

LE BULLETIN *d'information sur l'intelligence économique stratégique pour les PME-PMI*

ÉDITO

Quelle sécurité et pour quel risque ?

L'actualité nous le rappelle régulièrement, il est important de se prémunir contre les risques liés à notre dépendance vis-à-vis de l'informatique : la panne d'un ordinateur ou le vol d'informations sont des incidents qui peuvent arriver très vite et handicaper une entreprise pour de longs mois. Fort heureusement des solutions existent. Il convient donc de les adopter de manière cohérente avec son propre besoin.

Quelle sécurité et pour quel risque ? Tout d'abord, il nous faut identifier les différents risques opérationnels :

- Ceux liés aux pannes inhérentes à tout système : plusieurs moyens techniques existent depuis la sauvegarde régulière de vos données jusqu'à la duplication de vos systèmes pour une plus grande sécurité. Certains prestataires fournissent des solutions de sauvegarde dynamique sur le réseau, en continu, pour vos données et programmes. Attention néanmoins à vérifier l'intégrité de vos fichiers avant transfert et à créer une protection supplémentaire entre votre disque dur et le lieu de stockage.
- Risques liés à la protection contre les « pirates » : tous nos ordinateurs sont aujourd'hui connectés via l'internet... dans ce grand village dit global, des bandits sévissent. Ils peuvent faire propager des



virus contre lesquels des protections existent mais ils peuvent aussi accéder à nos données pour les voler à notre insu ! Evitez donc la connexion permanente et dotez-vous de logiciels spécialisés contre les intrusions.

- Ceux liés à la malversation interne : il s'agit là du risque le plus fréquent et le moins contrôlable ; comment se protéger contre les attaques venues de l'intérieur ? La réponse ne se limite pas là à des produits de protection mais également à des processus organisationnels à mettre en place. A ces risques opérationnels, il nous faudra ajouter les risques d'ordre stratégique où notre savoir est plagié par un concurrent qu'on croyait partenaire sur une affaire.

Un entrepreneur prend des risques, certes, mais ceci ne doit pas vouloir dire s'exposer. La sécurité informatique est un domaine vaste et vouloir se protéger peut mener très loin. Il faut donc une analyse interne, puis se protéger sans tomber dans la paranoïa car il ne faut pas que l'informatique, moteur de croissance des entreprises, devienne un handicap. Dans ces pages, nous vous donnerons des indications : il vous appartiendra alors de mesurer vos risques !
Bonne lecture

Georges MOKHBAT,
Consultant en télécommunications
Président de l'AFPI (Association Franco-Libanaise
des Professionnels de l'Informatique)

L'enquêteur Ntech : un maillon clé

Une interview de l'Adjudant Dominique DOMINGUES, enquêteur en technologie numérique (Ntech) à la Cellule d'Identification Criminelles (C.I.C) de la région de Gendarmerie d'Ile de France.

La Ministre de l'Intérieur a dévoilé, en février dernier, un plan d'action pour contrer la Cybercriminalité dont l'impact néfaste fait suite à l'explosion d'Internet en France. Où en sommes nous aujourd'hui ?

Adjudant Domingues : depuis 2005, le dispositif « intelligence économique » de la Gendarmerie se décline de la direction générale jusque dans chaque département. La chaîne ainsi constituée, composée de personnels spécialisés, s'appuie sur un réseau d'environ 4000 unités, réparties sur 95 % du territoire. Les enquêteurs Ntech, regroupés dans des CIC, sont l'un des maillons de cette chaîne. Encore peu nombreux il y a quelques années, notre effectif va croissant. On compte aujourd'hui environ 150 Ntechs en France.

Quelles sont leurs missions ?

Les Ntechs sont formés spécialement pour les enquêtes touchant à l'informatique et aux réseaux (internet, téléphonie...). Nous avons donc pour mission de mener toutes les formes d'enquêtes liées aux nouvelles technologies et d'aider les enquêteurs non formés dans leurs démarches : réquisitions, analyse de disques durs (recherches des connexions internet, création de site, photos, documents en tous genres, usage de logiciels permettant de faire du hacking...), surveillance de

l'internet, analyse de téléphone mobile, cartes bancaires, clés USB, etc. A noter que du côté de la police, il existe les ESCI, Enquêteurs Spécialisés en Criminalité Informatique.

En quoi une PME peut-elle être concernée ?

Elle peut être confrontée à des vols de données informatiques soit de l'intérieur (employé indélicat), soit de l'extérieur, par un hacker cherchant à pénétrer son réseau. Elle peut aussi être soumise, via son propre réseau, à des connexions Internet ayant pour objet le téléchargement de données illicites (divx, musique, photos pédo-pornographiques...).

Dans tous les cas, elle doit impérativement se rapprocher de la Gendarmerie dont elle dépend.

Pouvez-vous nous donner un exemple ?

Récemment, une PME constatait que son concurrent déposait systématiquement et juste avant elle, un brevet. Une enquête menée en interne par son Responsable de la Sécurité du Système Informatique (RSSI) a démontré qu'une employée correspondait via son poste de travail avec un employé de la société concurrente. L'entreprise a donc porté plainte et une enquête a été diligentée. A la suite de l'autorisation donnée par un Procureur de la République, une surveillance des courriels entrant/sortant a été effectuée et la mise en cause démasquée. Il ne s'agissait pas vraiment de vol d'informations. Elle ne fournissait que quelques bribes mais son interlocuteur savait parfaitement comment les exploiter. L'analyse des mails et des postes utilisés a déterminé la date exacte du début de ces échanges. Cet épisode regrettable a néanmoins révélé à l'entreprise une faille dans l'organisation de son système de sécurité. Par la suite, tous ses employés ont été formés aux enjeux de l'intelligence économique et notamment à ceux liés à la sécurité informatique.

LE CHIFFRE CLÉ :
375 000 EUROS

C'est le montant de l'amende assortie d'une peine de prison de 5 ans maximum qui est prévue en cas d'escroquerie, selon l'article 313-1 du code pénal.

Parmi les techniques identifiées : le fishing (envoi de mails incitant les victimes à cliquer sur un lien

les entraînant sur un site malfaisant, en se fondant sur la peur ou l'espérance de gain), le SCAM (envoi d'un mail faisant croire à la personne qu'elle peut venir en aide à quelqu'un ou obtenir un bénéfice). Source : la BEFTI juin 2007

TÉMOIGNAGE

La sécurité informatique : une clé de l'intelligence économique

Retour sur les enjeux de la sécurité informatique avec Stéphane Fantuz, consultant au sein du Cabinet Expenciel spécialisé dans le conseil financier aux entreprises et Président de l'association CNCIF agréée par l'Autorité des Marchés Financiers - AMF - et membre de la CGPME Ile de France.

Les systèmes informatiques sont désormais le centre névralgique de la plupart des entreprises. Leur savoir-faire, leurs connaissances, l'ensemble de leurs données se trouvent concentrés bien souvent dans de petites unités. À ce titre, elles semblent faire l'objet d'une recrudescence des attaques via Internet. Mais est-ce vraiment le cas pour les PME ?

Stéphane Fantuz : quelle que soit la taille de l'entreprise, le nombre d'attaques progresse constamment. Déjà, en 2003/2004, une étude a démontré que 44 % des PME de moins de 20 personnes avaient subi au moins une tentative d'infiltration dans leur système informatique. Les chiffres montrent que la tendance n'est pas prête de s'inverser d'autant que la rapidité des attaques va, elle aussi, en s'accroissant. Il y a encore un an, il fallait environ ¼ d'heure avant de subir une attaque via le net. Aujourd'hui quelques minutes suffisent.

La menace est donc bien réelle mais quelle est la nature des risques encourus ?

Chacun doit d'abord prendre conscience que l'enjeu pour les PME et TPE est considérable car c'est leur viabilité même qui peut être mise en péril. Un large éventail de cas de figure est possible. Cela peut aller de la simple gêne à la mise hors service de toute sa ressource informatique et avec elle, trop souvent la disparition de son expertise. Elle peut subir des vols d'informations confidentielles, des vols de savoir-faire technologique, des intrusions dans ses bases de données à des fins mafieuses voire des cas d'usurpation d'identité etc. Les conséquences s'avèrent parfois très lourdes : retards qui entraînent des pertes d'exploitation, pertes de temps et d'énergie conséquentes, coûts financiers.

D'après la même étude : 50 % des PME attaquées ont dû suspendre leur activité durant plusieurs heures ; 36 % ont perdu leurs données ; 18 % ont dû investir dans un nouveau matériel et 16 % ont propagé des virus à leur insu.

Le tableau est plutôt sombre mais existe-t-il des outils vraiment efficaces pour lutter ?

L'effort de protection doit évidemment être à la hauteur des risques encourus. Aujourd'hui, nous disposons de toute une gamme d'outils performants. Encore faut-il prendre le temps de les installer et de s'en servir correctement : anti-spam, anti-virus, coffre-fort numérique, données cryptées etc. La CGPME Ile-de-France va prochainement mettre en place des outils qui montrent clairement aux utilisateurs le déroulement des manipulations à effectuer pour que les outils soient totalement efficaces.

**“La menace
est donc
bien réelle”**

Néanmoins, je tiens ici à souligner deux bonnes pratiques essentielles que nous avons tendance à oublier. La première consiste à pratiquer des sauvegardes régulières de ses données. Si votre système informatique tombe en panne ou subit une attaque, le plan de récupération de vos données sera largement simplifié. La deuxième consiste à actualiser par des mises à jour régulières les outils installés. À ce titre, la CGPME Ile-de-France a vocation à accompagner les PME au travers de différentes actions de sensibilisation mais aussi de formation.

FOCUS SUR :

Michèle Alliot-Marie a dévoilé, le 14 février dernier, le plan d'action du Gouvernement en matière de cybercriminalité. Il contient notamment des mesures contre l'usurpation d'identité et l'escroquerie en ligne.

Des peines spécifiques contre le piratage et l'usurpation d'identité : l'usurpation d'identité sur internet sera punie comme un délit, passible d'un an d'emprisonnement et de 15 000 euros d'amende.

Parallèlement, des peines alternatives de travaux d'intérêt général pour les hackers sont prévues. "Ainsi, leurs réelles compétences en la matière pourront être nettement mieux utilisées au service de la collectivité".

La ministre veut aussi un renforcement des dispositifs d'enquête : cela passerait par la mise en place, dès septembre 2008, d'une plate-forme de signalement automatique de toute forme de malversation, escroquerie, incitation à la haine raciale ou pédopornographie constatée sur internet.

Autres moyens prévus : le doublement du nombre d'enquêteurs spécialisés en criminalité informatique, au sein de la direction centrale de la police judiciaire, et d'enquêteurs en technologie numérique de la gendarmerie ; la création de cursus à vocation technologique au sein de la police nationale, comme il en existe dans la gendarmerie.

EN SAVOIR PLUS

Brigade d'Enquêtes sur les Fraudes aux Technologies de l'Information (BEFTI) pour Paris et la Petite Couronne (92,93,94).

122, rue du Château des rentiers
75013 Paris.
Tél : 01 55 75 26 19

La Confédération Générale des Petites et Moyennes Entreprises Ile-de-France (CGPME IDF).

Site Internet : <http://www.cgpme-idf.fr/>
Tél : 01 47 78 78 35

Conseil Régional d'Ile-de-France Direction du développement économique et de l'emploi. Chargé de mission intelligence économique et stratégique.

Tél : 01 53 85 67 14
Fax : 01 53 85 60 49
Site Internet : www.iledefrance.fr

Institut d'Etudes et de Recherche pour la Sécurité des Entreprises (IERSE) Ecole Militaire CESC

21, place Joffre
75007 Paris
Tél : 01 44 42 39 24
Site Internet : <http://www.ierse.fr/>

Office Central de Lutte contre la Criminalité liées aux Technologies de l'Information et de la Communication (OCLCTIC).

101, rue des 3 Fontanot
92000 NANTERRE
Tél : 01 49 27 49 27
Fax : 01 40 97 88 59
E-mail : oclctic@interieur.gouv.fr

État Major de la Région Gendarmerie Ile-de-France

Hôtel National des Invalides
PB 114 - 75326 Paris Cedex 07

CONTACT

I.E.S Le Bulletin est édité en complément du Guide "Le dirigeant de PME-PMI & l'intelligence économique", projet régional en partenariat avec Agefos PME Ile-de-France, le Conseil Régional d'Ile-de-France et la CGPME Ile-de-France.
Tél : 01 47 78 78 35 - Mail : contact@cgpme-idf.fr

Secrétaire Général de la CGPME Ile-de-France: Abdallah MEZZIOUANE

Ont participé à ce numéro : Dominique DOMINGUES, de la Cellule d'Identification Criminelle de la région de Gendarmerie d'Ile-de-France - Stéphane FANTUZ, Consultant au sein du Cabinet Expencil et Président de l'association CNCIF - Georges MOKHBAT, Consultant en communication et Président de

l'AFPI - Karine LAYMOND, Chargée de communication à la CGPME Ile-de-France - Cyril PATTEGAY, Chargé de Mission à la CGPME Ile-de-France - Véronique MONCEL - Conception, réalisation : CHALLENGE'R - 43, rue Raspail 92300 Levallois