Cybermenaces : sommes-nous condamnés à l’échec ?

Intermarché, Amazon, Free… En l’espace de quelques semaines, ces entreprises ont été confrontées à des fuites de données d’une ampleur inédite, soulignant l'urgence d'un changement en profondeur à mettre en œuvre dans l’ensemble de l’écosystème. Par Brice Augras, président de BZHunt, dans nos Tribunes d'hiver.

Temps de lecture : minute

---

2 janvier 2025

Les atteintes numériques ont bondi de 40 % ces cinq dernières années en France. Un chiffre tristement record. Face à cette escalade, une question centrale demeure : comment y faire face ? Si la technologie est cruciale, elle ne constitue pas une réponse suffisante. L’humain, souvent perçu comme le maillon faible, pourrait paradoxalement être notre meilleur atout en la matière, à condition d’adresser les problèmes de fond. Car les responsabilités qui pèsent sur les directions ne cessent de croître, rendant urgente la recherche de solutions adaptées pour renforcer la résilience collective.

Des impacts économiques et psychologiques, liés à un no man’s land juridique

Les impacts économiques et réputationnels d’une cyber attaque ne sont plus à démontrer. Mais elles ont aussi un coût psychologique. Les dirigeants IT portent aujourd’hui sur leurs épaules le poids d’une immense responsabilité. Et pour cause : les entreprises, quel que soit leur secteur ou leur taille, dépendent désormais d'une activité numérique, qui implique une plus grande responsabilité pour l’ensemble des métiers IT.

Cette année, un client, victime d’une cyber attaque, me confiait avoir vécu un véritable traumatisme professionnel, marqué par une semaine d’angoisse et de stress. L’équipe IT, en particulier sa responsable, a même mentionné une paranoïa constante à l’égard des moindres signaux de danger. Et ce n’est pas un cas isolé.

Selon une récente étude, 83 % des professionnels de la cybersécurité estiment que l’épuisement professionnel a même causé des erreurs dans leur service. Ces situations pullulent dans la profession, où les responsabilités sont de plus en plus importantes. Et je ne peux que les comprendre. Ils sont garants de toute la sécurité et de la bonne santé de l’ensemble d’un système d’information d’une entreprise. Et in fine, ils peuvent se retrouver sur un siège éjectable, du jour au lendemain. Car d’un point de vue juridique, la situation reste complètement floue.

En cas de cyber incident, un employeur peut-il licencier un.e RSSI pour faute grave, alors même que des plans de formations et de sensibilisations adéquats n'ont pas été mis en place ? Comment le droit du travail peut-il évoluer et prendre en compte les enjeux cyber ? Nous avons des directives européennes, des autorités de contrôle et des textes de loi. Mais rien sur le sujet de la responsabilité professionnelle. Personne ne s’est encore saisi du sujet - pas même le code du travail. Ce vide juridique sera nécessaire à adresser urgemment dans les années à venir.

Avec une couverture qui n’assure pas suffisamment nos arrières

Si le code du travail n’a pas intégré cette nouvelle réalité métier, le marché de l’assurance cyber semble, lui aussi, encore loin - très loin - d’être mature. Depuis la prise de conscience générale des risques et impacts économiques des cyberattaques, le marché de l’assurance semble avoir connu trois grandes phases : celle d’un marché quasi-inexistant, puis celle d’un marché stratégiquement porteur d’un point de

vue économique. Et enfin, celle d’un marché marqué par une rentabilité en déclin, voire à perte, qui a conduit à une stratégie de rétropédalage.

En effet, si certaines assurances ont tenté de couvrir les rançongiciels dans un premier temps, les exclusions sont aujourd’hui si nombreuses que les contrats peuvent s’avérer devenir de véritables casses-têtes. Par ailleurs, les primes d’assurance ont explosé, tandis que les conditions d'accès aux remboursements sont devenues particulièrement strictes. Ce durcissement a poussé certains dirigeants à revoir leur stratégie d’investissement. Certains d’entre eux m’ont même confié préférer réinvestir le budget alloué à leur assurance directement dans la gestion de leur cybersécurité ou dans leurs infrastructures ; estimant que les restrictions des contrats ne couvriraient de toute façon pas l’intégralité des frais en cas de cyber incident. C’est donc inévitable.

Quelle que soit la taille de l’entreprise : l’humain doit être placé au cœur de la stratégie de réduction des cyber risques. Et sans une sensibilisation continue, les entreprises resteront vulnérables. C’est de la responsabilité des entreprises de… donner les responsabilités à chacun et chacune d’entre nous.

La course à l’IA nous fait encourir un risque supplémentaire

Depuis deux ans, l’IA est sur toutes les lèvres. Et sa médiatisation – à outrance – a occulté un fait majeur : elle n’est pas nouvelle. La véritable nouveauté : elle est passée des mains d’experts initiés à celles du grand public. C’est parce qu’elle s’est immiscée dans le quotidien professionnel de tous les actifs qu’il s’agit aujourd’hui d’un véritable basculement technologique. Néanmoins, nous assistons aujourd’hui à une course effrénée à son implémentation, qui pose de sérieux risques. En voulant aller trop vite, les entreprises sacrifient parfois la sécurité au profit de la performance. À ce jour, seulement 63 techniques de vulnérabilité liées à

l’IA ont été définies et dont l’exploitation a été décrite selon le référentiel MITRE ATLAS. Nous ne connaissons pas encore l'ensemble des failles potentielles – d'autant plus que de nouvelles fonctionnalités apparaissent chaque mois. La communauté de chercheurs travaille ardemment à ce sujet. Mais les travaux sont actuellement en cours et ne sont pas encore aboutis. Prudence est donc, infailliblement, mère de sûreté.

En cette fin d’année 2024, nous nous trouvons à un tournant critique. La cybersécurité ne peut plus être perçue comme une contrainte ou une simple option : elle doit être intégrée dans les stratégies des entreprises et devenir une priorité pour l’ensemble des dirigeants. Nous devons mettre en place une conduite du changement collective et efficace, car, si 2024 a marqué un tournant dans la cyber insécurité, 2025 pourrait bien être l'année du pivot. En tout cas, j’espère que ce sera le cas. Parce que nous ne pouvons pas être condamnés à l’échec.

À lire aussi
Cybersécurité : un startup studio lancé au Campus Cyber pour propulser 10 pépites européennes en 5 ans

MADDYNEWS

La newsletter qu'il vous faut pour ne rien rater de l'actualité des startups françaises !

JE M’INSCRIS

Article écrit par Brice Augras, président de BZHunt