ACTUALITÉS EN SUISSE ROMANDE

Les cyberattaques sont une réalité: prémunissez-vous!

Lors de la conférence annuelle d'inter-pension, qui s'est déroulée à Lausanne fin novembre, il a été question de risques liés au monde cybernétique. Un sujet délicat, à ne pas prendre à la légère.

Imaginez un voleur qui remonte une rue où sont parqués des véhicules et qui essaie d'ouvrir les portières jusqu'à ce qu'il en trouve une qui ne soit pas verrouillée. Alexandre Voisin, consultant en gestion des risques chez Kessler, aime utiliser cette métaphore pour évoquer le mécanisme des cyberattaques. «On ne peut plus les ignorer, tant elles sont devenues nombreuses et inévitables», estime le spécialiste, qui explique que l'on peut louer un hacker sur le dark web pour quelques dizaines de dollars, selon la tâche à accomplir. Pas étonnant, dès lors, que l'économie du cybercrime ait dépassé celle de la vente de drogue en 2022! Corolaire logique: les annonces de cyberattaques auprès du Centre national pour la cybersécurité (NCSC), qui apporte en priorité son soutien aux exploitants d'infrastructures critiques, sont en constante hausse. «Le télétravail a amplifié le phénomène et, cette année, nous avons enregistré environ 32 000 annonces de cyberincidents», explique Pascal Lamia, délégué fédéral adjoint à la cybersécurité.

David Cabero, Security Officer chez Hotela, livre un autre chiffre qui permet de prendre la mesure du phénomène: «Près de 90 % des emails reçus chaque jour par nos entreprises sont identifiés comme spams et bloqués, mais il arrive que quelques-uns passent à travers les mailles des filets. La vigilance des utilisateurs finaux est donc essentielle.» Aujourd'hui, plus personne n'est à l'abri d'une cyberattaque – dans un tiers des cas, il s'agit de ransomwares, c'est-à-dire des logiciels malveillants qui prennent en otage des données personnelles. Si la menace est là, à un clic de souris, on peut en revanche l'anticiper et atténuer ses effets …

Comment? «Il est capital de faire un gros travail de préparation en amont, qui passe notamment par une sensibilisation des collaborateurs aux mails douteux ou encore sur le fait qu'une adresse email et un mot de passe ne suffisent plus à garantir une bonne sécurité», répond David Cabero. «La vulnérabilité principale reste, malheureusement, l'humain.»

Choisir en connaissance de cause

Et dans ce domaine, moins on anticipe, plus les répercussions réputationnelles et financières seront grandes. Car les montants impliqués peuvent vite être colossaux, eu égard aux multiples spécialistes auxquels il faut avoir recours pour gérer la crise, mais aussi pour faire face aux divers dommages occasionnés. «Le conseil d'administration doit donc pouvoir décider en connaissance de cause de l'allocation des ressources humaines et financières», estime Alexandre Voisin. De fait, cette thématique doit leur être présentée dans son ensemble et les décisions bien documentées. Cela passe notamment par des audits des systèmes (repérer les failles …), par une évaluation des risques par rapport au modèle d'affaires (que se passera-t-il si cela devait arriver?) et par la prise en compte du risque résiduel (souhaite-t-on transférer ce risque à un tiers, comme une assurance?). On peut aussi se projeter en imaginant les conséquences de la perte de données ou encore la manière dont on compte communiquer. Mieux vaut prendre des décisions par temps calme que dans la tourmente, et si possible de manière globale et en compagnie d'un spécialiste en cybersécurité. En matière de cybercriminalité, la prudence est mère de sureté.

Frédéric Rein
Correspondant en Suisse romande

Est-ce intéressant de contracter une assurance?

On peut s'assurer contre une grande diversité de risques (incendies, vols …). Les cyberattaques ne font pas exception. Si le montant de la prime d'assurance dépend grandement du niveau de préparation et des montants de couverture souhaités, Alexandre Voisin avance avec prudence un chiffre de 15 000 à 20 000 francs par million de couverture recherchée, avec une franchise de 150 000 à 200 000 francs selon les cas. Bref, ce n'est pas donné, mais cela peut en valoir la peine. Pour être éligible auprès d'un assureur du domaine cyber, il faut toutefois faire preuve d'une «bonne hygiène informatique». «Pour être accepté, il convient au préalable de démontrer un minimum de maîtrise sur douze contrôles incontournables», note le connaisseur. Quels sont-ils? Authentification multi-facteurs pour tous les accès externes; concept de sauvegarde solide; formation régulière et actualisée sur la protection des données et la sécurité des informations; plans de réponse aux cyberincidents existants et testés; traitement et protection des comptes d'utilisateurs, des droits d'utilisateur et d'accès; gestion des risques liés aux fournisseurs et à la chaîne d'approvisionnement numérique; surveillance et détection efficace des cyberévénements; segmentation appropriée du réseau; cryptage approprié pour la transmission et le stockage des données; mesures et outils efficaces contre les logiciels malveillants et les ransomwares; organisation et gouvernance appropriées en matière de cybersécurité; gestion efficace des correctifs et remplacement ou protection des systèmes en fin de vie.