Travail hybride : nouvel enjeu de la cybersÃ©curitÃ©
Internet
PostÃ© par : JulieM
PubliÃ©e le : 22/9/2021 13:00:00

Selon une enquÃªte rÃ©cente de Teknowlogy pour 3DS OUTSCALE, 56 % des entreprises ont perÃ§u une nette recrudescence des attaques. Le tÃ©lÃ©travail a en effet changÃ© les normes des collaborateurs Ã travers le monde entier, et il est plus aisÃ© dâ□□infiltrer un rÃ©seau professionnel via un tÃ©lÃ©travailleur mal protÃ©gÃ© contre les cybermenaces.

Il devient urgent pour les entreprises dâ□□adapter en consÃ©quence leur stratÃ©gie et pratiques de cybersÃ©curitÃ© pour mettre un terme Ã la recrudescence des attaques.

Selon Pierre-Louis Lussan, Country manager France & Directeur South-West Europe Netwrix, si le travail hybride offre davantage dâ□□opportunitÃ©s, tant pour les employÃ©s, qui peuvent travailler dâ□□oÃ¹ ils le souhaitent, que pour les employeurs, qui parviennent Ã rÃ©aliser des Ã©conomies en rÃ©duisant la surface des bureaux ; ce changement n'est pas sans risque.

Â« Les considÃ©rations clÃ©s se rÃ©sument Ã l'engagement et Ã la sÃ©curitÃ©. Bien que cela soit plus difficile, il est Ã la fois possible et important de favoriser des relations saines et une bonne communication au sein de l'Ã©quipe.

Cela peut passer par la crÃ©ation dâ□□un environnement de soutien et de collaboration pour que les employÃ©s aient toujours le sentiment de faire partie d'une Ã©quipe. Sans efforts dans ces domaines, de nombreux employÃ©s se sentiront dÃ©sengagÃ©s, ce qui entraÃ®nera sans aucun doute une augmentation des dÃ©parts et une baisse de la productivitÃ©.

Les contrÃ´les et les rÃ¨gles de sÃ©curitÃ© dÃ©ployÃ©s sont Ã©galement cruciaux pour la viabilitÃ© et le succÃ¨s Ã long terme de l'entreprise qui adopte le travail hybride.

Ce dernier impacte fortement le volume des attaques, telles que le phishing, en raison des vulnÃ©rabilitÃ©s accrues liÃ©es au travail Ã domicile : les distractions, le manque de soutien des Ã©quipes IT, ou encore des appareils non sÃ©curisÃ©s. Il est important de comprendre quelles sont les brÃ¨ches potentielles des contrÃ´les existants, et quels sont ceux qui ne fonctionnent tout simplement pas pour le travail hybride.

Pour ce faire, il est important de procÃ©der Ã des mises Ã jour rÃ©guliÃ¨res des rÃ¨gles de sÃ©curitÃ©, et de s'assurer que les collaborateurs suivent l'Ã©volution de l'entreprise et, surtout, quâ□□ils respectent les politiques de confidentialitÃ© et de sÃ©curitÃ© en place. Ces mesures permettent en effet de dresser une premiÃ¨re barriÃ¨re contre les cybercriminels qui sâ□□infiltrent dans le rÃ©seau de lâ□□entreprise par lâ□□espace numÃ©rique des employÃ©s non protÃ©gÃ©s.

De nombreuses considÃ©rations techniques sont les mÃªmes dans le cadre du travail hybride : systÃ¨mes de correction, formation des employÃ©s, couverture antivirus/malware cohÃ©rente, politiques de sauvegarde.

Elles sont cependant plus importantes que jamais, car les cybercriminels tirent profit de la moindre vulnÃ©rabilitÃ©, et les brÃ¨ches sont lÃ©gion depuis le dÃ©but de la pandÃ©mie du fait dâ□□une adoption du tÃ©lÃ©travail rapide et dâ□□une non mise Ã jour des politiques de sÃ©curitÃ© en parallÃ¨le. Â»