TECHNOLOGIES

Face à une cybermenace croissante, les PME belges obligées de s'adapter

Dans un contexte d'explosion des attaques informatiques visant tant le secteur public que privé, les PME sont mises face à de nouvelles responsabilités, notamment légales. Pas à pas, elles tentent de s'adapter, en dépit de plusieurs freins.

MATHIEU COLINET, ARTHUR SENTE

En septembre, *Le Soir* rapportait comment la PME namuroise Inforius, qui développe des solutions informatiques pour un très grand nombre de communes et qui manipule à ce titre beaucoup de données personnelles, avait vu une partie de ses données publiées délibérément sur le « dark-web » par des pirates peu scrupuleux. Un cas loin d'être isolé au cours de ces derniers mois.

Cet été, c'était notamment l'Ihecs (l'Institut des hautes écoles des communications sociales, à Bruxelles) qui faisait l'objet d'une attaque de type « *ransomware* » (une intrusion qui se caractérise par une paralysie des serveurs de la cible suivie d'une demande de rançon en échange d'un déchiffrement des données dérobées). On pense également à la société de production Dreamwall, sous-traitante de la RTBF, qui a fait les frais en mai dernier d'une telle intrusion, ce qui a eu pour effet de perturber certains programmes télévisés.

Entre janvier et juin 2024, le Centre belge pour la cybersécurité (CCB) a recensé par moins de 40 cyberattaques avec demande de rançon, d'après deux rapports trimestriels qu'il nous a transmis. Des cas extrêmes qui ne représentent cependant que le sommet de l'iceberg en matière de cybercriminalité. L'an dernier, les statistiques policières belges ont ainsi recensé pas moins de 5.074 faits relevant du « hacking » informatique, sur un total de 60.304 faits concernant de près ou de loin la « criminalité informatique ». Des chiffres qui, malgré une légère baisse affichée par rapport à l'année précédente, témoignent d'une explosion au cours des dix dernières années.

Nouvelles responsabilités légales

S'il est évident que toute entreprise, ASBL ou institution publique ciblée par une cyberattaque demeure avant tout une victime, cela n'exclut pas l'existence de certaines responsabilités incombant à toute entité qui manipule les données d'autrui. Des responsabilités qui, d'ailleurs, vont désormais être davantage balisées en ce qui concerne la prévention des cyberattaques et la réaction adéquate à adopter en cas d'incident.

A partir de ce vendredi 18 octobre, une nouvelle loi, dite « NIS2 », entre effectivement en vigueur en Belgique. Transposition de la seconde version de la directive européenne « sur la sécurité des réseaux et des systèmes d'information », celle-ci a pour objectif, selon le Centre pour la cybersécurité en Belgique (CCB), de « renforcer les mesures de cybersécurité, la gestion des incidents et la supervision des entités fournissant des services essentiels au maintien d'activités sociétales ou économiques critiques ». Au menu : enregistrement obligatoire auprès de l'autorité fédérale, obligation de rapporter tout incident et mise en place d'un cadre de base en matière d'hygiène numérique et de procédures.

Selon le porte-parole du CCB, Michele Rignanese, on peut anticiper au regard des critères définis qu'environ 2.500 entreprises de taille moyenne ou supérieure seront concernées (lire par ailleurs). Sont par ailleurs visées toutes les entreprises qui fournissent des services considérés comme « hautement critiques (santé, eau potable, administration publique…) et « critiques » (fournisseurs numériques, production/transformation/distribution alimentaire, services postaux…).

« Ce serait la fin de l'aventure »

Les attaques qui se répètent d'une part, les obligations qui proviennent de la nouvelle loi d'autre part : les entreprises belges devraient en principe avoir trouvé dans tout cela « matière » à faire de la cybersécurité un nouvel axe de travail ces derniers mois. Mais sur le terrain est-ce vraiment bien le cas ? Pour le savoir, petit coup de sonde qui vaut ce qu'il vaut dans quatre entreprises.

Première escale chez Rosa, une start-up bruxelloise qui a développé une application de prise de rendez-vous médicaux et qui emploie une cinquantaine de personnes. La cybersécurité y semble un sujet crucial. « C'est normal », affirme Sébastien Deletaille, administrateur délégué. « On travaille aujourd'hui avec une vingtaine d'hôpitaux. Si du jour du lendemain, disons pendant une semaine, ceux-ci ne pouvaient plus organiser de rendez-vous à la suite d'une attaque paralysant notre application, ce serait très clairement la fin de l'aventure… » Selon le responsable, la question de la cybersécurité a toujours été au centre des pratiques de l'entreprise. La sophistication des attaques l'a obligée fréquemment depuis lors à adapter sa protection. « Aujourd'hui, par exemple, on est passé à une authentification à plusieurs facteurs sur notre système. Ce qui nous oblige à nous *logger* avec une clé USB. »

A Mons, l'entreprise de traduction Stoquart, qui emploie une septantaine de personnes, a fait aussi semble-t-il de la cybersécurité un axe de travail. Ce qui l'a incitée à franchir le pas ? Le fait d'avoir dans son portefeuille de clients des entreprises appartenant à certains secteurs sensibles. La société a fait réaliser un audit par un consultant, un travail lui a permis d'identifier des vulnérabilités qu'elle a entrepris de corriger depuis lors. « On a déjà fait beaucoup », affirme Dimitri Stoquart, le CEO. « Le reste se fera progressivement en fonction des objectifs qu'on s'est fixés. »

De retour à Bruxelles, cette fois chez l'entreprise Accountable, qui a conçu une application comptable pour indépendants. Là aussi les cyberattaques ne sont pas un risque pris à la légère, répète-t-on. « On n'a pas attendu les accidents récents qui ont frappé certains organismes en Belgique pour le prendre en compte », explique Nicolas Quarré, le CEO. « On manipule des données comptables. C'est donc extrêmement sensible. On a toujours tenté d'aligner le risque existant aux mesures prises pour le diminuer. Notre croissance année après année le rend plus important. On adapte donc aussi la sécurité de nos procédures. »

Dernière escale à Frameries chez Rubbergreen, une entreprise innovante qui fabrique différents produits à partir de caoutchouc recyclé et qui emploie une quarantaine de personnes. « Au départ, c'est un des actionnaires qui a alerté sur ce danger après qu'une de ses entreprises a été ciblée », explique le responsable Olivier Prud'homme. « Depuis lors, on a commandé un audit et on a pris des mesures pour que le risque se situe à un niveau acceptable. »

Une préparation à nuancer

Quatre sociétés et autant de préoccupations affichées de faire de la cybersécurité un chantier comme un autre : les entreprises belges auraient-elles donc toutes fait déjà le *shift* nécessaire pour s'adapter à cette nouvelle donne ? Pas si sûr. Ce n'est en effet pas « l'écho » qui remontait cette semaine de la Cyberweek, un événement organisé en Wallonie par l'Agence du numérique et ses partenaires.

Sur place, des responsables informatiques et des consultants évoquaient ainsi de façon anonyme – le sujet est sensible – des efforts « très variables d'une société à l'autre », la difficulté de « sensibiliser certains patrons à l'importance d'entamer le chantier de la cybersécurité », une confiance « démesurée en la capacité de résilience des entreprises » en cas d'attaques ou encore le coût « non négligeable des mesures de protection » – *a fortiori* pour des PME.

De quoi en tout cas nuancer cette idée selon laquelle les entreprises seraient déjà toutes prêtes à affronter cette nouvelle réalité…

La loi « NIS2 » en bref

Qui est directement concerné par la nouvelle loi dite NIS2 ? Théoriquement, toutes les entreprises de taille moyenne (en règle générale, celles qui comptent plus de 50 ETP et un chiffre d'affaires annuel excédant les dix millions d'euros) ou les entreprises de plus grande échelle. Certaines sociétés qui ne rentrent pas dans ces critères de taille peuvent également être concernées en fonction de leurs activités spécifiques. Sur le site internet https://at-work.safeonweb.be/fr/nis2, un simulateur permet de savoir si une entreprise rentre ou non dans le champ d'application de la loi.
Pour les sociétés concernées, la première étape prévoit un enregistrement auprès du Centre pour la Cybersécurité Belgique, via la plateforme d'enregistrement Safeonweb@Work. Ensuite, la loi énumère onze mesures minimales à mettre en place. Par exemple, le fait de recourir à des solutions d'authentification à plusieurs facteurs pour leur personnel, ou de prévoir un cadre relatif à la formation à la cybersécurité en interne. Enfin, la loi prévoit l'obligation de rapporter tout incident « significatif » auprès du Centre pour Cybersécurité, dans un délai de 24 heures, et impose un devoir de coopération avec les autorités. A.SE

AUSTRALIE

Charles III à Sydney, son premier long voyage depuis l'annonce de son cancer

© REUTERS.

Le roi Charles III est arrivé vendredi soir en Australie pour une tournée de six jours, son voyage le plus éprouvant physiquement depuis l'annonce de son cancer en février, et au cours duquel il devrait aborder les sujets environnementaux, qui lui tiennent à cœur. Après un voyage de plus de 20 heures, le monarque de 75 ans et son épouse la reine Camilla ont atterri dans une ville de Sydney détrempée par la pluie et ont été accueillis par des dignitaires locaux et des enfants porteurs de bouquets. « Nous avions vraiment hâte de retourner dans ce beau pays pour célébrer les cultures et les communautés extraordinairement riches qui le rendent si spécial », a déclaré le couple dans un message posté sur les réseaux sociaux avant leur arrivée.

Le roi effectue une tournée de neuf jours dans les terres lointaines d'Australie et de Samoa, dont il est le monarque. Il participera à un barbecue, visitera des monuments célèbres. Il devrait en Australie souligner les dangers du changement climatique dans un pays marqué par les feux de brousse et les inondations. Il rencontrera aussi des scientifiques dans un laboratoire de recherche travaillant sur le cancer.

Charles est le premier monarque britannique en exercice à poser le pied en Australie depuis 2011. Cette année-là, sa mère, la reine Elizabeth II, avait été accueillie par une grande foule.

Son voyage, prévu de longue date, vise à renforcer le prestige de la monarchie auprès d'un public australien largement indifférent à la visite du souverain. AFP