L'AGEFI
QUOTIDIEN DE L'AGENCE ECONOMIQUE ET FINANCIÈRE À GENÈVE

Datum: 10.10.2017

Très vulnérables, les PME suisses ne sont pas prêtes à faire face aux cyberattaques

PWC. Une étude récemment publiée montre que toutes les entreprises suisses ont été victimes d'attaques en 2016, quels que soient leurs secteurs.

LEILA UEBERSCHLAG

Le risque de subir une cyberattaque fait désormais partie du quotidien de la plupart des entreprises suisses. Face à la brusque accélération d'attaques majeures depuis le début de l'année (Wannacry, NotPetya) et aux dégâts toujours plus ravageurs des malwares, des rançongiciels - ransomwares (logiciel malveillant qui crypte les données et réclame une rançon), des attaques par déni de services ou encore du vol de données, les entreprises sont – pour la plupart – mal équipées pour faire face à ces menaces. Une étude menée par PwC montre la vulnérabilité des sociétés helvétiques: en 2016, toutes les firmes interrogées ont été victimes – au moins une fois – d'une cyberattaque, quels que soient leurs domaines d'activités. «La Suisse, souvent identifiée à tord comme non ciblée, attire l'attention de nombreux cybercriminels», explique Nicolas Vernaz, Senior Manager Cyber Security chez PwC. «Le nombre d'attaques est en croissance continuelle et cela concerne tous les secteurs.

NICOLAS VERNAZ. *Selon le Senior Manager Cyber Security (PwC), le nombre d'attaques est en croissance continuelle.*

Parmi les cybermenaces existantes, les rançongiciels demeureraient aujourd'hui une des techniques favorites des criminels. Les ransomwares sont «relativement facile à mettre en place et font beaucoup de ravages. Si la victime n'a pas de sauvegarde, il est probable qu'elle se plie au chantage et paie la rançon», nous apprend Nicolas Vernaz. «C'est problématique, car la plupart du temps, le logiciel reste inexploitable, même après avoir payé.» Selon lui, il ne faudrait donc jamais céder au chantage, car cela ne servirait à rien. «Mieux vaut faire appel à une entreprise spécialisée dans le déchiffrage qui, pour la même somme, pourra peut-être récupérer les données.» Si les attaques de masses ne sont pas nouvelles, l'envergure d'une attaque telle que wannacry (qui a semé la pagaille planétaire et fait près d'un demi-million de victimes en mai dernier) est du «jamais vu».

Les PME sont les plus vulnérables

Les PME représentent l'épine dorsale de l'économie du pays, «La plus grande partie des entreprises en Suisse appartiennent à cette catégorie», rappelle Nicolas Vernaz. «En raison des précieux actifs immatériels qu'elles possèdent – comme les données de clients – elles sont particulièrement intéressantes», analyse-t-il. «De plus, les coûts pour attaquer les petites structures restent relativement bas, avec des retours sur investissements élevés.» Les PME sont donc les cibles privilégiées de rançongiciels ou encore d'escroqueries par e-mail. En juillet, 94 noms de domaine .ch et .li ont été détournés pour distribuer des logiciels malveillants. «Une telle attaque peut causer d'importants dommages à la réputation, la perte de clients et des répercussions juridiques (en cas de négligence).» Le défacement (modification non sollicitée de la présentation d'un site web, à la suite de son piratage) est également un problème majeur, puisque le site est la carte de visite de l'entreprise.

Perte de crédibilité

«Les ransomwares ont le potentiel de faire d'énormes dégâts. Il est primordial de construire des défenses et de conserver des sauvegardes sécurisées pour récupérer rapidement les données si une attaque se produit», avertit Nicolas Vernaz. Il observe pourtant une véritable méconnaissance quant aux risques encourus par les entreprises. «Elles ne se rendent pas compte de l'importance que prend le numérique dans leurs opérations quotidiennes. De plus en plus de processus sont digitalisés et si demain une PME

L'AGEFI
QUOTIDIEN DE L'AGENCE ECONOMIQUE ET FINANCIÈRE À GENÈVE

Datum: 10.10.2017

se fait hacker et qu'elle perd son système de paie ou de facturation, elle peut mettre la clé sous la porte. Il n'y a pas encore cette prise de conscience que le business peut réellement s'arrêter.»

Se protéger ne coûte pas cher

«Avec des mesures simples, il est possible d'augmenter le niveau de sécurité drastiquement», assure Nicolas Vernaz. «Former et informer les employés à ne pas ouvrir d'e-mails suspicieux par exemple». L'importance de connaître quels sont les actifs digitaux possédés est également, selon lui, primordiale. «La plupart des entreprises n'en ont aujourd'hui aucune idée. Il faut que la société comprenne ce qu'elle possède, pour amener une réponse appropriée par rapport à sa taille et son domaine d'activité.»■