nouvelle version de Solaris et celui où la version correspondante de Trusted Solaris devenait effectivement disponible. Iyer a affirmé que Sun espérait réduire ce

décalage dans la fourchette de six à neuf mois. Trusted Solaris en est actuellement à sa version 8. La version 9 n'existe pas et n'existera jamais. La version 10 de Solaris devrait quant à elle être lancée durant le troisième trimestre, ce qui veut dire que Trusted Solaris devrait arriver trois à six mois plus tard (NDLR: pour faire court, admettons une bonne fois pour toutes que ce sera pour 2005).

S'il n'y aura pas de nouvelles fonctionnalités de sécurité, certaines des améliorations générales de Solaris profiteront à la sécurité, a déclaré Iyer. En exemple, il a cité la combinaison de la technologie N1 Grid Containers, qui partitionne un serveur en compartiments séparés, et la technologie d'attribution de labels de Trusted Solaris qui permettra de mettre en œuvre un système à la sécurité considérablement renforcée. Trusted Solaris est disponible depuis le milieu des années 1990. Initialement conçu pour un usage militaire, il a été adopté par des clients civils qui avaient des besoins de sécurité élevés. Sun cite notamment un client de Chicago, Bank One, qui utilise Trusted Solaris pour son système de traitement des paiements. □



L'interface graphique typique de l'OS Solaris de Sun.

Sera-ce à présent David ou Goliath?

CheckPoint lance Interspect et Application Intelligence. Le pare-feu devenu monnaie courante, le spécialiste firewall se met en quête d'un nouvel avantage compétitif.

Depuis plusieurs années, CheckPoint est un acteur de premier plan dans l'univers de la sécurité IT, et en particulier des pare-feux. Au cours des derniers mois, des fissures sont toutefois apparues dans le blindage de ce géant de la sécurité. Aujourd'hui, l'essentiel du chiffre d'affaires de CheckPoint est encore réalisé par le produit auquel l'entreprise doit son expansion – à savoir son Firewall-1. Ce produit a connu et continue de connaître un succès incroyable, tant sur le plan technique qu'au niveau des chiffres de ventes. En dépit de bons résultats avec son propre client VPN, CheckPoint n'a jamais été en mesure de répéter ce succès pour des applications comme Meta-IP. Entre-temps, la société a dû faire face à une concurrence nourrie. Le marché compte aujourd'hui des dizaines de bons produits de pare-feu, parmi lesquels le client a souvent du mal à voir la différence. En outre, d'autres fabricants, comme Cisco, ont déjà un pied bien ancré chez le client avec des applications LAN et de routeurs. D'autres encore mènent une stratégie de prix et de marketing extrêmement agressive, comme NetScreen, qui s'est accaparé une sérieuse part du marché Benelux. Aujourd'hui, la 'unique selling proposition' de la technologie Stateful Inspection n'est plus réellement unique. De plus en plus de fournisseurs proposent des solutions stateful – bien que la dénomination Stateful Inspection soit une marque déposée de CheckPoint. Il faut ajouter à cela la crise économique mondiale et la politique d'upgrade vers CheckPoint-NG au succès mitigé. CheckPoint devait donc manifestement se reprendre. Et c'est chose faite, selon nous.

Tunnels

Avec Application Intelligence, CheckPoint résout un problème important dans les pare-feux existants. L'idée est que vous allez contrôler et bloquer non seulement le type de trafic qui passe par le pare-feu, mais que les contrôles nécessaires au sein de la connexion seront également exécutés. Jusqu'alors, la plupart des

pare-feux bloquaient le trafic réseau sur la base de critères externes (expéditeur, destinataire, type de trafic, port TCP). Ces critères étaient généralement faciles à déjouer pour un pirate. Sur un pare-feu standard, vous pouvez ainsi faire en sorte, en tant qu'administrateur, qu'aucun trafic SSH ne soit possible vers le port TCP 22 standard (FTP). Mais si vous voulez ouvrir ce port pour le trafic FTP vers le monde extérieur, vous ne pouvez pas empêcher que quelqu'un fasse également tourner SSH via cette connexion et mette en place un tunnel vers le réseau interne. La plupart des pare-feux sont dès lors faciles à contourner depuis l'intérieur, avec toutes les conséquences que cela peut avoir sur la sécurité. Avec Application Intelligence, vous pouvez inspecter la connexion et découvrir par exemple qu'une session FTP est en réalité une session SSH ou autre. Il s'agit sans aucun doute d'une technologie intéressante et extrêmement utile.

Diviser pour régner

Autre marché clairement visé par CheckPoint: la sécurité interne. Avec Interspect, la société lance un produit hardware qui permet de contrôler le trafic interne des serveurs et clients internes, en isolant éventuellement un client "suspect" au niveau du réseau. L'Interspect se place entre les différents composants réseau actifs de votre installation (entre 2 commutateurs, par exemple) pour y contrôler la situation. Lorsque, par exemple, une machine est infectée par un virus (comme Bugbear) qui tente de se propager sur le réseau, Interspect le détecte et isole cette machine, pour qu'un nombre aussi limité que possible d'autres machines soient contaminées. Une fois de plus, le marché attendait impatientement cette technologie. CheckPoint reste donc un acteur dynamique sur le marché de la sécurité : avec Application Intelligence et Interspect, les techniciens israéliens ont garanti l'avenir de leur entreprise pour deux ou trois ans sans problème.

JAN GULDENTOPS



Avec **CtrlSafe**, faites des affaires en toute sécurité!

CtrlSafeTM
by Saphico • • • • •

Si les nouvelles technologies n'ont pas de secret pour les PME, elles les exposent néanmoins à de nouveaux risques. **CtrlSafe**, la nouvelle solution modulaire développée par Saphico, maintient le niveau de sécurité de votre entreprise à hauteur de son évolution technologique. Avec CtrlSafe, vous devancez les risques. Externes et internes.

CtrlSafe propose à votre entreprise plusieurs fonctions de sécurité: analyse de la situation, protection contre les vols d'informations et les virus, contrôle des accès Internet et du courrier, protection de l'ensemble de votre réseau privé virtuel, rapports de tous les échanges suspects, contrôle à distance des tentatives d'intrusion (24 heures sur 24), blocage du spam dans toutes les directions, etc.

Saphico Industriepark 2M 9031 Drogen, tél. 09/280 75 85, fax 09/280 75 70, web www.saphico.be

Plus d'info au n° gratuit **0800 300 66**



Saphico a développé
CtrlSafe avec
ses partenaires



Microsoft[®]
CERTIFIED
Partner

SONICWALL

Peace of mind ...

Complete and
tailor-made security
solutions for your
company.



SkillTeam Security Services

- ▶ Firewalls & VPN
- Anti Virus & Content Filtering
- Access Management
- Intrusion Detection & Prevention
- High Availability



SkillTeam s.a. / n.v.

Av. de Roodebeeklaan 89 | Tel.: + 32 2 743 49 00
B - 1030 Brussels | Fax: +32 2 743 49 01

SkillTeam Luxembourg

1, Ceinture um Schlass
L - 5880 Hesperange

Tel.: + 352 36 95 95-1
Fax: +352 36 95 50

SkillTeam



Company Profile

SkillTeam, an IBM Company, delivers integrated value added ICT solutions and services in Belgium and Luxembourg, such as:

- **Design, architecture and implementation of Network and Server Infrastructures**
- **Security Solutions & Services**
- **Remote and Onsite Infrastructure Management**
- **Helpdesk and Support Solutions**
- **iSeries Solutions**
- **Application Development and Integration.**

Security is since long one of our core competences. Nowadays companies need to open up their corporate networks to the outside world, providing customers, partners and employees secured access to company applications and data.

Networks and applications need to be accessible, available, and manageable while maintaining a high level of security.

SkillTeam Security Solutions and Services can help you to achieve these goals. We design, implement and maintain security solutions that respond effectively to your business needs. Our competence and our professional approach, combined with first class hardware and software solutions from our business partners, guarantee robust security implementations that will fully protect your networks from external and internal threats.

....and provide you with the peace of mind you need

SkillTeam Belgium

Contact:

Avenue de Roodebeeklaan 89, 1030 Brussels

Tel. +32 2 743 49 00 - Fax. +32 2 743 49 01

web: <http://www.skillteam.com>

Mail: info@skillteam.com



It's going to shine cats and dogs this afternoon. Or however that old sayings goes. I've never been very good at remembering proverbs.

AVAILABLE AROUND THE GLOBE

IT Manager up to old tricks

After deploying a Nokia remote access solution, Amanda Mitchell, 31, enjoys more "alone time" at the office



"Amanda was always the crazy one," said her colleague Riza Guzman. "But for a while there she went very quiet - she seemed stressed - not her old self, but it all seemed to change with the implementation of the Nokia VPN solution. She reintroduced hallway races and the wacky Friday tie day that had become so popular. She's a riot and I am so glad she's back."

"The system came fully configured and integrated seamlessly into the network." Amanda was heard telling colleagues at the water cooler, "and with Seamless Integration, Nokia First Call - Final Resolution support, I know I am never alone - It's just so comforting to know there is someone out there who is willing to help. I've been able to use

Nokia Horizon Manager to centrally update security software and automate maintenance tasks for all remote offices, so now I don't suffer from jet-lag like I used to. At a recent IT industry seminar Amanda was seen chatting with her good friend Daniel He about her new lease on life, result of Nokia's best of breed network solutions - "The force and front line staff securely access data and sensitive information virtually anywhere with increased reliability." - "Yeah," said - "We just got over it and do you know what we discovered?" "What?" Amanda - "This amazing Mongolian BBQ restaurant three blocks from the office." He replied. Unconfirmed state that Amanda is stunned by this news

Nokia remote access solutions keep the people that matter connected wherever they are.

Employees, partners, customers and prospects all require quick, easy access to information over your corporate network. With Nokia and Check Point Software Technologies you can give it to them - securely and reliably. With award-winning VPN gateway and client solutions, connections are private, authenticated and authorised. What's more, the system comes



pre-configured and hardened on our purpose-built IP network security platform so it is fast to deploy and easy to manage. And, should you need it, we offer global, 24/7, First Call - Final Resolution support so you can focus on other things - like relaxing a little.

To have more fun, please contact:



NOXS Belgium (Trade Name of COMSOL nv/sa)
Koningin Astridlaan, 59/10
Avenue Reine Astrid, 59/10
1780 Wemmel - BELGIUM

Tel: +32 (0)2 461.01.70 - E mail: info@be.noxs.com
Fax: +32 (0)2 461.01.30 - http://be.noxs.com

Testimonials are fictionalised and do not depict actual Nokia customers. Copyright © 2003 Nokia. All rights reserved. Nokia and Nokia Connecting People are registered trademarks of Nokia Corporation. Other product and company names mentioned herein may be trademarks or trade names of their respective owners.

Number One for Excellence in Security



Profile

NOXS is the European Authority in Value Added Distribution, representing the **world's best authoring companies in the field of network security and e-business infrastructure**. As distributor, NOXS offers ICT-security products and (managed) services to its channel partners, who provide complete solutions to enterprises of all nature and magnitude - small, medium, and large - both locally and internationally.

NOXS is the common brand name of all the distributors of the Unit4Agresso group [U4AGR, Euronext Amsterdam] present today in 5 countries in Europe: the Netherlands, Germany, Ireland/UK and Belgium. NOXS is the new commercial name of COMSOL nv/sa.

The international dimension gives rise to significant economies of scale with regard to resources available, which **provide the company's resellers and vendor suppliers with competitive advantage and business opportunities**. By means of the pan-European collaboration, the company offers a significant volume as well as range of Best of Breed products and (managed) Services, **including Nokia Enterprise Solutions**.



About NOKIA Enterprise Solutions

Enterprise Solutions is the arm of Nokia dedicated to helping businesses and institutions worldwide improve their performance through extended mobility. Its end-to-end solution offerings range from business optimized mobile devices on the front end, to a robust portfolio of mobile business optimized gateways in the back end including: wireless email and internet, application mobility, message protection, virtual private networks, firewalls, and intrusion protection. As the global leader in mobile enterprise voice, Nokia Enterprise Solutions is well positioned to help companies mobilize data and free their workforces, while ensuring the security and reliability of their networks

For complete Solutions details and Knowledge Service Offering, please call, write or visit us at:

NOXS Belgium

(Trade Name of COMSOL nv/sa)

Koningin Astridlaan, 59/10
Avenue Reine Astrid, 59/10
1780 Wemmel - BELGIUM

Tel: +32 (0)2 461.01.70 - E mail: info@be.noxs.com
Fax: +32 (0)2 461.01.30 - <http://be.noxs.com>

- Anti-Virus
- Bandwidth Management
- Firewalls
- Intrusion Detection
- Content Management
- Web Filtering
- 24/7 Availability
- Traffic Management
- Server Analysis and Reporting
- Portals
- Web Switching
- Appliances
- PKI
- Training
- Hot Standby
- SLA support
- VPN

Security Solutions

TELINDUS

Security experts have begged their management for years for respect and struggled to get IT Security on the corporate road map.

Are corporations prepared to embrace the change?

In most organisations, there is a growing expectation that risk managers will not only be able to track and manage all forms of operational risk, but also report it on enough detail, to satisfy the board of directors and the government that is being adequately managed.

Telindus, the Belgian leader in security has a wide expertise and solutions that help companies to achieve a risk based approach and implement countermeasures to decrease company risks.



The solutions cover domains such as:

- Security Officer Support
- Security Reviews
- Penetration Testing
- Identity Management
- Internet Access Street
- One Care Connectivity
- Security in the Cloud
- Intrusion Prevention
- Internet Productivity Management
- Security Management Tools
- Mobility
- Managed Security Services

By implementing these solutions, you can increase the security posture of your company, taking into account the most urgent risks and allocating budgets where needed.

We would like to meet you at INFOSECURITY
10-11 March 2004 at Brussels Kart
Be Secure. Be There.



TELINDUS NV • GELDENAACKSEBAAN 335 • B-3001 Heverlee
Tel: +32 (16) 38 20 11 • Fax: +32 (16) 40 01 02

TELINDUS

Telindus



Company Profile

The publicly listed Telindus Group (Euronext Brussels, ticker TEL) is a one-stop service partner, solution provider and manufacturer for fixed and mobile networks.

Telindus, the Integrator, has extensive expertise, encompassing consulting, integration and managed services, in all areas of modern telecommunications applications and technologies for local area networks (LAN), metropolitan area networks (MAN), wide area networks (WAN), virtual private networks (VPN), network access and security, surveillance and networked applications.

Telindus is a manufacturer of broadband access and video surveillance solutions. Combined with

a large networking product portfolio of strategic suppliers and partners, Telindus is the best route to leading edge technology and best of breed products and services for both operators and enterprises. Since its foundation in 1969, Telindus has made significant investments in establishing a solid footprint in networking and security expertise in Europe and beyond.

With a full operational presence in as many as 14 countries across Europe and South East Asia and almost 2,200 employees, Telindus provides customers with both business and technology based solutions. Telindus' own products are distributed by an extensive network of agents across the globe.



Telindus Belgium

Contact: Luc Van Utterbeeck

Head of Marketing & Alliances

Geldenaaksebaan 335 - B - 3001 Heverlee

Tél.: 016/38.28.69 - Fax: 016/40.01.02

Mail: info@telindus.be - Web: www.telindus.com



Chaos.



Control.

Take control of your Internet security.

Introducing Proventia™ Enterprise Protection Products. Just because Internet threats are complex, doesn't mean your security has to be. Finally, a single, unified protection appliance that protects more with less, eliminating the cost and chaos of multiple stand-alone security products. Proventia™ centrally-managed products range from detection up to completely unified and proactive multi-function protection appliances, combining firewall, intrusion prevention, web filtering, anti-spam and anti-virus technologies. Take control of your enterprise security. Switch to Internet Security Systems today. +32 2 479 6797. www.iss.net/emea.



**INTERNET
SECURITY
SYSTEMS®**

Internet Security Systems



Company Profile

What We Do:

Internet Security Systems provides network security products and services that protect against Internet threats. ISS helps organizations understand their threat environment, identify what to protect and choose the security solution that best meets their needs. All Internet Security Systems solutions are based on world-renowned security intelligence and the most up-to-date information on threats and vulnerabilities. In addition, Internet Security Systems protects its customers around-the-clock with managed services.



The Problem We Address:

Internet risks are increasing as more enterprises connect with customers, partners, vendors and employees via the Web, exposing business systems and information to online risk. Each day, new vulnerabilities in software are discovered and new online attacks are created and unleashed that bypass traditional security products like firewalls and anti-virus. The endless task of patching software vulnerabilities puts proactive protection further out of reach. Unfortunately, the current approach to network security - a collection of stand-alone technologies, including anti-virus, firewalls, intrusion detection and prevention, content filtering and anti-spam - adds complexity and cost without truly solving the problem. Internet Security Systems' pro-

ducts and services protect against all threats in a way that makes sense and delivers maximum value.

How We Do It:

Internet Security Systems' network security products and services deliver advanced protection at lower cost. All ISS offerings are based on the most up-to-date security intelligence available conducted by ISS' X-Force® research and development organization, the unequivocal world authority in vulnerability and threat research. ISS security services help organizations assess their risk, identify critical assets, then design and deploy a protection solution. Depending on the organization's security resources, Internet Security Systems offers 24/7 monitoring and management and hands-on security education and training.

Internet Security Systems

Contact: Wim Temmerman - Country Manager Belux

Ringlaan 39 box 5

B - 1853 Strombeek-Bever, Belgium

Phone: 02/479.67.97 - Fax: 02/479.75.18

Mail: belux-info@iss.net - Web: www.iss.net



UNISKILL

Am I at risk?
Am I under attack?
How should I respond to the attack?
How effective is the response?

Looking for answers?

www.uniskill.com

Caller ID:

Microsoft à la pêche aux spams

Microsoft a choisi de dévoiler les spécifications de sa nouvelle technologie anti-spam baptisée Caller ID lors de la conférence RSA qui s'est tenue à San Francisco en février. L'espoir: rendre plus difficile le masquage de la source d'envoi réelle d'un e-mail commercial non sollicité.

L'authentification de l'expéditeur recueille rapidement l'adhésion des spécialistes de l'e-mail et des ISP comme arme de lutte contre le spam. Dans le courant de février, Sendmail a annoncé qu'il développerait et distribuerait des technologies d'authentification de l'expéditeur à ses clients et à la communauté open source pour combattre le spam, les virus et les e-mails associés à des identités frauduleuses. Sendmail intègrera certaines technologies au sein du Mail Transfer Agent (MTA), notamment

sa syntaxe propre pour classifier les adresses de domaines, Caller ID de Microsoft utilise le langage XML.

SPF permet également d'analyser l'enveloppe de l'e-mail au niveau des gateways. Une partie de l'information sur le mail transite entre les serveurs avant que la totalité du message soit bel et bien envoyée. Les messages qui émanent de serveurs qui ne sont pas associés au bon domaine sont éliminés avant même leur envoi. De son côté, Caller ID analyse l'in-



DomainKeys qui est poussé par Yahoo, mais aussi "des propositions mises en avant par Microsoft et par d'autres", a déclaré un représentant de Sendmail. Un porte-parole de Microsoft a confirmé des rapports selon lesquels la compagnie s'apprête à lancer un plug-in d'authentification d'expéditeur parallèlement à Sendmail.

Caller ID est apparentée à d'autres propositions qui circulent parmi les grands ISP et les spécialistes de l'e-mail, a expliqué John Levine, co-président de l'Antispam Research Group, un organe indépendant rattaché à l'Internet Engineering Task Force. Elle est en particulier proche d'une technologie émergente appelée Sender Policy Framework (SPF) développée par Meng Wong, un chercheur indépendant. Wong travaille actuellement pour Pobox.com, un service d'email-forwarding. Au lieu d'analyser le contenu des mails pour détecter les spams, le protocole SPF permet aux administrateurs de domaines Internet de décrire leurs serveurs mails dans un registre lié à celui du DNS en utilisant un langage de description spécifique au SPF. Les autres domaines Internet peuvent alors rejeter tout message qui prétend venir de ce domaine alors qu'il n'a pas été envoyé par un serveur autorisé, a expliqué Wong. Pour l'efficacité du système, les administrateurs doivent fournir à Caller ID des listes des serveurs mails au registre DNS pour leurs domaines Internet. Là où le SPF uti-

lisation liée à l'adresse IP de l'expéditeur dans l'en-tête du message. Cela signifie que la totalité du message doit être téléchargée par le serveur mail destinataire avant qu'il puisse être accepté ou rejeté, a déclaré Levine. Selon les experts, la technologie Caller ID a ses forces et ses faiblesses. D'un côté, elle impose aux serveurs mails de télécharger la totalité des messages bidons, ce qui pourrait faire chuter leur performance. De plus, il ne vérifie que l'adresse IP de l'expéditeur, au lieu de scanner le contenu. Caller ID réclame de plus la connaissance du langage XML, ce qui rend l'implémentation plus compliquée. Enfin, la longueur supplémentaire imposée par le contenu XML obligatoire pourrait excéder la limite des 512 caractères pour les messages de réponse aux requêtes DNS, a expliqué Wong. Selon les spécifications DNS, les messages qui excèdent cette limite doivent transiter via un circuit Transmission Control Protocol séparé au lieu d'utiliser le User Datagram Protocol. Si c'est techniquement faisable, c'est rarement utilisé, ce qui introduit un élément d'incertitude quant à l'implémentation, ont reconnu Wong et Levine. "Cette fonction existe depuis 25 ans, mais n'a jamais été utilisée", a déclaré Levine. Cette technologie pourrait cependant donner de meilleurs résultats pour déterminer la source réelle d'un mail que le SPF, en particulier parce que l'enveloppe des adresses mails n'ont pas à correspondre à l'adresse de l'entête de l'e-mail. □



LUDOVIC GILLES ludovic.gilles@best.be

Spywares, à vous de vous protéger!

Dans l'esprit de nombre d'internautes, la sécurité informatique est exclusivement associée à la problématique des virus. C'est oublier un peu vite l'autre forme parasitaire que sont les spywares ou logiciels espions...

L'apparition subite de fenêtres pop-up et de courriers indésirables peut être révélatrice de la présence d'un spyware au sein de votre machine. Mais il existe d'autres formes de logiciels espions dont les conséquences peuvent être beaucoup plus lourdes. Les dialers, par exemple, connectent l'ordinateur à Internet via des numéros téléphoniques surtaxés. D'autres parasites collectent les données confidentielles saisies au clavier comme les numéros de carte bancaire, les mots de passe, etc. Certains vont même jusqu'à exploiter la machine victime pour envoyer des spams, voire effectuer des virements bancaires que l'utilisateur ne découvre qu'à la réception de son relevé de compte. Connexions sécurisées et antivirus n'y peuvent pas grand-chose puisque le logiciel espion s'installe généralement au cœur même du système d'exploitation qui, s'il n'est pas administré avec la sécurité minimale, répond automatiquement à leurs requêtes. D'autre part, lorsqu'un spyware fonctionne en binôme

avec un tel logiciel espion qui tourne sur son ordinateur. Car si des logiciels comme Gator et WhenU se doivent de prévenir le consommateur qu'il s'apprête à télécharger leur programme, l'information est souvent perdue au milieu des conditions générales d'utilisation des logiciels avec lesquels ils sont couplés. Mais même préalablement informé d'un éventuel tracking, l'utilisateur n'en reste pas moins soumis à une surveillance dont la nature peut s'avérer illégale du point de vue de la législation. L'analyse de sa navigation sur internet peut ainsi par exemple permettre de déduire et de stocker des informations - réelles ou supposées - sur ses origines raciales, ses opinions politiques, philosophiques ou religieuses ou encore son appartenance syndicale, ce qui est interdit chez nous sans le consentement de l'intéressé.

Quelques règles à respecter

Depuis les scandales provoqués en 1999 par la découverte de spywares dans SmartUpdate (Netscape) et RealJukeBox (Real Networks), la pratique est devenue plus transparente dans le cas des

Certains spywares vont jusqu'à exploiter la machine victime pour envoyer des spams, voire effectuer des virements bancaires que l'utilisateur ne découvre qu'à la réception de son relevé de compte.

me avec une application, l'utilisateur, en autorisant les connexions Internet, permet la sortie des informations sur le réseau. Le meilleur des firewalls est impuissant face à cette stratégie.

"Savoir contrôler son environnement"

Aux utilisateurs de se protéger! En effet, un juge fédéral américain n'a récemment rien trouvé de répréhensible aux pratiques commerciales de la société de marketing WhenU. Elle permet à ses clients de faire de la publicité sur les sites de leurs concurrents par le biais de "pop-ups" (fenêtres automatiques). Selon le magistrat, ce sont les internautes eux-mêmes qui ont «invité» ces pop-ups à apparaître, en téléchargeant volontairement le spyware. «Au bout du compte, c'est l'utilisateur de l'ordinateur qui contrôle comment les fenêtres peuvent apparaître sur son écran», écrit-il dans sa décision, que s'est procuré le Wall Street Journal. Pourtant, l'internaute n'est pas tou-

jours conscient d'avoir un tel logiciel espion qui tourne sur son ordinateur. Quelques règles simples peuvent être observées :

- lisez attentivement les conditions d'utilisation d'un logiciel avant de l'installer. L'existence d'un spyware commercial et de ses fonctionnalités annexes y sont normalement signalées, même si tout est fait pour que l'utilisateur évite de lire lesdites conditions.
- réfléchissez bien avant de dévoiler des informations personnelles.
- n'acceptez pas sans réfléchir les programmes supplémentaires éventuellement proposés lors de l'installation d'un logiciel.
- installez un firewall personnel et surveillez les demandes d'autorisation de connexion à internet, afin de détecter toute application suspecte.
- informez-vous auprès de sites spécialisés.
- gardez enfin à l'esprit qu'installer un logiciel n'est jamais une opération anodine: cela revient à autoriser le programme à effectuer toutes les opérations qu'il souhaite sur votre disque dur. □