Cybersécurité: les PME pas à l'abri

PAR MATTHIEU HOFFSTETTER

Face aux menaces sur les données et la sécurisation des systèmes informatiques, les PME sont loin d'être épargnées. Tour d'horizon des dangers pour celles qui constituent le coeur du tissu économique suisse.

#pme #cybersécurité

Selon une récente enquête, 65% des PME suisses se sentent concernés par le cyber-risque mais seulement 1% a identifié les cyber-risques qu'elle peut elle-même encourir. Face à cette disproportion, nombreux sont les acteurs du système à tirer la sonnette d'alarme. Du côté d'AlpICT, qui organisait mi-septembre une rencontre sur ce thème à Crissier, Delphine Seitiee pointe «la fréquence croissante des attaques cyber contre des entreprises suisses, et particulièrement des PME», mais également «les enjeux actuels avec l'étude de la loi sur la sécurisation des données».

Pour Ciaran Bryce, professeur à la HES Genève, «ces PME cherchent souvent de l'accompagnement. Le premier blocage quand il s'agit de cyber-risque n'est autre que la qu'est-ce que je fais? Et la réponse semble souvent complexe». Faut-il se contenter de logiciels et solutions toutes faites, ou au contraire investir de façon très poussée dans des dispositifs spécifiques en interne? La réponse est loin d'être évidente au premier regard. Et la complexité des enjeux pour des entrepreneurs n'ayant pas de connaissances approfondies du domaine a de quoi décontenancer.

Un constat que partage Nicolas Frey, co-fondateur de l'association Cyber-Safe, qui vise à mettre en place un label pour les PME: «Il convient de se poser une série de questions. Quels risques? Il faut identifier les dangers, trouver les vulnérabilités, savoir quelle est la valeur de ses biens et données qui seraient en danger. La confidentialité ensuite: qu'est-ce que ça va me coûter si mes données sont publiées en ligne et que mes concurrents y ont accès? L'intégrité également: quel impact est-ce que ça peut avoir si une personne peut modifier les données? Il y a aussi l'accessibilité: quel coût cela représente-t-il si je ne peux plus accéder à mes données? A titre d'exemple, quinze personnes ont travaillé pendant trois mois récemment au service d'une PME suisse pour récupérer les données cryptées par un pirate qui effectuait du chantage. Pour conclure, je dirais que toutes les protections ont des failles. Il faut vérifier et valider les protections existantes».

Toutes les données ont de la valeur

Et le tissu suisse de PME de pointe suscite les convoitises de pirates à travers la planète. Jusque dans des domaines où on n'attend pas forcément ces dangers sur les données. Ainsi, Cla-Val est l'un des leaders mondiaux des valves utilisées dans les réseaux d'eau. «L'innovation aujourd'hui c'est l'électronique: nos valves sont connectées et qui dit connexion dit données. Or, l'eau potable est un sujet sensible. Vous pouvez donc imaginer les enjeux», témoigne Christophe Zaretti, directeur général adjoint de Cla-Val Europe. Et les exemples de pépites de ce genre en Suisse sont très nombreux.

Pour Steven Meyer, CEO de ZenDATA, «les PME sont souvent réticentes à implémenter des dispositifs de cybersécurité, car elles s'estiment trop petites… mais on ne parle jamais des petits vols. Elles pensent n'avoir rien de sensible en leur sein, mais tout est monétisable. Enfin, nous rencontrons des dirigeants parfois fatalistes: les grands groupes se font hacker alors qu'ils ont des budgets importants pour la cybersécurité… quel coût faut-il dès lors investir pour se protéger? Mais ce raisonnement est faillible: les hackers investissent selon le gain estimé: s'ils peuvent avoir un petit gain facilement, ils s'attaqueront à de petites proies».

Cependant, quelle attitude adopter? Quelles précautions prendre? Comment s'assurer que les mesures élémentaires soient déjà en oeuvre? Patrick Amaru, directeur général de la Direction générale du numérique et des systèmes d'information (DGNSI) à l'Etat de Vaud, explique que la politique cantonale s'appuie sur cinq piliers: «Données, infrastructures, accompagnement des personnes, accompagnement des entreprises, gouvernance. Sur notre site web, nous avons mis une dizaine de bonnes pratiques pour les cas concrets». Sur cette voie, le canton de Vaud s'est d'ailleurs allié aux autorités genevoises pour engager une initiative commune baptisée Trust Valley, qui doit démarrer en octobre 2020. Lors de l'annonce du lancement de cette plateforme en juin, le conseiller d'état vaudois Philippe Leuba affirmait que cette «Trust Valley» a le mérite de «dépasser les intérêts locaux». Signe que ces enjeux permettent de dépasser les clivages cantonaux ou partisans.

Des coûts à comparer aux risques

Une initiative d'autant plus cruciale qu'elle intervient à peine plus d'un an après l'entrée en vigueur du Règlement général pour la protection des données (RGPD) pour l'Europe depuis mai 2018, et alors que la révision de la loi suisse, qui date des années 1990, est en cours de traitement actuellement. «Il faut tenir compte de ce changement de paradigme et des attentes des autorités, afin de viser la maîtrise des données personnelles», insiste Philipp Fischer, partenaire fondateur du cabinet d'avocats Oberson Abels. Pour lui, «Le risque principal n'est pas la sanction encourue mais on aura un préposé fédéral à la sécurisation des données qui pourra noter des entreprises et le risque réputationnel lié à cela est sans doute bien plus important».

Après l'incompréhension et la méconnaissance des enjeux, un autre facteur d'inaction des dirigeants de PME réside dans les coûts de cette protection. Or, la gamme des prix dans la sécurisation des données est extrêmement variable. «Le coût n'est évidemment pas le même à avoir ses données chez soi avec ses propres serveurs sécurisés, dans un data-center ou dans un cloud. Il ne faut pas ignorer le risque émotionnel à confier ses données à un prestataire de service mais avoir une démarche pragmatique est crucial», insiste Steven Meyer. Toujours évaluer le risque et ses coûts en cas d'attaque, et le prix d'une sécurisation de nature à décourager les pirates de s'y attaquer. Mais ne pas faire l'impasse sur les éléments d'une sécurité élémentaire.

Ciaran Bryce esquisse une analogie avec le domaine de la construction et du bâtiment: «On ne demande pas à un architecte de renoncer aux portes de sécurité incendie pour des raisons de délais ou de budget; il ne faut pas que les informaticiens renoncent à des sécurités pour des raisons de temps ou de coût, et il ne faut pas que les clients se passent de ces sécurités. Il faut que les PME comprennent que ces enjeux sont cruciaux».

Pour Steven Meyer, l'une des premières précautions réside dans une formation adéquate aux enjeux et aux bonnes pratiques pour les collaborateurs. Et pour motiver ces derniers, il y un argument tout trouvé: «Former ses employés c'est aussi leur faire comprendre que les compétences acquises en entreprise pour protéger les données de l'entreprise vont aussi leur servir dans leur vie privée, afin de protéger la sérénité de leur famille».