Cybersécurité : les entreprises trop vulnérables ?

Alors que la loi impose désormais aux entreprises de veiller activement à la sécurité de leurs données, le point de vue de deux pros de la cybersécurité.

Propos recueillis par Lomig Guillo

THIERRY AUGER
DSI ADJOINT DU GROUPE LAGARDÈRE
Ce responsable de la sécurité des systèmes d'information veille depuis dix ans sur les ordinateurs et les données du groupe. Il est aussi juré de nombreux hackathons, ce qui lui permet de rester en veille sur la cybersécurité.

Le Règlement général sur la protection des données (RGPD), qui entrera en vigueur en mai 2018, va obliger les entreprises à renforcer leur sécurité informatique. Or, selon une étude publiée par Microsoft en octobre, 41% des entreprises ne disposent pas ou ont peu de visibilité sur le nombre d'attaques subies, et seules 38% de celles ayant connu un vol de données savent exactement ce qu'on leur a dérobé ! Pour les spécialistes, la question n'est plus de savoir si on va être attaqué, mais quand. Et de se préparer non pas à empêcher les attaques, mais à redémarrer une fois qu'on a été touché.

MANAGEMENT : Est-ce que, dans les entreprises, tout le monde se sent concerné par la sécurité informatique ?

MOHAMMED BOUMEDIANE : Les entreprises ont conscience du danger, car elles connaissent désormais la valeur des données. Tout le monde a en tête les exemples de Yahoo ou de Snapchat, dont la valorisation a chuté après une attaque informatique. Il y a donc une prise de conscience des décideurs pour se donner les moyens de financer la protection.

THIERRY AUGER : Globalement, dans l'entreprise, oui. Dans le grand public, moins. Il faut faire de la pédagogie. C'est vital, car ce sont ces utilisateurs-là qu'on va potentiellement retrouver à la source de gros pépins.

Comment, par exemple ?

T. A. : Dans le commerce, on trouve des unités de stockage et de sauvegarde des données en réseau, des NAS. Elles sont utiles en cas de perte de ses photos ou de crash de son disque dur. Sauf que, quand vous connectez ces serveurs domestiques à votre box, vos données se retrouvent accessibles sur Internet très facilement. Imaginez : vous êtes un commercial, souvent sur le terrain. En rentrant le soir, vous

Photos : Arnaud Meyer pour Management

sauvegardez vos données dessus et répliquez ainsi chez vous les données de l'entreprise. Ces dernières ne sont pas protégées comme dans votre société… alors que ce sont les mêmes.

M. B. : Le pire, c'est avec les médecins. On a lancé une technologie qui s'appelle Map, consultable sur notre site, qui est capable de scanner le Net, le Darknet et le Deep Web à la recherche des dernières tendances et des failles de sécurité. Avec ça, on détecte énormément de données de santé en accès libre, car beaucoup de médecins et de petits cabinets utilisent ces systèmes de stockage connectés pour sauvegarder dossiers médicaux, ordonnances… C'est un vrai problème.

T. A. : Ça résume bien la problématique : d'un côté, le monde professionnel, où on s'occupe de la sécurité, et, de l'autre, la maison, où rien ou presque n'est fait. Même dans une entreprise hypersécurisée, un problème peut arriver par un biais insoupçonné. On ne peut plus penser la sécurité informatique comme quelque chose de fermé. Plutôt que de chercher à rendre nos systèmes inviolables, on doit s'occuper de la donnée, quel que soit l'endroit où elle est créée, stockée, mise à jour, transférée…

Les entreprises sont-elles prêtes à payer pour leur sécurité ?

T. A. : Oui, à partir du moment où elles comprennent que cela permet à la fois de protéger un patrimoine, mais aussi de garantir la disponibilité des systèmes d'information, donc la continuité du business. Ça leur parle.

M. B. : Si une entreprise estime que le blocage du système informatique durant une journée lui fait perdre des milliers d'euros de CA, elle peut décider d'investir cette somme dans la protection afin d'éviter ce type de problème.

T. A. : Récemment, une PME de Clermont-Ferrand, victime d'un piratage, a été obligée de fermer, car tous ses ordinateurs étaient bloqués : fichiers clients, fournisseurs, opérations en cours, comptabilité… Une catastrophe.

Quelles sont les nouvelles menaces que vous voyez apparaître ?

M. B. : Des logiciels malveillants qui ne sont pas des *ransomwares,* mais qui font du • • •

MOHAMMED BOUMEDIANE
FONDATEUR ET PDG DE ZIWIT
Cet ingénieur informaticien a fondé sa société en 2011 à Montpellier… et en a fait le leader européen de la cybersécurité. Parmi ses clients, 70% des sociétés du CAC 40, mais aussi des géants : Adobe, Oracle, Salesforce, Google…

"EN MATIÈRE DE CYBERDÉFENSE, NOUS NE SOMMES PAS LES PIRES... MAIS PAS NON PLUS LES MEILLEURS !"

... cybersabotage en détruisant des données de façon à les rendre irrécupérables. On s'attend à une grande campagne de ce type d'ici à la fin de l'année. Le but de ces attaques est de montrer qu'on peut bloquer tout un pays.

Est-ce vraiment possible, ça ?

M. B. : Bien sûr. C'est aussi pour ça que des pays nous confient leur cyberprotection, comme l'Arabie saoudite, dont nous sommes chargés de protéger la souveraineté numérique. Un peu comme si on plaçait des chars tout le long de leur frontière... virtuelle.

Face à ces programmes malveillants, quelle est la parade ?

T. A. : Accepter le fait qu'on est vulnérable, comme les autres. Anticiper les problèmes et, surtout, avoir un plan de reprise adapté qui va permettre de redémarrer et de poursuivre l'activité de l'entreprise en limitant les pertes.

M. B. : Ne pas se voiler la face en se disant qu'il ne peut rien nous arriver. Ne pas nier la menace, c'est un premier pas vers la sécurité.

Et vous, êtes-vous souvent attaqués ?

M. B. : Des centaines de milliers de fois par jour, comme presque toutes les boîtes. Il y a eu plein d'histoires de sociétés de cybersécurité qui se sont fait hacker. Pour minimiser le risque, on se fait auditer tous les trois mois par d'autres spécialistes de la cybersécurité, car on ne peut pas être juge et partie.

Est-on bien protégé en France face à ces menaces informatiques ?

T. A. : On a la chance d'avoir l'Agence nationale de la sécurité des systèmes d'information, qui fait beaucoup de pédagogie et édite des guides très pratiques, même pour les petites entreprises qui n'ont pas toujours les moyens de financer leur sécurité.

M. B. : Nous ne sommes pas les pires, mais nous sommes loin d'être les meilleurs... Il commence à y avoir une prise de conscience, mais il faut aller plus loin. C'est pour cela que nous avons lancé cet été un fonds d'investissement, Stratinvest, doté de 6 millions d'euros, consacré aux start-up de la cyberdéfense. Car ces start-up, quand elles sont très techniques, ne savent souvent pas bien se vendre. Ce sont des mathématiciens très pointus... mais pas très bons en marketing. Ensuite, il faut du temps et une vraie expertise pour voir si ces solutions tiennent la route. Enfin, les investisseurs ne sont pas intéressés par ces start-up, car il est très difficile d'en sortir après trois ou cinq ans, notamment quand les technologies touchent à la sécurité de l'Etat. En quelques semaines, on a déjà reçu 800 dossiers... preuve qu'il y a un vrai besoin. ●

COWORKING ET COCOONING
On se croirait presque dans un boutique-hôtel. Plantes aux murs, fauteuils design et déco branchée... Nous avons été accueillis dans le nouvel espace ouvert par Kwerk, spécialiste du coworking haut de gamme, au 29 rue de Courcelles, à Paris. Un immeuble de 4200 m², aux services dignes d'un palace (à partir de 400 € par mois, kwerk.fr).