Les PME sont accusées d’être trop naïves face aux cyberattaques. Est-ce vrai?

Technologie

En Suisse, les études mettant en avant l’impréparation des petites entreprises face aux cyberrisques se multiplient. Mais la réalité est plus nuancée que cela et des progrès ont été réalisés, affirme un expert. L’identité des auteurs de ces études est aussi débattue

Les études montrant la naïveté des PME se multiplient. — © bongkarn - stock.adobe.com

Anouch Seydtaghia
Publié jeudi 1 septembre 2022 à 20:00

Modifié vendredi 2 septembre 2022 à 08:39

Les PME suisses? Pour la plupart, elles sont mal préparées face aux cyberattaques, dont elles minimisent totalement les risques. Qui plus est, elles ne forment pas assez leur personnel. Sans parler de leur méconnaissance de la future loi sur les données, qui entrera en vigueur dans un an. Voilà, en substance, le contenu de la dernière étude d’Axa, parue cette semaine. Des conclusions qui rejoignent précisément celles d’autres rapports publiés ces derniers mois. Alors, les PME sont-elles aussi nulles que cela en cybersécurité?

Commençons par l’étude d’Axa, parue ce lundi. Selon son sondage, 15% des entreprises interrogées disent avoir été victimes d’une cyberattaque au cours des dernières années, des

personnes extérieures ayant tenté de pénétrer leur réseau interne. Ce qui n'empêche pas les patrons de PME de dormir, selon Axa: 62% d'entre eux estiment faible le risque d'être victime d'une telle attaque, seuls 12% le qualifiant d'élevé.

«De plus en plus visées»

Conséquence directe, peu prennent des mesures pour se protéger: seules 73% des PME effectuent des sauvegardes régulières de leurs données, et un peu plus des deux tiers utilisent un logiciel antivirus. Plus alarmant encore, un peu plus de la moitié (55%) ont installé un pare-feu afin de protéger leur réseau et 46% ont défini des règles pour la création de mots de passe. Et pourtant, le risque est élevé, selon Andrea Rothenbühler, responsable de l'assurance Cyber d'AXA: «Les PME sont de plus en plus visées par les hackers, qui profitent du fait qu'elles ne peuvent investir autant dans leur sécurité informatique que les grands groupes.»

Axa n'est pas la seule à constater cette impréparation. Fin juin, une étude commanditée notamment par Digitalswitzerland et La Mobilière, réalisée elle aussi sur la base d'un sondage, montrait que seule une PME sur cinq considérait comme élevé le risque de se faire attaquer. Et deux tiers des entreprises sondées disaient effectuer régulièrement des mises à jour de leurs logiciels et utilisaient des pare-feu. De plus, seule une PME sur dix estimait que la cybersécurité était l'affaire de chaque employé. La Mobilière estime à environ 13 000 le nombre de PME attaquées par des pirates. «Bon nombre de PME ont déjà été victimes de cyberattaques. Les directeurs disent être sensibilisés à ce propos, mais restent malgré tout passifs», affirmait cet été Andreas Hölzli, responsable du centre de compétence Cyber Risk à La Mobilière.

Deux catégories

Qu'en penser? «Attention, il faut différencier les toutes petites entreprises de celles comptant 50 à 200 employés, nuance Steven Meyer, directeur de la société de cybersécurité Zendata. Le coiffeur, le restaurateur ou le menuisier ne se sentent pas du tout concernés car ils ne manipulent a priori pas de données jugées sensibles. Par contre, ils pourraient tout de même se faire attaquer et voir leur activité paralysée.»

Selon Steven Meyer, «les entreprises gérant des données sensibles, comme les médecins, les notaires ou les responsables de fiduciaires, sont aujourd'hui très attentives à leur sécurité. L'immense majorité d'entre elles prennent des mesures pour accroître leur protection.» Pour le responsable de Zendata, «désormais, les grandes PME intègrent la sécurité dans leurs processus internes. C'est une évolution réjouissante.»

Mises à jour négligées

Un avis que partage en partie le Centre national de cybersécurité (NCSC): «La sensibilisation au thème de la cybersécurité s'est améliorée au cours des dernières années, tant au niveau des entreprises que de la population. Mais de nombreuses PME continuent de sous-estimer le danger d'une cyberattaque. Elles pensent qu'elles sont trop petites pour être intéressantes pour les cybercriminels. Or, les cyberattaques peuvent toucher tout le monde», répond une porte-parole du NCSC. Selon elle, «dans de nombreuses PME, le thème de la cybersécurité n'est pas encore abordé au niveau de la direction. De plus, les mesures de sécurité nécessaires sont malheureusement souvent négligées. Par exemple, les mises à jour de sécurité des logiciels ne sont pas appliquées à temps, ce qui est exploité par les cybercriminels.»

Se pose aussi la question des commanditaires des études précitées, souvent des assurances… qui veulent vendre des produits liés à la cybersécurité. «Les assureurs veulent vendre des assurances, mais avant tout aux entreprises qui présentent le moins de risques, estime Steven Meyer. Il faut donc être très prudent face à ces assurances, dont les prix explosent et le périmètre se réduit. La bonne chose, c'est que ces assureurs exigent des entreprises qui signent un plus haut niveau de sécurité. Normalement, les rançons demandées par les pirates ne sont pas couvertes, mais libre aux entreprises d'utiliser l'argent tout de même reçu pour ce qu'elles désirent, et pas uniquement la restauration de leur informatique.»
Lire aussi: Comment les PME peuvent se protéger des cyberattaques