Cyberassurance : le nouvel incontournable des PME

Les cyberattaques font désormais partie de la réalité des temps modernes. Toute entreprise peut en être victime, peu importe son envergure. D'ailleurs, dans une période de 12 mois étudiée en 2012, 69 % des entreprises canadiennes interrogées ont signalé avoir été victime d'une forme ou d'une autre de cyberattaque. « La question n'est donc pas de savoir *si* on sera attaqué, mais *quand*... » constate Suzanne Tavaszy, directrice de production régionale (Québec et région de l'Atlantique), à la compagnie d'assurances RSA.

Les frais de restauration d'un système informatique à la suite d'une atteinte à la sécurité des données s'élèvent en moyenne à 1 027 053 $, relève un rapport publié en septembre dernier par l'Institut Ponemon, un établissement spécialisé en recherche sur la protection des données et les politiques en matière de sécurité informatique. À cela s'ajoutent les pertes liées à l'interruption du fonctionnement de l'entreprise, qui valent en moyenne 1 207 965 $, toujours selon le même rapport. Quand on tient compte du nombre total de sinistres à être signalés, on comprend qu'il s'agit là d'un véritable fléau.

Lourde de conséquences, une cyberattaque entraîne en effet des pertes de temps et d'importantes dépenses, notamment en services techniques et de restauration de données, quand ce n'est pas le paiement d'une rançon ! À cela s'ajoute le tort causé à la réputation, du fait qu'une précieuse information confidentielle, comme des renseignements personnels concernant des clients ou des employés, se retrouve alors dans les mains de personnes de toute évidence mal intentionnées.

Suzanne Tavaszy fait remarquer que toutes les assurances ne sont pas égales. « Il est essentiel d'avoir un cyberproduit offrant une couverture aussi complète que possible, signale-t-elle. Il faut surtout que les courtiers prennent soin de proposer une protection à la fois en responsabilité de première partie (*'first-party'*) et en responsabilité civile (*'third-party'*).»

La responsabilité de première partie est celle qui entraîne des coûts directs ou indirects pour l'assuré, par exemple à cause de l'interruption de la bonne marche de l'entreprise (inaccessibilité des données, déni de service du site Web, etc.) ou de la perte de l'exclusivité d'un secret commercial. Cette protection est particulièrement importante dans les petites entreprises, qui doivent se retourner rapidement pour limiter les dégâts en continuant de bien servir leur clientèle. À cet égard, l'assurance

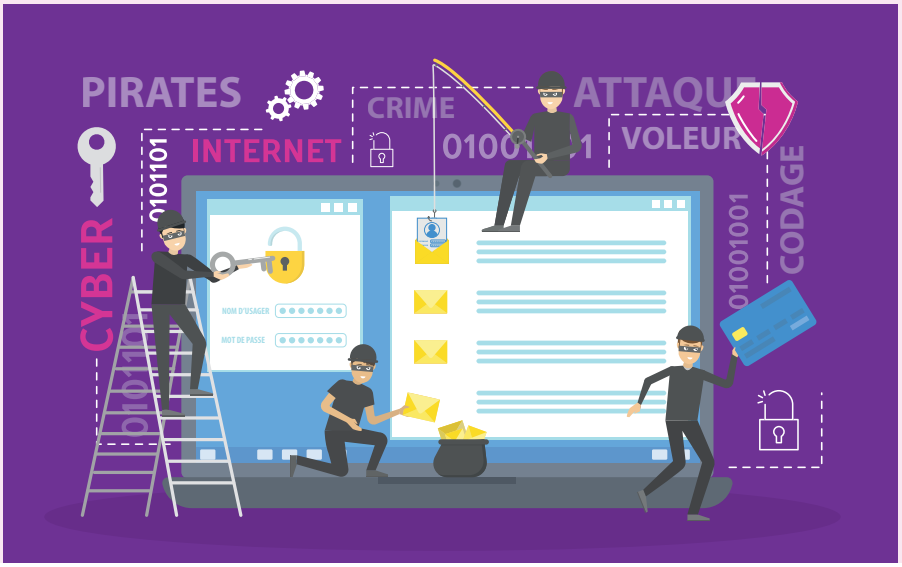
Les types d'attaques

En tout, 27 % des incidents informatiques qui entraînent des pertes sont imputables à une activité de piratage, mentionne Suzanne Tavaszy. Elles peuvent prendre diverses formes, car les malfaiteurs sont très créatifs!

Hameçonnage : Appelée « *phishing* » en anglais, cette technique permet au fraudeur d'obtenir des renseignements confidentiels qui leur permettent ensuite d'agir sous une fausse identité. Il peut par exemple amener la victime à cliquer sur un hyperlien censé lui donner une information attendue ou effectuer la mise à jour d'un programme. Or, elle se trouve plutôt à installer un logiciel espion.

Ingénierie sociale : Cette forme de cyberattaque est aussi très coûteuse. Elle mise sur des pratiques de manipulation psychologique à des fins d'escroquerie. La victime peut avoir été leurrée et amenée à donner elle-même une information menaçant l'intégrité du système informatique, par exemple parce que le pirate s'est fait passer pour un supérieur hiérarchique et a invoqué une urgence pour que le processus de vérification habituel soit outrepassé.

Déni de service : Dans ce cas, l'auteur cherche à rendre une machine ou une ressource de réseau inaccessible aux utilisateurs légitimes en perturbant temporairement ou indéfiniment les services d'un ordinateur hôte connecté à Internet.



4 mots clés à rechercher

Réelle ou redoutée : Comme la rapidité de l'intervention est primordiale pour limiter les dégâts d'une cyberattaque, il est important que le libellé de l'assurance protège en cas d'atteinte « réelle ou redoutée » — c'est-à-dire supposée, souligne Suzanne Tavaszy. « Quand on craint d'avoir subi une attaque, on a autre chose à faire que d'avoir à se battre avec son assureur pour le convaincre d'intervenir. Voilà pourquoi notre équipe d'intervention entre en scène, que l'attaque soit réelle ou présumée. Vous pensez ne serait-ce qu'un instant que votre entreprise a fait l'objet d'une attaque ? Appelez la RSA quelle que soit l'heure du jour ou de la nuit, car ces mots figurent bel et bien en noir et blanc sur nos polices : 'atteinte réelle ou redoutée'. »

Mondial : Recherchez une protection contre les attaques de toutes provenances. Car, oui : on peut vous attaquer de n'importe quel coin de la planète.

Mise à jour : Beaucoup de produits s'adressant aux PME comportent une exclusion qui élimine la protection si l'entreprise a omis de faire les mises à jour de ses *antimalwares* et autres produits antipiratage. Il est important de choisir un produit qui n'exige pas un suivi aussi strict et qui reste valide si l'assuré peut démontrer qu'il voit généralement à la mise à jour des produits en question. « Il faut éviter que, si par malheur l'absence exceptionnelle d'un employé a empêché une mise à jour en particulier, l'entreprise se trouve pénalisée », explique Suzanne Tavaszy.

Employé malveillant : Il faut se protéger contre les attaques commises par ou par l'entremise d'un employé malveillant. Or, celles-ci font souvent l'objet d'une exclusion.

Suzanne Tavaszy, directrice de production régionale (Québec et région de l'Atlantique), à la compagnie d'assurances RSA

doit absolument intégrer l'accès à une équipe d'intervention, préconise Suzanne Tavaszy.

L'assurance responsabilité, elle, est nécessaire lorsqu'une exfiltration des données sensibles peut donner lieu à des recours devant les tribunaux. Un client, un fournisseur ou des actionnaires peuvent en effet entamer des poursuites judiciaires s'ils estiment que vous n'avez pas adéquatement protégé l'information qui les concerne.

Indispensable équipe d'intervention

« La première façon d'atténuer la déferlante qui va de pair avec une cyberattaque consiste à avoir accès à une équipe d'intervention. Celle-ci peut potentiellement faire baisser la facture de 24 % », calcule Suzanne Tavaszy.

Comme la plupart des PME ne disposent pas de telles ressources à l'interne, il est crucial que leur assurance leur donne accès à ce service. Accessible jour et nuit, cette équipe agira rapidement de concert avec l'équipe informatique de l'organisation touchée. Les spécialistes dans le domaine avec lesquels la RSA fait affaire peuvent effectuer une analyse technico-légale informatique et même coordonner le travail des autres intervenants, comme la firme de relations publiques ou les experts judiciaires de renommée internationale avec lesquels la RSA a l'habitude de travailler.

« Je peux vous dire qu'une petite entreprise qui pense faire l'objet d'une cyberattaque est très soulagée d'avoir au bout du fil une personne expérimentée qui la guide pas à pas dans les mesures à prendre ! Elle se sent en contrôle et non en panique ! » mentionne Suzanne Tavaszy. Son intervention permettra de non seulement résoudre le problème en cours, mais de colmater la fameuse 'porte dérobée' créée par les pirates pour s'assurer qu'ils ne reviennent pas », dit-elle.

Car la gestion de l'après-crise est aussi délicate que la crise elle-même. On peut en outre devoir rechercher les ressources humaines et matérielles nécessaires pour avertir toutes les entités en cause — notamment en confiant le tout à un centre d'appels ou en organisant une équipe en interne. Tout cela est extrêmement coûteux.

Il faut également prévoir un suivi des dossiers de crédit touchés, soit celui de l'entreprise victime et ceux de ses clients dont les données auraient pu être volées. « La police d'assurance contre les cyberrisques de la RSA fournit une telle surveillance durant un an, relève Suzanne Tavaszy. Toute entreprise assurée par la RSA peut souscrire à cette police complémentaire. »

Précisons qu'une bonne assurance vous fournira à l'avance du matériel informatif vous permettant d'entreprendre vous-mêmes certaines démarches clés dès qu'il y a un doute de cyberattaque.

Bref, les cyberattaques menacent véritablement les PME, car celles-ci n'ont pas autant de ressources en TI que les grandes entreprises pour s'en protéger. L'entreprise qui fait le nécessaire pour protéger son infrastructure de TI fait déjà un superbe pas en avant, mais elle doit aussi savoir distinguer les assurances peu utiles de celles qui sont adéquates. ■

RSA