NOV. DEC. 2014 - JAN. 2015
n°88
13€

GÉRER | PRÉVOIR | OPTIMISER

GPO Magazine

LE MAGAZINE DES DIRIGEANTS D'ENTREPRISE

www.gpomag.fr

> ENQUÊTE
Soutenir la volonté d'entreprendre en France

> DOSSIER
Comment sécuriser l'entreprise face aux menaces du numérique

Gestion | Organisation

Courrier & Impression
Des pistes pour réduire efficacement les coûts

Social | RH & Management

Titres restaurant
Le point sur les cartes restaurant dématérialisées

Portrait

Sébastien Chabal
Fondateur de Chabal Sport

DOSSIER

Comment sécuriser face du

- **Protégez-vous efficacement contre les menaces informatiques**
  - Comment se protéger des risques ?
  - En cas d'incident...
- **Comment gérer la mobilité en toute sécurité**
  - Compréhension et appropriation
  - Des portails pour la mobilité
  - Sécurité et BYOD, une question indissociable
- **La prévention du risque juridique lié à la sécurité de l'entreprise numérique**
  - Est-ce possible de prévenir juridiquement ces risques informatiques ?
  - Quelle responsabilité et quelles sanctions pour l'hébergeur ?
- **Internet : une avancée et un fléau pour les marques**
  - Quelles sont les précautions à prendre ?
  - Quelles sont les différentes atteintes aux marques ?
  - Quelles sont les sanctions judiciaires et extrajudiciaires ?

Tout dirigeant d'entreprise et, *a fortiori*, tout responsable informatique doit prendre en compte le risque informatique inhérent aux sites *web*, au *Cloud* et au réseau interne ainsi qu'aux tablettes et smartphones. En effet, l'essor de l'entreprise tout numérique peut favoriser un certain nombre d'attaques qui vont toucher le cœur même du système d'information de l'entreprise.

l'entreprise aux menaces numérique

Protégez-vous efficacement contre les atteintes informatiques

Perte des services essentiels, vol d'informations confidentielles ou panne informatique importante, autant de menaces réelles et très pénalisantes pour les entreprises de toutes tailles.

La mise en place d'une politique préventive de sécurité repose autant sur les outils que sur leur utilisation bien comprise. De nombreux prestataires en sécurité informatique proposent des solutions de protection et de sauvegarde efficaces mais le facteur humain est une part importante de la sécurité. Lionel Mourer, responsable d'études du Clusif (Club de la sécurité de l'information français) cite ainsi le cas d'une entreprise française dont le projet de *joint-venture* avec une société chinoise a capoté à cause du vol de données cruciales. La raison triviale de cet échec ? Lors

Interview

Comment protéger son entreprise ?

Lionel Mourer, Responsable d'études au Clusif, Président de la société de conseil Atexio

GPO Magazine : Quels sont les risques majeurs pour une entreprise en matière de sécurité ?

Concrètement, ce sont la perte ou la modification de données sensibles de l'entreprise. La situation la plus critique est sans doute la modification d'informations sans que leurs détenteurs en aient connaissance, suite à une attaque invisible d'un serveur, d'un site *web*, à l'insu des dirigeants de l'entreprise.

GPO Magazine : La taille d'une entreprise change-t-elle la nature des problèmes de sécurité ?

Quelle que soit la taille d'une société, c'est le degré de sensibilité des données qu'il faut prendre en compte pour définir le périmètre de sécurité. Les fichiers sensibles sont, entre autres, les projets de R&D, les brevets, ou encore les processus de fabrication. Je pense, par exemple, à la formule de production d'un type spécifique de béton.

GPO Magazine : Quels conseils préconisez-vous pour protéger une entreprise?

Il faut d'abord procéder à une évaluation des risques informatiques du parc installé et sur les réseaux. La protection ne doit pas être seulement technique mais aussi organisationnelle. Pour ce dernier point, il faut vérifier le contrôle d'accès au-delà des services traditionnellement protégés, comme les ressources humaines ou les services liés à la paie. Pour les sociétés qui travaillent dans la finance ou la banque, il y a des obligations légales sur la protection et la confidentialité des données. L'industrie est en retard sur le plan de la sécurité informatique alors que les entreprises dans ce secteur d'activité détiennent des données qui sont au cœur de leur savoir-faire.

De plus, la sauvegarde doit être bien gérée (mise à jour fréquente et complète des éléments essentiels). En prévision de petits problèmes (perte de fichiers non importants) ou gros incidents (mise hors service d'un serveur par incendie ou autre). ■

d'un déplacement en Chine pour finaliser l'opération, le PDG et le directeur financier se sont simplement fait dérober leur ordinateur portable contenant tous les détails du projet de fusion. La meilleure solution technique perd son efficacité si les règles basiques de la sécurité informatique ne sont pas appliquées comme la création de mots de passe complexes et régulièrement modifiés.

Côté *web*, le vol, la modification ou la destruction de données sensibles est une réalité, précisément identifiée et mesurée par un observatoire comme le Clusif en France. Les développeurs d'un site *web* devront être particulièrement attentifs à la protection des applications métiers, à la base de contacts clients ou aux numéros de cartes bancaires stockés sur les serveurs de l'hébergeur du site. La liste n'est pas exhaustive et dépend de l'activité de l'entreprise. Ainsi, TPE et PME doivent protéger les projets susceptibles d'intéresser la concurrence. Une des attaques les plus pénalisantes consiste à « prendre en otage » les informations importantes sur un serveur, en cryptant les données et en demandant une rançon de l'ordre de 10 000 € à 50 000 € à la société victime en échange de la clé de déchiffrage. Parfois, les « ravisseurs » ne livrent même pas cette clé après paiement de la somme réclamée par les pirates. Le *Cloud*, tendance forte, est adopté aujourd'hui par près d'un tiers des PME en 2014 (Source : Markess International). Malgré des avantages sur

l'aspect sécurité, avec la mise à jour automatique et régulière des outils de protection, ce mode de traitement des données comporte des risques dus à la perte de la maîtrise des données sensibles de l'entreprise.

Comment se protéger des risques ?

La première étape vise à identifier le degré d'importance des données. Les documents sensibles de l'entreprise sont, notamment, les bases de données des clients, les contrats commerciaux ou les brevets, les données de production, les dossiers des usagers, les démarches administratives ou encore les informations concernant un marché public. Il est possible ensuite de lister les risques encourus.

Pour un site *web* ou un intranet, cet audit peut être complété par des tests d'intrusion qui consistent à se mettre à la place d'un attaquant pour détecter toutes les vulnérabilités et à y remédier en ajoutant des correctifs. L'audit sera ensuite suivi d'un plan d'action.

Les mesures de prévention sur le réseau local de l'entreprise concernent la mise à jour des logiciels, la mise en place d'une politique de sécurité pour l'administration des postes de travail, la formalisation des règles de sécurité pour les collaborateurs ainsi que le contrôle d'accès physiques aux locaux.

Côté *Cloud*, il faut bien analyser le niveau de service fourni, avec entre autres, le degré de sécurité proposé par le prestataire, concernant les réseaux, le matériel et les stratégies de contrôle déployées afin de protéger les données, les applications et l'infrastructure du *Cloud*.

Hervé Schauer, consultant en sécurité informatique, fondateur et dirigeant de HSC, précise que « *pour choisir une solution sécurisée de* Cloud, *il faut interroger le fournisseur sur les points suivants : peut-on agir librement sur les données ? Où se trouvent-elles ? Qui a accès aux données ? Peut-on changer facilement de prestataire ? Existe-t-il un niveau de protection suffisant pour les données à caractère personnel ?* », sans oublier la notion de réversibilité des données, à savoir la possibilité en fin de contrat de pouvoir les exploiter chez un nouveau prestataire sans qu'il y ait une coupure du service.

En cas d'incident ...

Une attaque informatique génère un stress qui pousse à prendre de mauvaises décisions. Si le réseau local est compromis, il ne faut jamais se contenter de traiter l'infection d'une machine sans tenter de savoir si le code malveillant a pu se propager ailleurs dans le réseau. De nombreuses entreprises qui ne cherchent pas d'emblée à connaître le périmètre réel d'une infection, ont perdu plusieurs semaines, voire plusieurs mois, dans le traitement de l'incident. Dans un futur proche, l'irruption des objets connectés viendra bousculer profondément la donne en termes de sécurité, car pour l'heure, ils sont mal sécurisés. ■

Serge ESCALÉ

Cloud : sous la surveillance attentive des Américains

L'affaire Snowden a révélé au grand public que les services de renseignements américains disposent de considérables moyens de surveillance des flux informationnels et qu'ils les utilisent. Si une société travaille beaucoup à l'exportation, mieux vaut ne pas confier de données sensibles à des services américains comme Amazon Web Service, Microsoft Azure ou Google storage. Amazon, par exemple, dispose pour l'Europe, de serveurs en Irlande qui sont répliqués aux États-Unis.

Or, depuis 2001, pour lutter contre le terrorisme, le « Patriot Act » impose une ouverture sans restriction aux données des sociétés américaines.

Dans le cadre du projet français de *Cloud* souverain, il existe 2 prestataires : Cloudwatt dont les actionnaires sont Orange et Thalès ainsi que Numergy dont l'actionnariat est composé de SFR et Bull.

À l'heure actuelle, leur bilan financier n'est pas satisfaisant.

D'autres acteurs français et de moindre taille, tels Cloud Services ou Ikoula, présentent aussi des garanties de confidentialité. ■

8 solutions de sécurité en *Cloud* et les ressources qu'elles protègent

Prestataire	Solutions	Ressources protégées
DenyAll	rWeb, DenyAll Detect	Infrastructure Web, contrôle politique de sécurité
Microsoft	Exchange Online Protection	Messagerie Exchange
Panda Security	Cloud Office de vulnérabilité Cloud Email	Protection PC, PC portables et serveurs, analyse Protection Messagerie
Qualys	QualysGuard	Analyse de vulnérabilité du réseau, gestion de la conformité
Cisco	Cloud Web Security	Infrastructure Web Flux Web PC portables
Symantec	Web Security.cloud chiffrement	Flux Web, messagerie, messagerie instantanée
Trend Micro	Secure Cloud	Sous forme de service *cloud* ou en local. Chiffrement des données
WebSense	Web security Gateway selon politique de sécurité	Infrastructure Web, applications, protections