TABLE RONDE

PME: Quelle politique de sécurité

Eddy Dobbelaere
Managing Director Porthus

Louis Lempereur
General Manager Celem Computers nv

Rudi Steyaert
Managing Director C-Logic

Luc Schauvaerts
ICT Manager Erudict

Peter Ryckaert
CEO DigiPoint

Fabrice Wuyts
Administrateur délégué
Proximedia nv

Marc Van De Verre
Fondateur Extra Consult

informatique adopter?

De simple gadget pour quelques personnes exigeantes, la sécurité informatique est devenue en quelques années un service informatique à part entière, un élément indispensable de stratégie. Toutefois, bon nombre de PME sont encore trop peu conscientes des risques: virus, falsification de données, vol de supports, destruction de matériel à la suite d'un incendie, de dégâts des eaux, d'impact de foudre, etc.

La question est de savoir qui, quand, comment mettre en place une politique efficace de sécurité informatique dans sa PME. Comme pour tout service, il faut des objectifs clairs, une organisation appropriée, une veille permanente pour anticiper et faire face à une situation changeante, disséminer/former pour convaincre des mesures et réflexes à prendre. In fine, la sécurité informatique apporte tout un lot de contraintes à chacun.

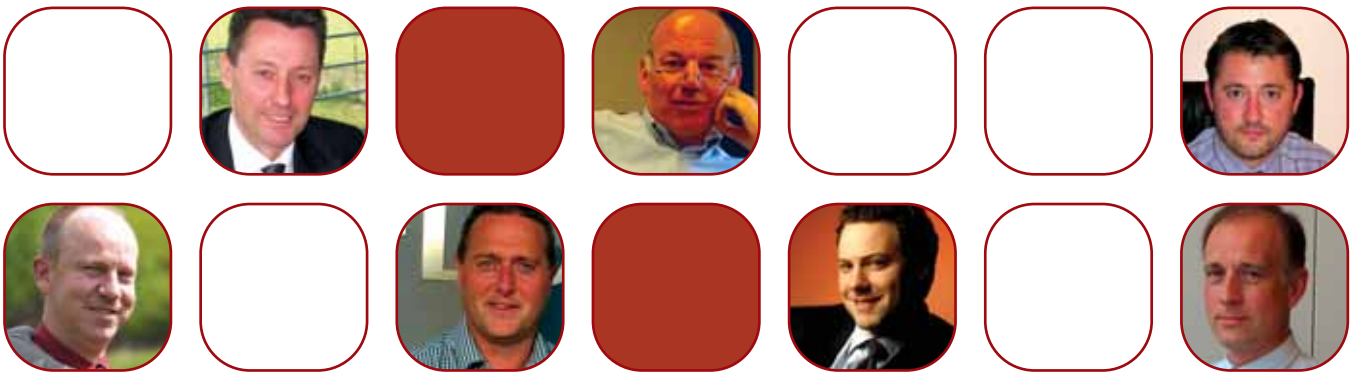
Exemples à suivre par 9 dirigeants de PME conscients des enjeux de la sécurité informatique et réunis lors d'une table ronde.

« *Les conséquences d'une protection insuffisante sont toujours catastrophiques pour l'entreprise.* » soulignent en chœur les participants.

Les problèmes survenus chez nos dirigeants de PME interrogés sont de natures très variées et sont souvent provoqués par des attaques de virus. On se souvient encore du virus 'I LOVE YOU' il y a quelques années. Après cette attaque, un patron a affiné le filtrage de ses e-mails afin de supprimer les composants actifs de courriels entrant. Un autre a eu des problèmes avec un ancien collaborateur qui, par le biais du mot de passe d'un collègue, a tenté d'accéder au réseau via une connexion modem. D'autres sont en butte aux attaques du

Participants

Pascal Saesen, ICT Manager Microfibres Europe
Wim Polfliet, Manager EM DataCenter, member of EM Group
Marc Van De Verre, Fondateur d'Extra Consult
Eddy Dobbelaere, Managing Director Porthus
Peter Ryckaert, CEO DigiPoint
Louis Lempereur, General Manager Celem Computers
Fabrice Wuyts, Administrateur délégué Proximedia
Luc Schauwaerts, ICT Manager Erudict
Rudi Steyaert, Managing Director C-Logic



genre denial-of-service, divers types de virus ou d'attaques visant à forcer le mot de passe. Enfin, chez tous le nombre de SPAM est en augmentation.

Louis Lempereur: Les entreprises n'investissent pas suffisamment dans la protection de leur informatique. Même les plus simples copies de sécurité sont souvent ignorées. En ce qui nous concerne, nous avons déjà été confrontés à des problèmes de sécurité comme les virus ainsi que des attaques de notre site.

Wim Polfliet: Jusqu'ici nous n'avons pas rencontré de problèmes grâce à un firewall et une protection anti-virus de premier plan.

Fabrice Wuyts: En tant que fournisseur de services Internet, nous sommes quotidiennement confrontés à des problèmes de sécurité. Régulièrement, des hackers tentent d'attaquer nos serveurs web, qui heureusement sont bien protégés. Pour les virus, à titre d'exemple, les 10.000 mails box que nous gérons pour nos clients génèrent plus ou moins 40.000 mails par jour dont 40 % sont bloqués par notre serveur anti-virus.

Perte de chiffre d'affaires. Il semble assez logique de dire que les 'attaques de l'extérieur' puissent entraîner des pertes du chiffre d'affaires mais ici aussi, les réponses diffèrent entre les participants à la table ronde. Pour une entreprise, les attaques ont provoqué la perte d'une quinzaine de journées de travail, étalée sur une ou plusieurs années. Pour une autre, pas de perte du chiffre mais bien de temps. D'autre part, des mesures de protection et des investissements en personnel et matériel sont également la conséquence de ces agressions.

Peter Ryckaert: Grâce à la protection mise en place, les 'attaques de l'extérieur' n'ont pas d'impact sur le chiffre d'affaires. Par contre, il y a des coûts supplémentaires en heures de travail suite à la surcharge du système de sécurité ce qui a une influence directe sur la rentabilité.

Louis Lempereur: Nous n'avons pas enregistré de perte du chiffre d'affaires, mais bien une perte de temps. Depuis, notre site internet est hébergé ailleurs ce qui entraîne un certain coût.

Fabrice Wuyts: Heureusement, nous n'avons pas eu à déplorer de pertes de chiffre d'affaires étant donné que la protection informatique fait partie de notre métier.

Louis Lempereur: *"Nous n'avons pas enregistré de perte du chiffre d'affaires, mais bien une perte de temps. Depuis, notre site internet est hébergé ailleurs ce qui entraîne un certain coût.*

Qui protège? Pour nos interlocuteurs, la sécurité informatique est souvent une affaire interne. Une des entreprises fait appel à ses techniciens, une autre PME emploie deux collaborateurs qui ces derniers mois sont en charge d'une partie importante de la sécurité informatique. Une troisième compte deux collaborateurs chargés de cette sécurité et une quatrième emploit d'une part un security officer responsable de la direction générale et d'autre part un security engineer. Cette dernière a également un contrat d'assistance avec un spécialiste sécurité externe. Un des participants s'appuie sur sa propre expertise: les collaborateurs suivent régulièrement un recyclage pour rester au courant des techniques les plus récentes en matière d'anti-virus et de firewall.

Pascal Saesen : Nous assurons la sécurité en interne, mais faisons également appel à une société extérieure. Le collaborateur interne s'occupe de la stratégie à suivre en protection informatique. Le gestionnaire de systèmes est responsable des programmes anti-virus et anti-spam.

Règlements. Un grand nombre d'entreprises n'ont toujours pas de règles pour la protection d'informations importantes. Mais certaines choses changent. Une des sociétés participantes possède un site portail où le client peut obtenir des informations sur ses projets. Les visiteurs et/ou membres échangent certes des informations sensibles via le portail, mais cette information est protégée en ligne comme hors ligne. Pour une autre entreprise, le traitement d'informations se réfère à la convention de travail. Une autre encore a développé des policies en matière de sécurité. On y décrit, entre autres, comment traiter les mises à jour sécurité provenant de distributeurs de logiciels, quelle attitude adopter pour l'accès aux données, le back up, la restauration, etc. Pour l'un des participants, il n'y a pas de contrôle strict des données entrantes et sortantes, sauf lorsqu'il y a de fortes présomptions d'abus.

Luc Schauwaerts: Pour la protection de notre informatique sensible, nous n'avons pas de règles écrites.

Fabrice Wuyts : Le règlement est assez simple: toutes les données informatiques sont sauvegardées deux fois à l'extérieur grâce à notre logiciel de sauvegarde en ligne.

Luc Schauwaerts: "Pour la protection de notre informatique sensible, nous n'avons pas de règles écrites."

MESURES CONCRÈTES. Parmi les mesures, on compte évidemment les back-ups. Pour l'un des participants, le serveur est protégé par un UPS (Uninterruptable Power Supply) pour éviter toute interruption de fonctionnement et autres perturbations du réseau. Les données techniques sont également chargées sur un laptop deux fois par jour et à la fin de la journée, un back-up complet sur un disque dur externe est planifié. Ce disque dur est emporté le soir à la maison. Très bientôt, les données du serveur de cette entreprise seront reprises dans un second ordinateur qui se trouvera dans une pièce spéciale dans une firme extérieure. Un autre participant signale que des composants informatiques importants sont localisés dans des espaces protégés spéciaux. Des back-ups y sont aussi conservés à l'abri du feu et en dehors du siège de l'entreprise.

Louis Lempereur : Parmi les mesures concrètes, des copies de sécurité sont emportées à l'extérieur.

Fabrice Wuyts: Nous avons développé et nous commercialisons notre propre logiciel de sauvegarde en ligne, Dataprotex. Nous disposons donc de deux serveurs de back-up décentralisés (dans deux centres télécoms) qui hébergent les sauvegardes cryptées de nos clients (et les nôtres, bien entendu). Nous éditons par ailleurs le portail de la sécurité informatique (belge) www.dataprotex.be

Eddy Dobbelaere: Nous avons pris toutes les mesures possibles pour éviter les nuisances. Cela a débouché sur le choix d'un centre de données 'state of the art' avec prévention contre l'eau, UPS pour pallier aux pannes de courant et générateur diesel pour faire face à une panne UPS. Si ces mesures devaient malgré tout être insuffisantes, nous avons un plan anti-désastre comprenant la restauration des données les plus critiques et l'édification d'un environnement de travail dans un centre de données à distance.

INVENTAIRE. Toutes les PME n'ont pas conscience de l'importance que revêt un inventaire annuel des outils informatiques. Ils représentent pourtant un capital appréciable… Plusieurs participants à la table ronde reconnaissent en effet ne pas inventorier leurs outils informatiques. Un des participants dispose d'une base de données comprenant tous les serveurs de même que les composants réseau avec leur configuration.

Rudy Steyaert: Au sein de la société, nous avons établi un inventaire complet des outils informatiques disponibles.

Louis Lempereur : Nous possédons un inventaire de tous les outils informatiques tant hardware que software; toutefois, beaucoup d'outils logiciels viennent par Internet et ne sont pas comptabilisés.

Fabrice Wuyts : Au sein de notre entreprise, nous disposons d'un inventaire de tous les outils informatiques présents.

PLAN DE SECOURS. Bien qu'un plan de secours soit vital pour faire face à certaines situations, toutes les entreprises n'en ont pas ou n'ont pas testé leur valeur opérationnelle. Un des participants signale ne pas avoir de plan officiel, mais des ressources existent selon les besoins. Un autre intervenant souligne disposer d'un monitoring automatique des systèmes et d'une permanence 24 heures sur 24 pour les cas d'urgence. Une entreprise possède même différents plans de secours prêts à être utilisés selon la forme et la gravité de l'incident.

Marc Van De Verre: Extra Consult a une très petite structure et peut ainsi réagir avec souplesse aux coups du sort. La perte du serveur peut être résolue en un jour. L'achat et la configuration d'un nouveau serveur ne demanderont pas plus de huit heures pour être à nouveau totalement opérationnel. Le client/fournisseur ne subira aucun préjudice car tout le monde dans la firme travaille avec un laptop et possède une connexion à la maison. En d'autres termes, nous ne sommes jamais totalement dépendant du serveur du siège central à Bruxelles.

Fabrice Wuyts: Comme toute entreprise, nous avons déjà connu quelques crashs de disque qui ont nécessité la réinstallation d'un back-up. Cela s'est très bien passé étant donné que les sauvegardes sont effectuées quotidiennement, grâce notamment à la fonction de programmation automatique de notre logiciel.