Lorsque la sécurité est considérée comme un moteur d'activité, tout le monde y gagne

Avec la Covid-19, nous avons appris à nous adapter. La bonne nouvelle c'est que l'adaptation génère parfois du bon. En effet, la crise du Covid19 et les contraintes qu'elle a engendrées nous ont appris à définir les priorités en fonction des résultats les plus importants. Elle nous a montré que bon nombre d'activités jugées « prioritaires » avant le mois de mars ne l'étaient pas vraiment.

La résilience est également apparue comme l'un des principaux objectifs des programmes de sécurité, un moyen pour les entreprises de maintenir leur productivité et de bénéficier d'un avantage concurrentiel.

Durant cette période, qui aura des effets durables sur nos modes de vie et de travail, nous devons continuer à privilégier les priorités qui nous permettent de rester concentrés sur nos objectifs clés. À supposer que le travail distribué devienne la norme et non l'exception, la question est de savoir comment sécuriser les données, les processus et les communications quel que soit l'endroit où se trouvent les employés et les tiers.

Les équipes de sécurité commencent à réajuster leur temps, leurs efforts et leur budget en conséquence. McKinsey & Company a récemment mené une enquête auprès de 250 RSSI et professionnels de la sécurité au niveau mondial. Il en ressort qu'au cours des 12 prochains mois, les grandes entreprises dépenseront encore plus dans la sécurité des réseaux, la gestion des identités et des accès, et la sécurité des systèmes de messagerie, c'est-à-dire les priorités liées à la mise en place d'un personnel et d'une infrastructure distribués.

Concernant les fournisseurs en cybersécurité, McKinsey a identifié diverses façons d'aider les clients, notamment par la refonte des modèles de prestation de services et de déploiement de solutions, et la création d'offres supplémentaires.

Du côté des entreprises, nous avons observé une réaffectation des priorités et des investissements au cours des derniers mois, les équipes de sécurité travaillant en partenariat avec les dirigeants d'entreprise pour relever les défis de longue date suivants :

• **Dynamiser l'activité, en toute sécurité :** L'époque où la sécurité constituait un frein à l'activité est bien révolue. La crise du Covid19 nous a montré que la sécurité permettait aux entreprises d'évoluer rapidement et en toute sécurité. Pratiquement du jour au lendemain, des projets de transformation numérique, de modernisation de l'infrastructure et des accès, et de collaboration ont vu le jour. Ils ont été payants puisqu'ils ont aidé les entreprises à améliorer leurs résultats et à aller de l'avant.
Et ce n'est qu'un début. En poursuivant ces initiatives, l'objectif est d'intégrer la sécurité à ces nouveaux processus et à cette nouvelle infrastructure. Il nous faudra revoir nos vieilles méthodes de travail, mais cela ne doit pas nous arrêter. Nous savons à présent tout ce qu'il est possible d'accomplir lorsque la sécurité est perçue comme un moteur d'activité.

• Réduire la complexité : Pendant des années, nous n'avons rien trouvé de mieux à faire pour atténuer les risques que d'ajouter une couche de sécurité supplémentaire.
Résultat : la plupart des équipes de sécurité des grandes entreprises utilisent aujourd'hui des dizaines de produits de sécurité qui sont souvent mal intégrés.
Cette complexité constitue une perte de temps considérable, mais aussi un gaspillage de ressources. Il devient évident que, dans de nombreux cas, la meilleure stratégie consiste à repenser notre façon d'aborder les contrôles de sécurité spécifiques et à chercher des moyens de réduire la complexité en remplaçant plusieurs produits par une nouvelle catégorie de solutions, car les besoins ont évolué. Tout comme pour le premier point, changer complètement d'approche et prendre des décisions n'est pas simple à court terme, mais offre des avantages à long terme.

• Assurer la résilience : L'environnement actuel a démontré que la défense n'était pas un processus binaire. Il est impossible d'anticiper tous les vecteurs et scénarios d'attaque potentiels.
Nous devons donc intégrer la résilience dans notre infrastructure et nos contrôles de sécurité.
La cyber-résilience mesure la capacité d'une entreprise à gérer une cyberattaque ou une faille de données tout en continuant à exercer efficacement ses activités.
Là encore, les programmes de sécurité doivent être considérés comme des moteurs d'activité, même en cas d'attaque.
À présent que la ruée initiale vers un modèle plus distribué est derrière nous, il serait bon de nous demander comment renforcer la résilience. Ces mesures proactives doivent être au cœur de tout programme de sécurité.

Tout cela est parfaitement logique d'un point de vue intellectuel, mais nous savons que l'être humain est attaché à ses habitudes et n'aime pas y déroger. Au début de la crise, nous étions disposés à changer pendant une courte période. Mais comment inscrire ces changements dans la durée ? Il est nécessaire de modifier les indicateurs clés de performances (KPI) pour qu'ils reflètent l'importance de la résilience et de l'accélération de la transformation numérique.

Les RSSI doivent rendre compte au conseil d'administration de la façon dont la sécurité favorise des initiatives spécifiques, comme la collecte de données, leur stockage et leur analyse dans le Cloud, ou la surveillance et la gestion à distance des processus de fabrication, qui permettent de répondre aux objectifs opérationnels et d'atténuer les risques. C'est en alignant les indicateurs et les mesures incitatives sur les nouvelles priorités que les RSSI et les conseils d'administration pourront maintenir la dynamique.

Enfin, les fournisseurs de technologies et les offres doivent également évoluer pour s'adapter au changement de priorités et au caractère distribué des opérations métiers. Nous constatons déjà une hausse de l'activité, avec notamment :

• Une plus grande facilité de déploiement, une simplicité d'utilisation et une conception intuitive : Les outils de sécurité d'entreprise ont toujours souffert de lacunes à ces égards, mais les choses se sont améliorées au cours des dernières années. La pandémie de Covid-19 n'a fait qu'exacerber la nécessité de telles caractéristiques.

• L'exploitation de l'accès à distance pour les projets de transformation et la prestation de services : Dans certains domaines opérationnels, comme l'optimisation de la production, les prestataires qui, auparavant, fournissaient ces services sur site ont désormais besoin d'accéder à

distance aux équipements pour honorer leur contrat et assurer le bon fonctionnement des lignes de production. À l'avenir, ce mode d'interaction devrait, dans la mesure du possible, être privilégié.

• La reprise des discussions autour du Cloud en mettant l'accent sur des mises à jour simplifiées, une meilleure sécurité des solutions Cloud et l'ajout accéléré de nouvelles fonctionnalités. Lorsque la résilience est un objectif clé, ces avantages sont très appréciés. Face à notre nouvelle réalité, seules les solutions Cloud natives et faciles à déployer à grande échelle ne seront pas menacées d'obsolescence étant donné que les clients exigent une infrastructure flexible et sécurisée facile à étendre et à mettre à niveau.

Avec la pandémie de Covid□19, les programmes de sécurité et les offres technologiques évoluent. Il est très encourageant de voir les équipes de sécurité et les dirigeants d'entreprise tendre vers un avenir plus résilient et distribué. C'est l'un des points positifs de cette situation, car lorsque la sécurité est considérée comme un moteur d'activité, les défenseurs sont gagnants.