LIVRE BLANC

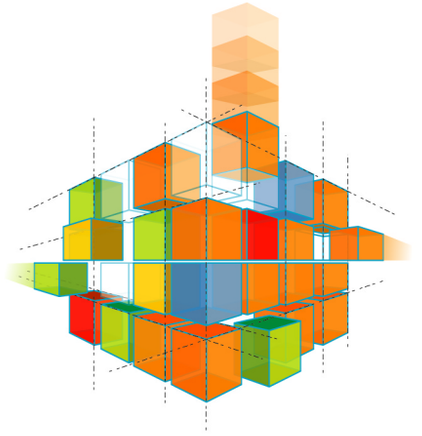
AVRIL 2007

LE FILTRAGE DE CONTENUS

FACTEUR D'ÉCONOMIE ET DE PRODUCTIVITÉ

ARKOON NETWORK SECURITY

Conçu initialement comme une simple technique de dépollution des boîtes aux lettres électroniques, l'antispam devient plus global et plus incontournable que jamais. Il aide à lutter contre les vers et virus ainsi que contre le phishing et ses faux sites Web. Il maintient la productivité des utilisateurs au meilleur niveau. Et il préserve la bande passante du réseau d'entreprise.



ADAPTIVE SECURITY

AMC SSL360 FAST360 Security BOX

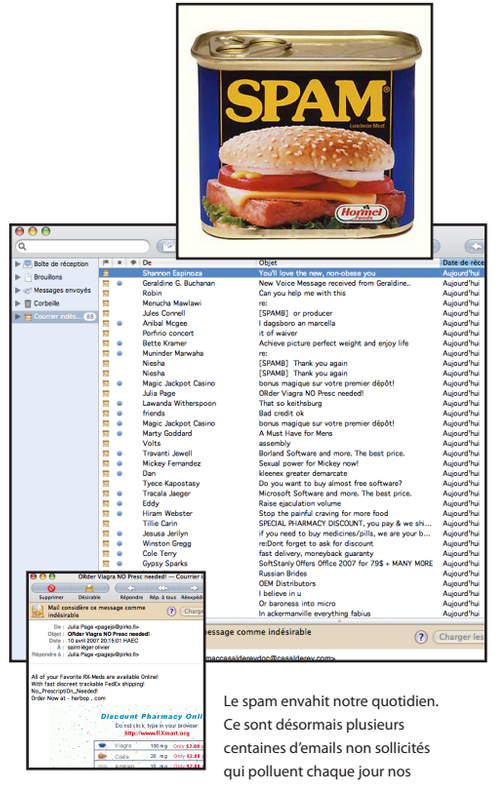
LE SPAM VÉHICULE PLUSIEURS MENACES NUMÉRIQUES

MESSAGES NON SOLLICITÉS, ARNAQUES ET VIRUS INFORMATIQUES GAGNENT EN AMPLEUR AVEC LA POPULARITÉ DE LA MESSAGERIE INTERNET. ILS IMPOSENT L'IDENTIFICATION ET LE FILTRAGE SOIGNÉS DES CONTENUS NUMÉRIQUES.

Le spam désigne plusieurs formes de publicité indésirable depuis près d'un siècle. L'origine du terme ? Une conserve peu appétissante destinée aux militaires américains : le « Spicy Ham ». Ce jambon épicé (dit spam en abrégé) a fait l'objet d'une réclame martelée dès la fin des années 1930, avant de donner naissance à un sketch satirique des Monty Python. Avec l'essor de la messagerie Internet dans les entreprises et auprès du grand public, le spam définit à présent les mémos électroniques qui polluent, quotidiennement, nos boîtes aux lettres. Ces messages promettent d'illusoires remèdes ou fortunes et cachent parfois des pièges plus élaborés, comme le phishing, une technique visant à détourner les identifiants bancaires des destinataires, par le biais de fausses banques en ligne. Au détour d'une image ou d'une pièce jointe, en apparence anodine, le spam peut ajouter au système d'exploitation un logiciel espion ou une porte dérobée. La meilleure destination de ce courrier parasite reste donc la poubelle.

Le tri manuel des spams engendre une perte de productivité individuelle et un manque à gagner conséquent pour l'entreprise, à mesure que le nombre de spams augmente. Distribuer tous les courriers électroniques sans distinction requiert aussi une bande passante accrue sur le réseau d'entreprise et un volume de stockage de plus en plus important.

C'est la raison pour laquelle, les entreprises tout comme les fournisseurs d'accès Internet recherchent des solutions de filtrage à la fois efficaces et rentables. Car les courriers indésirables représentent, à l'échelle mondiale, un coût total de 39 milliards de dollars, estime le cabinet d'études Ferris Research. L'objectif du spam consiste souvent à conduire l'internaute vers des services d'informations, des offres financières ou vers une pharmacie virtuelle. Ses liens hypertexte (URL) mènent parfois vers des jeux ou des paris en ligne. Pour se rendre crédible à vos yeux, le spammeur n'hésitera pas à emprunter l'adresse Internet d'un de vos collaborateurs. Pire, il profitera aussi de votre messagerie instantanée, d'un port ouvert ou d'une faille système pour projeter, de façon intrusive, ses messages publicitaires. Cette fenêtre Windows qui surgit en prétendant avoir détecté un virus vous incite-t-elle à télécharger une nouvelle protection ? Méfiance : en fait de remède, le code proposé pourrait être un cheval de Troie ou un logiciel espion capturant la saisie de vos mots de passe au clavier.



Le spam envahit notre quotidien. Ce sont désormais plusieurs centaines d'emails non sollicités qui polluent chaque jour nos boîtes électroniques, dégradant par là même les performances globales du réseau.

Incidence par contenus néfastes	Performances systèmes	Bande passante du réseau	Productivité des utilisateurs	Confidentialité des informations	Sécurité de l'infrastructure
Virus, vers	FORTE	FORTE	FORTE	FORTE	FORTE
Spam	MOYENNE	FORTE	FORTE	NÉGLIGEABLE	NÉGLIGEABLE
Phishing	NÉGLIGEABLE	NÉGLIGEABLE	MOYENNE	FORTE	NÉGLIGEABLE
Site Web malveillant	MOYENNE	MOYENNE	MOYENNE	MOYENNE	MOYENNE
Key logger	MOYENNE	MOYENNE	NÉGLIGEABLE	FORTE	FORTE
Cheval de Troie	FORTE	MOYENNE	MOYENNE	FORTE	FORTE

PLUSIEURS TECHNIQUES POUR FILTRER LE SPAM

POUR LE DESTINATAIRE, LA MEILLEURE DESTINATION DU POURRIEL RESTE LA POUBELLE. CORRECTEMENT PARAMÉTRÉE, L'UTM DÉBARRASSE AUTOMATIQUEMENT LE SPAM SANS ÉVINCER LES MESSAGES LÉGITIMES.

Avant de proposer une solution de filtrage antispam, il convient de s'interroger sur ce qu'est réellement un spam pour chaque groupe de travail dans l'entreprise. Les métiers exercés facilitent la distinction entre message légitime et spam. Dans un centre hospitalier, par exemple, l'usage de filtres de contenus sur l'anatomie humaine ou sur le nom de certains médicaments pourra bloquer des mémos importants pour l'utilisateur. De même, la détection de tons « chair » dans les images jointes s'avère inappropriée dans ce cas. Contrairement à l'antivirus, l'antispam ne doit pas stopper 100% des messages a priori suspects. Il exige un paramétrage fin et la faculté de retrouver d'éventuels faux-positifs.

L'équipement UTM intervient dès la périphérie du réseau, en filtrant les messages électroniques à leur arrivée afin d'éviter le cheminement du spam sur toute l'infrastructure d'entreprise. Il réduit ainsi le risque de saturation ou de surdimensionnement du réseau. Il regroupe plusieurs techniques de filtrage pour distinguer le spam sans introduire d'erreur d'interprétation, ce qui n'a rien de trivial.

Les premières techniques de filtrage portent sur l'adresse de l'émetteur. De véritables « listes noires » d'expéditeurs sont ainsi formées puis échangées pour freiner l'expansion du spam par comparaisons d'adresses. Mais cette approche se révèle insuffisante car de nombreux spammeurs renouvellent l'émetteur à chaque envoi dorénavant. L'usage de véritables réseaux de PC « zombies » facilite le pillage des carnets d'adresses et le relais du spam. L'antispam ajoute aux listes noires un second mode de filtrage qui porte, cette fois, sur le contenu du message. Plusieurs techniques sont alors possibles. Une approche est comparable au moteur antivirus : une signature est définie pour chaque spam connu grâce à un algorithme de hachage. Puis les messages reçus sont comparés aux empreintes. Cette technique requiert une mise à jour fréquente des bases de signatures pour stopper les nouveaux spams. Pour forcer le passage, les spammeurs modifient quelques mots dans le corps du message, à chaque envoi. Du coup, la comparaison effectuée entre les contenus, est déjouée.

Les autres approches statistiques, pour efficaces qu'elles soient, requierent souvent un important travail au niveau de la maintenance. Avec les filtres sémantiques et les statistiques Bayesiennes, l'utilisateur - ou l'administrateur - est mis à contribution. Il perfectionne le moteur antispam au travers d'un apprentissage réduisant le taux d'erreurs de détection. Plus ce travail de corrections est personnalisé et régulier, plus le filtrage se révèle efficace.

UNE BATAILLE SANS FIN

Les auteurs de spam et les éditeurs d'antispam se livrent une véritable partie d'échecs. L'objectif du spammeur consiste à atteindre sa cible. Il doit donc contourner les toutes dernières méthodes d'analyse mises au point. Le remplacement de certains caractères par des caractères aléatoires ('@#%) a confondu la première génération d'outils à base de dictionnaires. Les images jointes étant maintenant analysées par OCR, des images gif animées sont utilisées tandis que de petits traits colorés viennent brouiller les algorithmes de lecture automatique. Tant que les spammeurs trouveront de nouvelles astuces, le filtrage devra évoluer.

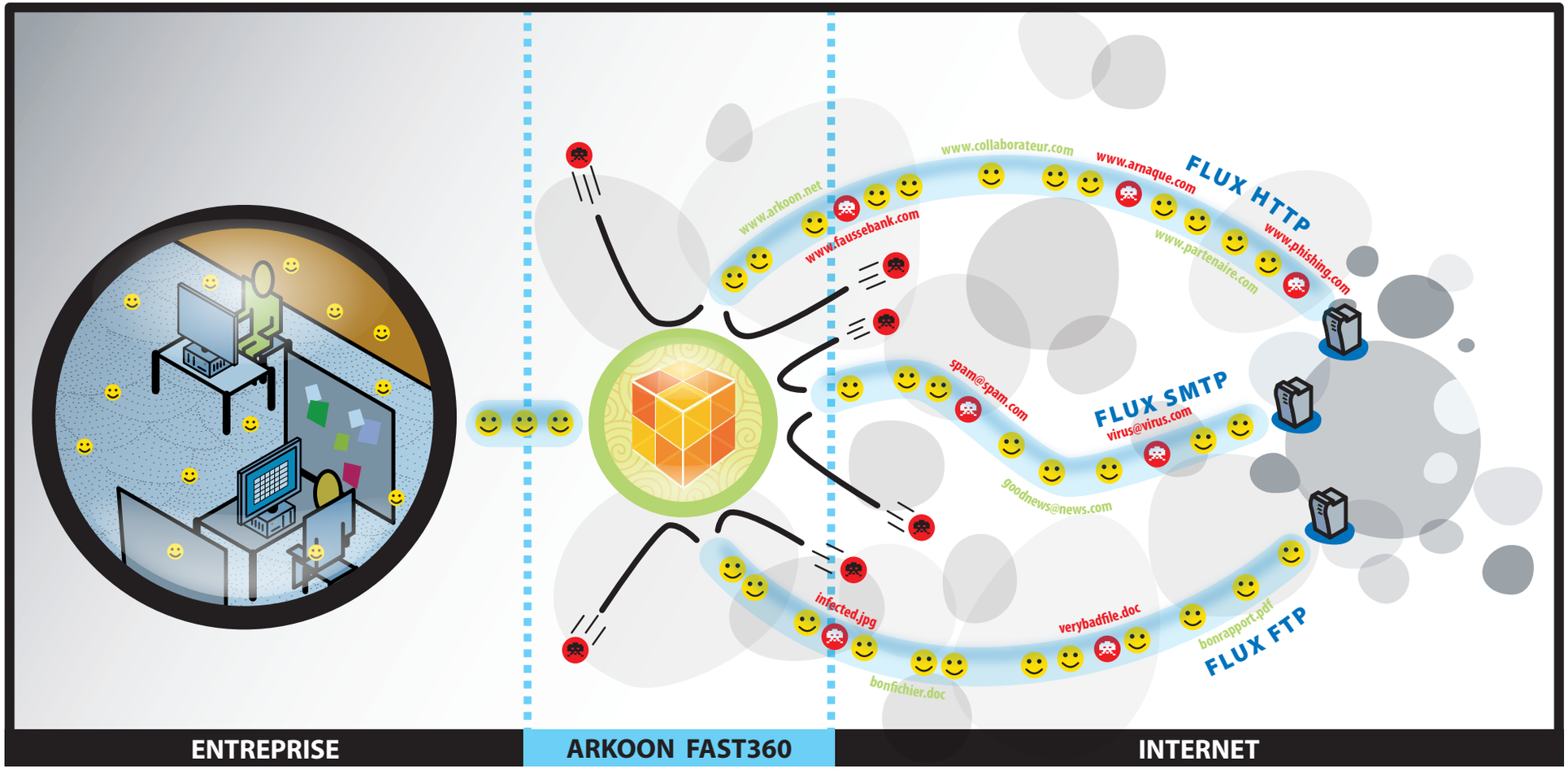
UNE BONNE COHÉRENCE DES RÈGLES

L'équipementier Arkoon regroupe sous la console d'administration de son appliance FAST360 toutes les règles de filtrage, d'authentification, de lutte contre le spam et tous les codes malveillants. Cela sécurise les équipements du réseau d'entreprise, les serveurs et les postes de travail, tout en limitant l'accès aux sites falsifiés (le phishing). Le moteur antispam étant exécuté au niveau du noyau de l'architecture SSA (Scalable Security Architecture) d'Arkoon, la vitesse de traitement est jusqu'à huit fois supérieure à celle des moteurs concurrents. Cette position centrale optimise aussi les échanges d'informations entre l'antispam, l'antivirus et le coupe-feu ; elle permet un filtrage mieux coordonné et global.

Dès la propagation d'un nouveau ver ou virus par le biais d'un message non sollicité, l'antispam Arkoon intercepte la menace avant même que la signature antivirale ne soit transmise. La console d'administration unifiée réduit aussi les coûts d'administration et de possession du boîtier UTM. En effet, l'entreprise multisite peut mutualiser l'administration des services de sécurité et réduire ainsi, de façon significative, ses coûts d'exploitation. Simple à installer, à paramétrer et à utiliser, l'UTM Arkoon facilite la tâche de l'administrateur et celle des utilisateurs. Par exemple, le téléchargement régulier et sécurisé à partir des serveurs Arkoon assure une mise à jour constante des règles de filtrage. Cet automatisme protège le réseau d'entreprise contre les dernières menaces ; il évite aussi aux utilisateurs locaux et distants de visiter des sites interdits ou potentiellement dangereux pour l'activité de l'entreprise.

L'UTM, UN BOUCLIER EFFICACE CONTRE LES MENACES INTERNET

L'INFORMATION DE VOTRE ENTREPRISE CIRCULE SUR VOTRE RÉSEAU INTERNE, MAIS AUSSI AU-DEHORS, VIA LES ORDINATEURS PORTABLES, LES PDA, LES SERVICES EN LIGNE OU L'EXTRANET DE VOS PARTENAIRES. L'APPLIANCE FAST360 D'ARKOON INSPECTE TOUS LES ÉCHANGES POUR GARANTIR LA SÉCURITÉ ET LA CONFIDENTIALITÉ DE VOS INFORMATIONS.



SPANGHERO PROTÈGE SES FLUX VOIX-DONNÉES CONVERGENTS

POUR PRODUIRE ET COMMERCIALISER DAVANTAGE DE PLATS CUISINÉS, SPANGHERO S'APPUIE SUR UN RÉSEAU CONVERGENT. LES FLUX VOIX ET DONNÉES SUR IP SONT ANALYSÉS ET FILTRÉS PAR UN COUPLE DE BOÎTIERS ARKOON. LES APPLIANCES A200 ET A210 D'ARKOON FORMENT UNE COMBINAISON ROBUSTE POUR LE FILTRAGE DES SPAMS ET DES CONTENUS NUMÉRIQUES.

Les frères Spanghero ont créé, en 1970, l'entreprise agro-alimentaire qui porte leur nom, à Castelnaudary. Avec cinq cent salariés et un chiffre d'affaires de plus de 100 millions d'Euros, l'entreprise est engagée, depuis trois ans, dans une démarche qualité. Son activité de plats cuisinés a reçu la certification I.S.O. 9001 (Version 2000) ; cette politique s'étend maintenant aux autres services. Le système d'informations repose sur une infrastructure IP de bout en bout. Les collaborateurs échangent leurs données en toute sécurité, sur le terrain, au siège ou depuis le site de préparation de porcs du Tarn, grâce au réseau local et aux liens privés virtuels (IPSEC).

Depuis l'an 2000, l'augmentation des codes malveillants transmis par Internet, le canal de communication emprunté par un nombre croissant de clients et partenaires de Spanghero, a contraint l'entreprise à envisager le déploiement d'une solution de sécurité globale : « *plusieurs dizaines d'attaques virales quotidiennes menaçaient l'intégrité des données et celle des postes de travail reliés au serveur de fichiers partagés. Une première boîte noire Cube d'Arkoon, regroupant les fonctions de parefeu, d'antivirus et de filtrage d'URL, a permis d'isoler le réseau local des liens étendus* », explique José Marson, le responsable du système d'information. La boîte noire installée en 2002 par l'intégrateur SCC de Toulouse filtre les flux web (HTTP) et ceux de la messagerie SMTP.

Fin 2004, la migration vers un boîtier A200 d'Arkoon permet à Spanghero de créer une zone démilitarisée pour héberger ses serveurs partagés sous l'environnement Windows Citrix, pour la messagerie et la bureautique. Le boîtier Arkoon A200 disposait de quatre ports Ethernet contre deux pour le précédent. Il permet, en outre, la création de tunnels sécurisés IPSEC pour chiffrer les échanges entre le siège et les utilisateurs distants. Sa console d'administration, plus évoluée, fournie une visibilité globale des connexions au système d'information : « *Avec près d'une centaine de postes distants accédant au réseau du siège depuis l'extérieur, nous avons dû soigner la configuration des droits d'accès. Les commerciaux nomades de Spanghero utilisent, pour leur part, une solution VPN et une messagerie mobile gérées par l'opérateur Orange* », explique José Marson.

Pour plus de sécurité, les lecteurs de médias amovibles ont été retirés des ordinateurs portables et les ports USB sont débrayés, limitant tout risque de contamination virale par une clé USB. Depuis l'été 2006, une seconde appliance A210 complète l'A200 à Castelnaudary. Il apporte une redondance précieuse en cas de panne et aussi de nouvelles facultés de filtrage : « *le nouveau appliance A210 Arkoon filtre davantage de contenus et il est particulièrement bien adapté à notre trafic voix-données sur IP. Nous avons pu mettre en oeuvre les fonctions antispam et alléger les boîtes aux lettres électroniques. La formation est rapide et l'exploitation peu exigeante. La combinaison de deux appliances Arkoon installées sur le réseau du siège social nous offre une grande autonomie d'administration* », apprécie le responsable informatique de Spanghero.

FILTRAGE, TUNNELS VPN ET PAREFEU INTÉGRÉS

Comme la plupart des entreprises reliées par Internet, la société Spanghero perçoit le réseau mondial comme une opportunité - pour dialoguer avec ses clients et élargir sa zone de chalandise -, mais aussi comme une menace permanente. Se prémunir des vers informatiques, des virus et des spams polluant son propre réseau est devenu indispensable dès l'an 2000. Dans le secteur agro-alimentaire, la traçabilité des biens est primordiale. Celle des flux voix-données suit une même démarche rigoureuse à Castelnaudary avec deux appliances de sécurité redondantes. Outre le filtrage des contenus, les deux UTM Arkoon établissent les tunnels chiffrés et assurent la gestion des accès distants, via une seule et même console d'administration.

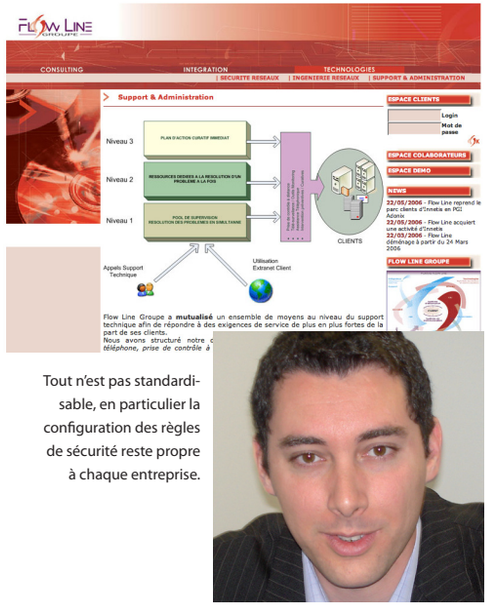
L'APPLIANCE UTM AU CŒUR D'UNE STRATÉGIE GAGNANTE

LA LUTTE CONTRE L'INTRUSION ET LES ACCÈS FRAUDULEUX PEUT S'ORGANISER AUTOUR D'UN BON NOYAU COUPE-FEU. A CONDITION D'ORCHESTRER SOIGNEUSEMENT LA CONFIGURATION DU BOÎTIER UTM ET SA SUPERVISION. LE CENTRE D'OPÉRATIONS DE FLOW LINE TECHNOLOGIES FORME UN SOCLE POUR GARANTIR LA GESTION ET L'ÉVOLUTION DES RÈGLES DE SÉCURITÉ.

A quoi bon acheter les coffres forts les plus robustes si on conserve la combinaison triple-zéro ? Le secret d'une bonne sécurité informatique, c'est une combinaison gagnante partant d'un très bon produit, bien intégré, avec une bonne administration et un support sans faille. Tous ces aspects doivent être étudiés avec attention », recommande Sébastien Gas, le DG de Flow Line Technologies, un spécialiste des solutions d'infrastructure et sécurité.

Avec 400 appliances UTM d'origine Arkoon, administrées à distance pour les PME clientes, le prestataire lyonnais a mis au point des procédures efficaces de remontées de sauvegardes (lire l'encadré ci-contre). En effet, l'efficacité du filtrage numérique dépend d'une configuration « aux petits oignons ». Il s'agit d'intégrer au moteur coupe-feu, l'authentification des utilisateurs, l'antivirus, l'antispam et le filtrage d'URLs notamment. Mais, dans cette initiative, on se heurte à un paradoxe : moins on enregistre de règles, plus le système est fonctionnel.

« *Il s'agit donc de trouver le bon équilibre entre la sécurisation du réseau et la productivité de l'entreprise. Or, il n'existe pas d'automatisation possible à ce niveau* », observe Sébastien Gas. Pour une sécurité parfaite, il faut donc personnaliser la solution, « travailler en relation étroite avec les règles de l'entreprise ». C'est pourquoi l'équipe Flow Line Technologies compte une vingtaine de personnes déroulant une méthodologie globale, susceptible d'offrir une sécurité informatique à 360 degrés : sur les accès, les échanges, la mobilité, le réseau local et les systèmes, avec un plan de reprise d'activités à la clé. « *Nous parvenons à industrialiser le management de la sécurité, mais pas son implémentation. On configure donc deux éléments : le noyau de base de l'UTM et son administration à distance* ».



Tout n'est pas standardisable, en particulier la configuration des règles de sécurité reste propre à chaque entreprise.

En pratique, deux cas de figure se présentent : l'entreprise sans compétence interne en sécurité informatique se tourne volontiers vers l'appliance UTM car il répond à 80% des besoins standards de sécurité. Il faut néanmoins trouver des partenaires souples et à l'écoute pour le gérer. « *Arkoon est très réactif sur l'UTM et propose des adaptations rapides, une nouvelle ingénierie ou une autre source OEM dès qu'un service de sécurité n'est plus en adéquation avec le marché* », apprécie Sébastien Gas. Deuxième cas de figure, les sociétés en quête de solutions plus expertes, retiennent généralement une solution hétérogène, présentant forcément des compromis. Arkoon reste une brique centrale d'expertise grâce à son noyau de sécurité avancé, sa technologie FAST. En fonction du cahier des charges des services de sécurité, un compromis entre l'UTM et des solutions dédiées pourra être retenu.

UN NOC POUR MIEUX GÉRER L'UTM

Basé à Lyon, Clermont-Ferrand et Paris, Flow Line conseille les PME du MidMarket cherchant à mieux gérer les risques apportés par Internet ou par les ordinateurs portables des salariés (Virus, codes malveillants, etc.). Ces nuisances causent des pannes à répétition et des interruptions de services informatiques. Elles provoquent aussi une perte de productivité pour l'entreprise. « Il y a les menaces actuelles et aussi celles qu'on ne connaît pas encore aujourd'hui. Les deux doivent être prises en considération », précise Sébastien Gas. D'où le centre de services managés, le NOC (Network Operations Center) de Flow Line, structuré avec des compétences en supervision de réseaux sécurisés. Au minimum trois ingénieurs administrent, en permanence, l'infrastructure des clients. Ils garantissent que chaque dispositif rende bien le service prévu, à l'aide de procédures conçues pour déclencher l'alerte et offrir une reprise rapide d'activités en cas d'incident. Tandis qu'Arkoon apporte les mises à jour quotidiennes, directement sur l'UTM des sites clients, les ressources de Flow Line protègent les configurations de tous les équipements actifs. Elles assurent ainsi la stabilité, l'évolution et le support du système d'information : « Nous travaillons suivant une démarche collaborative avec nos clients, en délivrant des avis d'experts, certifiant que la mise à jour d'une règle ne mettra pas en péril la sécurité globale du réseau de l'entreprise ».

GLOSSAIRE

Antivirus : Logiciel ou équipement de protection contre les programmes maveillants, vers, virus, chevaux de Troie…

Antispam : Ensemble de systèmes et de moyens techniques et juridiques pour lutter contre le spam et contre les courriers électroniques publicitaires non sollicités

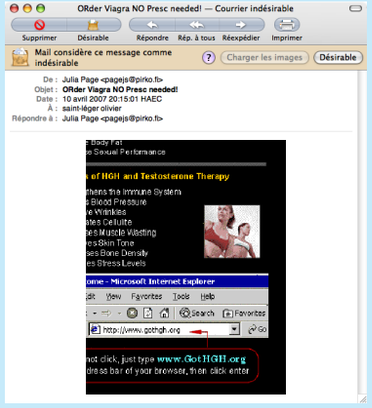
Courriel : Courrier électronique et traduction de l'e-mail anglais. Il désigne à la fois le message transmis et le service de transfert de messages par la messagerie électronique.

Hachage : La fonction de Hash, très utile au chiffrement et aux algorithmes de sécurité, associe à une chaîne de caractères un entier. Par extension, elle caractérise un vaste ensemble de données en une signature réduite à quelques octets seulement.

Hoax : Canular informatique, fréquemment relayé par l'utilisateur lui-même, de bonne foi, au travers de sa boîte aux lettres électroniques. Le Bonzai Kitten racontait ainsi le calvaire de chats, élevés en bocaux pour en brider la croissance à la manière des bonzaïs…

Phishing : Technique d'hameçonnage visant à usurper l'identité d'un utilisateur de service en ligne pour obtenir des renseignements comme l'identifiant et le solde bancaires, par le biais d'un site Web falsifié ou d'un spam.

Pourriel : Traduction française proposée pour le spam ; contraction de poubelle et de courriel.



Netiquette : Ensemble de règles de bon usage du courrier électronique.

Rogue : Faux anti-spyware. Proposé sur Internet, de façon non sollicitée le plus souvent, ce programme prétend éradiquer les logiciels espions alors qu'il contient lui-même un code malveillant.

Spam : Parasite électronique, courrier ou image indésirable envoyé à un grand nombre de destinataires.

Spyware : Mouchard électronique, logiciel espion ou service de recherche qui s'installe sur le navigateur Internet ou dans le système d'exploitation de l'ordinateur pour recueillir des informations personnelles, à l'insu de l'utilisateur.

UTM : Unified Threat Management, équipement de sécurité intégré associant au parefeu de niveau 2-3, le parefeu applicatif, la passerelle VPN, la prévention d'intrusion, l'antivirus et l'antispam.

Zombies : Ordinateurs connectés au réseau Internet à haut débit et mal protégés. Des milliers d'entre eux, notamment chez les particuliers, sont détournés de leur usage primaire, par intermittence, pour servir la cause des spammeurs.

POUR EN SAVOIR PLUS

Le dossier de la CNIL sur le spam
http://www.cnil.fr/index.php?id=1532

Communication de l'Union Européenne du 15/11/2006
http://europa.eu.int/information_society/policy/ecomm/doc/info_centre/communic_reports/spam/com_2006_0688_f_fr_acte.pdf

Communication de l'Union Européenne du 22/01/2004
http://europa.eu.int/information_society/policy/ecomm/doc/info_centre/communic_reports/spam/spam_com_2004_28_fr.pdf

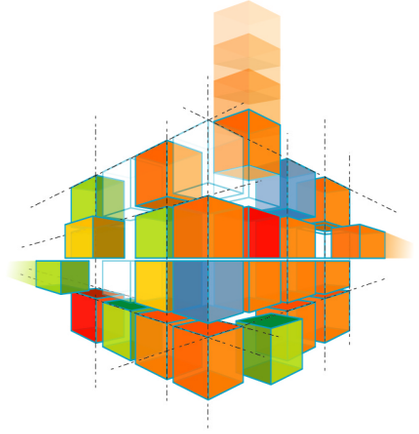
OCDE Antispam
http://www.oecd-antispam.org/

Messaging Anti-Abuse working group
http://www.maawg.org/home

POUR EN SAVOIR PLUS

ARKOON
NETWORK SECURITY

Arkoon propose une combinaison technologique inédite pour filtrer le spam, stopper les contenus malveillants et les logiciels espions tout en bloquant la navigation sur les sites suspects ou illicites.



ADAPTIVE SECURITY

SIÈGE SOCIAL
1 PLACE VERRAZZANO
CS 30603
69258 LYON CEDEX 09
TÉL : +33 (0)4 72 53 01 01
FAX : +33 (0)4 72 53 12 60

ILE DE FRANCE
IMMEUBLE LE PELISSIER
220 AV. PIERRE BROSSOLETTE
92240 MALAKOFF
TEL : +33 (0)1 57 63 67 00
FAX : +33 (0)1 57 63 67 37

www.arkoon.net / info@arkoon.net

AMC SSL360 FAST360 Security BOX

speedfire mediArchitects

Un livre blanc réalisé par Speedfire mediArchitects
www.speedfire.com / 0950 27 64 00 / infos@speedfire.com