Cybersécurité en entreprise : tous concernés

Outils connectés, données partagées... La cybercriminalité est le deuxième type de fraude reporté par les entreprises. Lucie Perrier, associée du groupe PTBG, fait le point et précise les mesures de protection que toutes les entreprises devraient prendre.

La cybercriminalité est en très forte augmentation depuis dix ans. Selon une étude récente*, c'est la deuxième cause de fraude en France après le détournement d'actifs. A noter également que les entreprises françaises sont parmi les plus touchées par la fraude dans le monde. Les dirigeants doivent être conscients que toutes les entreprises sont concernées, quelle que soit leur taille. Les précautions prises sont souvent insuffisantes, voire encore dans certains cas inexistantes, ou bien s'érodent avec le temps.

Les moyens de fraude les plus courants

Toujours selon cette même enquête, les pertes financières liées à la fraude par internet se seraient élevées à 3,7 milliards de dollars en 2015. De quoi faire réfléchir. Les techniques des escrocs évoluent en permanence. Une fraude peut être réalisée en interne, par un salarié, ou peut être le fait d'une personne extérieure qui vole des données. A titre d'exemple, les types de fraudes par internet les plus courantes sont :

- le vol de données, ou « ransomware » : un escroc vole les données de l'entreprise, ou les crypte, et exige une rançon pour les lui restituer ;
- l'usurpation d'identité : le fraudeur se fait passer pour un technicien et prend le contrôle de votre ordinateur en prétextant une mise à jour. De ce fait, il peut avoir accès aux mots de passe stockés sur les navigateurs (envoi de mails, connexion aux comptes bancaires...).

Toutes ces entrées de tiers peuvent provoquer des dégâts considérables, et pas seulement financiers. Dans le cas d'une chaîne de production automatisée, ces attaques peuvent provoquer jusqu'à son arrêt complet, de plusieurs jours à plusieurs semaines.

Il peut s'agir de données comptables, du fichier clients... une cyberattaque peut mettre une entreprise à terre en 24 heures. Il peut également s'agir d'un vol de propriété intellectuelle, de plus en plus répandu. Pour les escrocs, qui peuvent être des concurrents, les économies en recherche & développement ainsi réalisées peuvent s'avérer fort intéressantes... à l'inverse de l'entreprise piratée, qui perd son avantage concurrentiel. A combien évaluer le manque à gagner ?

Les préjudices comptables, financiers, en termes de production, de commercial peuvent représenter de quelques milliers à plusieurs millions d'euros.

Les techniques des escrocs

Comment font les fraudeurs pour s'introduire dans le système de l'entreprise ?

- via des clés USB : lors de salons, l'escroc installe un logiciel pirate dans une clé USB qu'il vous propose pour vous mettre à disposition des documents. Le logiciel pirate s'installe sur votre ordinateur soit pour crypter les données, soit pour les récupérer. Vous rendez la clé et vous n'avez rien vu.

- via les mails où l'on est incité à ouvrir une pièce jointe qui est un logiciel pirate qui va soit mettre l'ordinateur à l'arrêt, soit diffuser un virus.

- via tous les outils connectés. Les entreprises pensent de plus en plus à sécuriser les ordinateurs. En revanche les téléphones, les tablettes et autres outils connectés ne font pas encore l'objet de l'attention qu'ils devraient requérir. Les mesures de protection sont encore très insuffisantes.

Comment se protéger des cyber-criminels ?

Les entreprises doivent agir à plusieurs niveaux :

- Réaliser un audit informatique pour établir la cartographie de leurs risques, identifier les données sensibles, définir les sécurités déjà mises en place, et les mesures supplémentaires à prendre pour sécuriser les systèmes.

- Mettre en place une sauvegarde périodique et surtout l'actualiser. Cela paraît tellement évident. Oui, mais voici quelques histoires vraies pour servir de base de réflexion aux dirigeants:

La configuration de la sauvegarde d'une entreprise datait de plusieurs années, la comptabilité était bien sauvegardée, mais pas le fichier clients.

La sauvegarde n'est pas externalisée et reste stockée dans l'entreprise. Et s'il y a un incendie demain ?

Deux salariées reçoivent tous les jours un mail de la société informatique responsable de la sauvegarde. Elles y sont tellement habituées qu'elles le voient passer, mais ne le lisent pas. Or depuis un mois le message est « votre sauvegarde n'a pas pu être effectuée ». C'est une consultante extérieure, avec un œil neuf, qui s'en est rendu compte.

Dans ces trois cas, les dirigeants pensaient leur système de sauvegarde sans faille et pourtant... Quelques conseils : vérifier que la sauvegarde est opérationnelle avec des fichiers existants et exploitables ; lorsque l'on conserve la sauvegarde dans l'entreprise, investir dans un support inviolable, sécurisé, ignifugeable.

- Bien gérer les mots de passe. La gestion des mots de passe doit passer par une modification régulière et l'utilisation de combinaisons de lettres, chiffres et caractères spéciaux. La gestion des profils est également importante : combien d'entreprises ne prennent aucune mesure particulière lors du départ d'un salarié de l'entreprise.

- Segmenter le réseau en installant des firewall permettant d'isoler le réseau en plusieurs zones de sécurité et protéger le trafic de données. Qu'il n'y ait pas une seule « porte » verrouillée, mais plusieurs entrées avec différentes « portes ».

- Eviter de se connecter aux réseaux publics, par définition, ces zones d'accès ne sont pas du tout sécurisées et représentent un risque important pour toutes les informations envoyées (mails, pièces jointes, mots de passe, etc.), voire même pour l'ordinateur lui-même. L'utilisation de logiciel VPN, la désactivation des dossiers partagés peuvent permettre de limiter les dégâts.

Intégrer les réflexes de protection dans la culture de l'entreprise

Les salariés sont les premiers à être touchés. Le meilleur moyen pour les entreprises de se protéger est d'instaurer un dialogue avec les salariés, les inciter à en parler, entre eux, avec la direction, et les informer sur les techniques de fraude en incessante évolution.

Leur faire prendre conscience que n'importe qui, un jour, peut « se faire avoir ». A titre d'exemples, on peut citer la fameuse « fraude aux présidents » ou la « fraude au RIB » : les fraudeurs arrivent à récupérer des données très personnelles sur la direction, les salariés, leurs habitudes, leurs dates de congés... une bonne information des salariés en amont sur les risques existants permet de limiter ce type de fraudes.

De plus, l'entrée en vigueur d'un nouveau règlement européen sur la protection des données personnelles à partir de 2018 alourdit la responsabilité des entreprises. Désormais, si une entreprise se fait voler des fichiers incluant des données personnelles, elle risque des amendes si elle n'informe pas les personnes concernées.

** enquête PwC 2016*