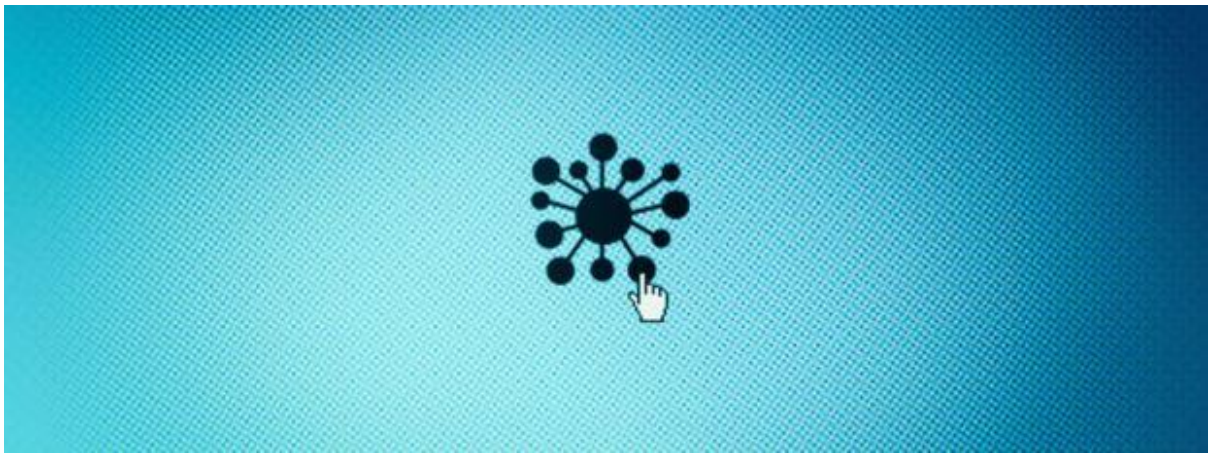
Cybersécurité : comment éviter une pandémie numérique

Le 06/04/2020

par **Cécile Vignial**



© GETTY IMAGES

Temps de lecture : 9 minutes

La crise sanitaire que nous traversons a de nombreuses conséquences collatérales. L'une d'elles est une vulnérabilité accrue des entreprises au risque cyber.

Le basculement de pans d'activité entiers en mode digital et le télétravail mettent à mal la cybersécurité des entreprises qui n'ont pas toutes pris leurs précautions. De plus, beaucoup d'acteurs malveillants ont déjà profité de ce moment où **l'urgence de la gestion de crise** prime souvent sur le respect des mesures de sécurité et où le désarroi fait baisser la vigilance pour multiplier les tentatives d'attaques.

Dans ce contexte, il est plus que jamais évident que **la cybersécurité ne relève pas uniquement du département informatique**. Il s'agit d'une urgence absolue. Il appartient donc aux dirigeants de prendre la mesure du risque, de s'assurer régulièrement que l'entreprise adapte la gestion de sa sécurité digitale à ce nouvel environnement et de communiquer largement sur la responsabilité de chacun pour la préserver. Cela suppose de battre en brèche, à tous les niveaux de l'entreprise, ces trois idées reçues qui sapent pernicieusement notre vigilance.

« Ça n’arrive qu’aux autres »

Bien connu des économistes et des experts en gestion des risques, le biais psychologique qui consiste à imaginer que seuls les autres peuvent être touchés est l’ennemi numéro un : parce qu’elles sous-estiment leur exposition aux risques numériques, de nombreuses entreprises n’investissent pas assez dans leur sécurité.

Ce comportement est particulièrement fréquent dans les PME, qui pensent passer sous le radar de hackers avides de rançons ou d’informations économiques clés. Or, comme elles disposent de moins de moyens que de plus grandes structures pour protéger leurs systèmes d’information et les données personnelles qu’elles récoltent, elles sont au contraire des cibles très attractives. Dès 2017, environ 75% des TPE-PME avaient déjà subi une cyberattaque (80% de rançongiciels, qui prennent en otage des données, et 40% de dénis de service, qui rendent un service indisponible pour ses utilisateurs), dont l’impact économique moyen était d’environ 50% du chiffre d’affaires.

Dans le contexte de propagation du Covid-19, la sous-estimation du risque cyber est particulièrement préoccupante. D’abord, parce que le risque d’attaques augmente. Comme dans tous les épisodes de crise, les observatoires du risque numérique recensent depuis le début de celle du coronavirus une intensification des activités cybercriminelles. Le cynisme des attaquants est sans limite : en une semaine, **l’AP-HP qui gère 39 hôpitaux en Ile-de-France, puis l’OMS ont été ciblées**. Le nombre d’attaques est tel que certains évoquent déjà un risque de pandémie numérique.

De plus, dans un environnement économique particulièrement tendu, le coût de la non-protection est décuplé. Une entreprise vulnérable peut mettre à risque non seulement ses propres opérations, mais également tout l’écosystème dont elle est le maillon faible. Des épisodes récents ont donné un avant-goût de l’impact financier potentiel d’une cyberattaque majeure : **les coûts cumulés de NotPetya par exemple s’élèveraient à 10 milliards de dollars**. Aujourd’hui, le coût d’une attaque d’ampleur comparable serait bien plus grand, car beaucoup d’entreprises victimes, déjà exsangues, ne s’en relèveraient pas.

Soulignons enfin que tous les incidents cyber ne sont pas liés à des attaques extérieures. Le nombre de pertes ou de **fuites de données causées par le personnel de l’entreprise** – par erreur ou par malveillance –, ou par des pannes ou des migrations défectueuses est loin d’être négligeable.

Quelle que soit leur taille, les entreprises ne doivent donc pas se demander *si* elles seront victimes d'un incident cyber, mais *quand*, et tout faire pour éviter d'être victimes d'un virus informatique quand la lutte contre le coronavirus requiert déjà toute leur énergie.

« Mon entreprise est immunisée contre le risque cyber »

Recrutement de risk managers et d'experts IT toujours plus compétents, audits de risques poussés, process, logiciels et pare-feux informatiques sophistiqués, externalisation de la maintenance des systèmes d'information et de l'hébergement des données (dont les dangers sont souvent ignorés), tests réguliers de la résilience par des simulations d'intrusion… Beaucoup d'entreprises déploient un arsenal de protection très complet, au point que l'ensemble de leur personnel, jusqu'aux cadres dirigeants, se pense, quoi qu'il se passe, immunisé contre le risque cyber.

Pourtant, les attaques incessantes (parmi les dernières en date, **celle d'Essilor, victime d'une attaque en mars 2020**, et **celle de Chubb, assureur spécialiste**… des risques numériques) nous rappellent que tous les acteurs, y compris les mieux préparés, peuvent être touchés.

Le risque de cyberattaques ne cesse de croître. Le profil des attaquants visant les acteurs les mieux protégés se professionnalise. Des bandes du crime organisé, parfois soutenues par des Etats et d'importants moyens financiers, ont succédé aux adolescents geeks. **Le risque évolue également au rythme des progrès technologiques**, et notamment de l'intelligence artificielle, qui permet de cibler les messages, et du **développement de l'Internet des objets**, dont les cybercriminels ont immédiatement tiré profit. L'Agence nationale de la sécurité des systèmes d'information (ANSII) attire également l'attention sur **le développement d'attaques par rançongiciels qualifiées de « Big Game Hunting »** perpétrées par des groupes extrêmement sophistiqués ciblant particulièrement les entreprises financièrement robustes.

Face à un risque accru, la crise du Covid-19 place les entreprises dans une situation de particulière vulnérabilité. En plus d'**un choc économique d'une rare violence**, elles doivent gérer deux mutations éclair en raison des politiques de confinement. D'abord, le passage, pour beaucoup d'entre elles, de l'ensemble de leurs ventes/prestations, et plus généralement de leurs opérations, en ligne. La rapidité de ce changement est un énorme défi que leurs services informatiques n'ont pas eu le temps d'anticiper. Ensuite, **l'explosion du télétravail**. Après le 16 mars, en France, le

télétravail a été déployé à une échelle jamais expérimentée par le passé : le gouvernement français a cité le chiffre de 8 millions d'emplois compatibles avec le télétravail dans le secteur privé. L'impréparation dans laquelle de nombreuses entreprises ont dû basculer en télétravail, sans formation préalable du personnel et avec des équipements restreints, a encore augmenté les sources de vulnérabilité aux risques cyber : l'utilisation à des fins professionnelles de matériel privé, moins protégé et sur lequel on constate souvent des manquements de mises à jour de sécurité ; la qualité dégradée des réseaux domestiques ; et la tendance à baisser son niveau de vigilance lorsqu'on est chez soi.
Dans ce contexte, il est urgent de rappeler que la résilience cyber des entreprises, même les plus grandes, les plus renommées et les plus préparées, n'est pas acquise ; il en va de la responsabilité de tous leurs collaborateurs. Des consignes régulières, relayées au plus haut niveau de l'entreprise, doivent les inviter à respecter au moins trois bonnes pratiques, qui sont des protections très efficaces contre bien des attaques.

1. L'utilisation des supports de l'entreprise pour ses activités professionnelles. Elle s'accompagnera d'un recours à des mots de passe sophistiqués (**la majorité des attaques est due à des mots de passe trop simples ou réutilisés**) et de mises à jour systématiques des systèmes d'exploitation et anti-virus pour adapter la protection en continu. Rappelons à titre d'analogie que **les attaques Wannacry et NotPetya** se sont répandues en exploitant une vulnérabilité logicielle connue faisant déjà l'objet d'une mise à jour de sécurité. C'est l'absence de cette mise à jour qui a permis la propagation de l'attaque.

2. L'obligation d'éviter les réseaux Wi-Fi publics ou inconnus et de connecter son PC en VPN (Virtual Private Network, qui crée un lien direct entre ordinateurs distants authentifiés et les isole du reste du trafic). En cas de ressource VPN insuffisante, des horaires distincts pourront être établis par équipe. Les horaires de connexion VPN devront être également étendus pour éviter des déconnexions automatiques et toute tentation de communication en dehors de ce cadre sécurisé.

3. Le respect scrupuleux des mises en garde contre les e-mails malveillants. La crise actuelle se caractérise notamment par une recrudescence des tentatives de fraude au président (ou fraude aux ordres de virement) : les pirates profitent de la situation de crise et de l'éloignement

géographique des salariés, qui compliquent les vérifications d'usage, pour se faire passer pour un dirigeant et ordonner des virements hors process sur des comptes, souvent à l'étranger – un procédé particulièrement dommageable quand la trésorerie des entreprises est dans un état critique. Les observatoires du risque cyber recensent également de très nombreux cas d'attaques par hameçonnage ou phishing (envoi d'e-mails qui usurpent l'identité d'un tiers de confiance pour soutirer des informations personnelles). La situation anxiogène liée au Covid-19 a été immédiatement mise à profit par des acteurs malveillants, incitant des salariés à ouvrir un e-mail dont l'objet affiché concerne des informations sur le coronavirus ou les moyens de s'en protéger. Le coronavirus serait en passe de devenir le leurre le plus utilisé de tous les temps. Votre entreprise a-t-elle communiqué à ce sujet ?

« Quoiqu'il arrive, on est assuré »

Dans la plupart des entreprises, le management est persuadé que les diverses polices d'assurance souscrites par l'entreprise la couvrent contre le risque cyber. Toutefois, ce qui s'apparente tantôt à un patchwork tantôt à un mille-feuille de contrats ne forme pas toujours une couverture sans faille. Et si l'entreprise est couverte, l'est-elle pour tous les types de faits générateurs ? Pour tous les types de dommages, d'arrêts de l'activité ou bien de responsabilités vis-à-vis de tiers ? Pour quels montants de pertes ? Il est impératif de faire le point avec son assureur ou son courtier pour éviter d'avoir la mauvaise surprise qu'ont eu beaucoup d'entreprises au lendemain d'une attaque en découvrant qu'elles n'étaient pas assurées pour leur sinistre en particulier.
En effet, on ne s'assure pas contre le risque cyber comme on s'assure contre le risque d'incendie, pour lequel les dommages sont plus faciles à modéliser et les contrats plus standardisés. Pour fixer le montant de la couverture, il faut notamment connaître le montant des biens à assurer, mais surtout estimer les conséquences financières des scénarios auxquels l'entreprise peut être confrontée. De plus, il faut appréhender une offre d'assurance qui demeure complexe et peu transparente en dépit des efforts récents des acteurs du marché. Le risque cyber est parfois partiellement couvert par des contrats traditionnels, qui n'ont pas été conçus pour l'économie actuelle, largement numérique. Des couvertures spécifiques cyber complémentaires ont donc été développées – mais beaucoup d'entreprises l'ignorent encore, et ces dernières ont également leurs limites.

Pour celles qui ne l’auraient pas déjà pratiqué, un audit de leur couverture cyber serait judicieux pour avoir une vision claire de leur risque et de la façon dont il est couvert par les contrats existants. Elles pourront alors décider de leur appétit au risque pour ce qui n’est pas intégralement couvert, en fonction également de leur capacité à mobiliser rapidement des ressources financières après une attaque. Pour les plus petites structures, des contrats simplifiés ont été développés, qui permettent en outre de sécuriser des ressources techniques de gestion de crise et de communication.

Pour beaucoup d’entreprises qui opèrent aujourd’hui en mode gestion de crise ou dégradé, la sécurité numérique n’est pas la première de leurs considérations. Or c’est précisément maintenant qu’il faut s’en soucier : en quelques semaines, la pandémie globale a non seulement fragilisé l’activité économique et la cohésion sociale, mais les a aussi rendues dépendantes du digital, dans des proportions inédites.

Pour les entreprises condamnées au confinement, le cyberspace est le dernier espace partagé. Il appartient à leurs dirigeants de tout faire pour en préserver l’intégrité.