L'effet des confinements sur la cybersécurité des entreprises en trois graphiques

Le développement brutal du télétravail a obligé les entreprises à revoir leurs standards en matière de cybersécurité. 2021 s'annonce comme une année cruciale en la matière.

Temps de lecture : minute

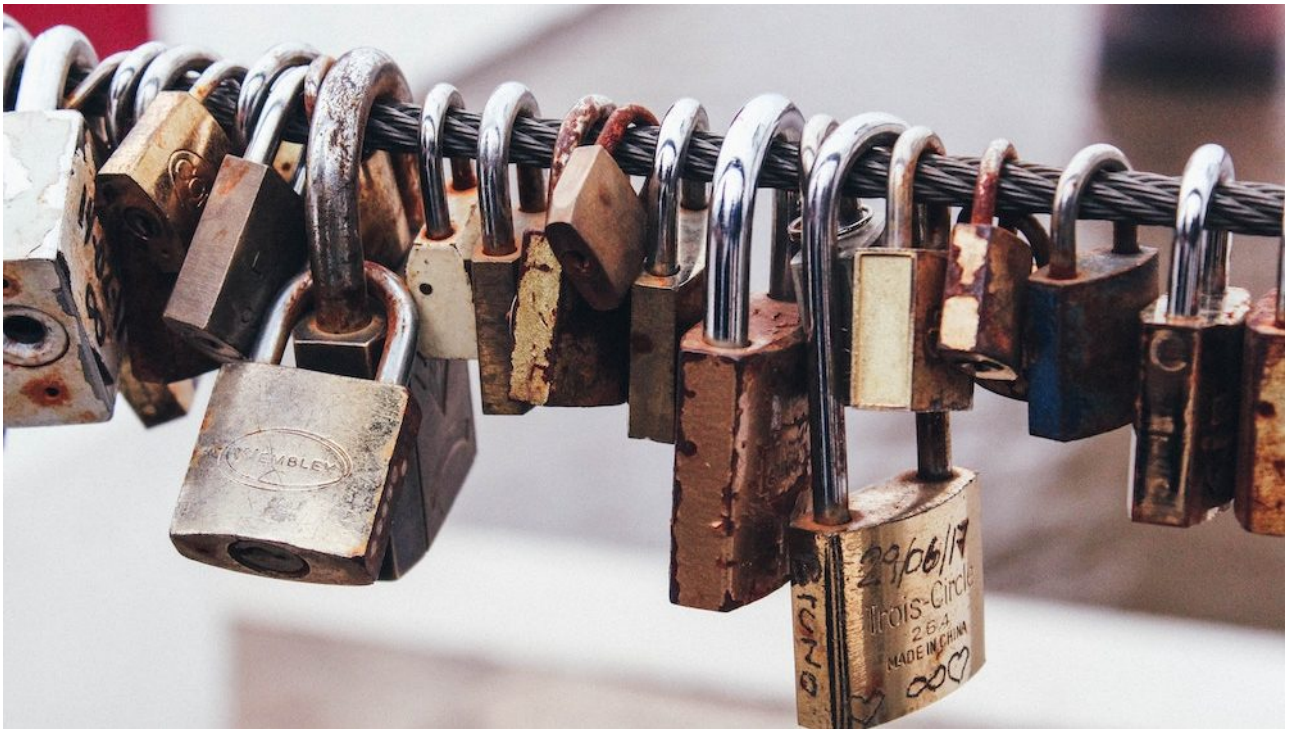
19 novembre 2020

Avec les confinements successifs, les entreprises ont pris bon gré mal gré le pli du travail à distance. De manière relativement brutale en mars et un peu plus préparée en octobre, elles ont - pour celles qui le pouvaient - dématérialisé une partie de leurs activités et de leurs communications internes ou externes. En-dehors des problématiques matérielles, elles ont également dû revoir leur stratégie en matière de cybersécurité.

Exit le réseau d'entreprise, le PC individuel et le téléphone fixe et sécurisé ; bonjour le wifi personnel, l'ordinateur portable partagé avec l'ado et le smartphone perso ouvert à tous les vents. Autant de brèches potentielles dans la sécurité de l'employeur...

À lire aussi
Les 10 erreurs de cybersécurité des startups technologiques

Et cela n'est pas près de se régler puisque les entreprises anticipent au contraire une accélération de leur numérisation, comme en atteste l'étude *Global Digital Trust Insights Survey 2021*, menée par PwC auprès de plus de 3000 entreprises. En 2021, 40% disent qu'elles accélèreront leur transition numérique, 39% s'organiseront pour passer leurs salariés en télétravail à temps plein et 37% accorderont davantage d'importance à la qualité des infrastructures de télécommunications pour leurs futures implantations de sites. De quoi encore accroître les besoins en matière de cybersécurité.



À lire aussi
Comment identifier vos besoins en cybersécurité ?

Ainsi, 55% des entreprises prévoient d'augmenter les budgets en cybersécurité. Mais 13% prévoient de les maintenir au même niveau et 26% de les diminuer. De quoi imposer à leurs équipes une certaine efficience. "*Clairement, la cybersécurité est devenu un enjeu business critique. Tirer le meilleur parti de chaque euro dépensé en la matière est devenu nécessaire au fur et à mesure de la numérisation des entreprises : chaque nouveau process ou atout numérique constitue une nouvelle vulnérabilité en matière de cybersécurité*" , note ainsi l'étude.

Rôle élargi des responsables en cybersécurité

L'évolution de ces budgets tient notamment compte des recrutements à venir au sein des équipes en cybersécurité. Plus de la moitié des entreprises prévoient ainsi de recruter des profils à temps plein en 2021

pour renforcer leur équipe. De quoi assécher littéralement le vivier de talents dans la branche : "*Recruter des experts en cybersécurité se heurte à certaines limites du marché,* note PwC*. Les études les plus récentes indiquent que, rien que sur le marché américain, il y a 50% de besoins non couverts. Dans le monde, 3,5 millions d'emplois en cybersécurité ne devraient pas trouver preneur en 2021*" .

Pas question pour autant d'embaucher sur n'importe quelles bases. Avec l'augmentation des besoins, les fiches de poste se sont allongées et les recrutements en cybersécurité réclament désormais autant de compétences techniques que business ou relationnelles. "*Définir le futur de la cybersécurité - qui doit être en phase avec l'activité de l'entreprise - signifie recruter des talents qui sont prêts à travailler de manière collaborative avec les autres pour régler des problèmes nouveaux et analyser l'information*, note PwC. *Ces qualités intrinsèques correspondent au rôle élargi des responsables en cybersécurité, qui sont non seulement des leaders techniques mais doivent aussi travailler avec les autres membres de la direction et présenter une valeur ajoutée à l'activité de l'entreprise.*"

Cette pénurie de talents couplée à des exigences toujours plus importantes des employeurs les encouragent à rechercher les perles rares en interne. Ainsi, ils sont de plus en plus nombreux à proposer des formations à certains collaborateurs afin de les faire monter en compétence sur les compétences qu'ils ne maîtrisent pas encore. Mais qui complètent utilement leur palette pour correspondre aux nouveaux besoins de leur employeur.

Article écrit par Geraldine Russell