Pour 6 entreprises sur 10, l'accès à distance est l'un des principaux cyber-risques dans cette nouvelle normalité

Jusqu'à la crise de la Covid-19, la plupart du travail était fait en présentiel. Cependant, le panorama a radicalement changé et les entreprises ont dû faire face à une nouvelle réalité professionnelle, dans laquelle elles devront combiner le travail dans les locaux

et à distance. Ceci rend nécessaire de disposer d'outils sécurisés pour l'accès à distance à l'information. Compte tenu de ce nouveau scénario, 62% des professionnels de la cybersécurité estiment que l'accès à distance sera l'un des principaux risques pour toutes les entreprises.

Dans ce nouveau contexte, 79 % des entreprises parient sur le renforcement de leur niveau de cybersécurité, car 3 sur 4 craignent une augmentation significative de l'utilisation des cybermenaces contre leur infrastructure. Il est évident que la situation actuelle est totalement nouvelle pour toutes les entreprises, ce qui implique que nous sommes dans un processus d'adaptation constant.

Les entreprises françaises ne sont pas totalement préparées à faire face aux défis que présente cette nouvelle normalité. Pour cette raison, et compte tenu du fait que l'accessibilité et la mobilité des données commerciales seront désormais un élément clé ; le choix des solutions de sécurité Zero Trust et la protection des environnements Cloud sont présentés comme le socle essentiel de la stratégie de sécurité.

En outre, il est important de souligner qu'il sera désormais primordial de sécuriser chacun des équipements qui seront connectés au réseau de l'entreprise, car l'adoption d'une approche basée sur la prévention en temps réel des menaces est indispensable dans ce nouveau paradigme.

L'un des plus grands défis : la cybersécurité dans le travail à distance

De même, face au défi de la nouvelle normalité, il est fréquent de penser qu'il y a beaucoup de différences entre une petite PME et une grande entité, mais au fond, il y a plus de facteurs déterminants que la taille des entreprises. Ceux qui travaillaient déjà à distance ont une expérience préalable qui leur permettra de gérer cette nouvelle situation de manière beaucoup plus fluide, tandis que ceux qui ont été contraints de faire du télétravail à partir de rien auront beaucoup plus de mal. La taille de l'entreprise est à cet égard tout à fait secondaire.

Dans cette nouvelle ère, où le travail à distance est au centre des préoccupations, la protection des équipements doit faire l'objet d'une attention particulière. Dans cette situation où la plupart des entreprises disposent d'une part importante des collaborateurs en situation de mobilité, 75 % des experts en cybersécurité s'accordent à dire que cet accès constitue un risque supplémentaire dans lequel les lacunes et les menaces en matière de sécurité vont se multiplier, augmentant ainsi le danger.

Pour faire face à cette situation, il faut appliquer des techniques de contrôle d'accès au réseau, c'est-à-dire contrôler quelles informations sont exposées, quels utilisateurs peuvent y accéder et avec quels types d'équipement. Ainsi, la surface d'attaque et le nombre de violations possibles seront considérablement réduits et l'impact des problèmes liés à l'accès à distance peut être considérablement réduit.

Cette nouvelle réalité dessine une nouvelle approche dans le monde de la cybersécurité, dans laquelle le travail à distance sera beaucoup plus présent dans les entreprises, le nombre d'appareils mobiles qui ont accès au réseau d'entreprise continuera à augmenter de manière exponentielle et cela ouvre la porte à des fichiers malveillants capables d'infect.