Renforcer la sécurité IT des espaces de travail

L'utilisation croissante du digital associée à la profonde modification des espaces de travail nous amène à faire face à un réel challenge pour sécuriser nos processus de travail au quotidien. Dans ce contexte, un point clé ne doit pas être écarté au profit d'une seule sécurisation de sujets à la mode comme le cloud. Il s'agit plus précisément de prendre en compte le sujet de la protection des accès liés aux périphériques amovibles. En effet, encore largement utilisés pour stocker et partager des informations, ces systèmes peuvent représenter une réelle menace et impacter la sécurité de tout le Système d'Information faute d'être pris en compte dans la gouvernance cyber.L'usage des supports amovibles est même renforcé en cette période de crise sanitaire dans différents cas d'usage car même si nombre de collaborateurs sont aujourd'hui en télétravail force est de constater que l'échanges de données par supports amovibles ne s'est pas tari (informations sensibles, mises à jours critiques…).

Alors, comment faire ?

Sur ce point, il convient de cartographier les spécificités de chaque organisation et de déployer en plusieurs points clés des dispositifs simples et éprouvés. Ces derniers permettront de s'assurer que les périphériques utilisés par les collaborateurs, partenaires, intervenants externes ou autres sont réellement de confiance et qu'ils ne contiennent pas de programmes malveillants qui pourraient être lancés lors de la connexion du périphérique à une station de travail, à un serveur ou à un équipement de l'entreprise.

Prendre en compte la notion d'expérience utilisateur

Plus que tout autre sujet, la notion d'expérience utilisateur doit être le point clé qui permettra à chacun de se positionner en acteur actif de la cybersécurité. Ainsi, il est fondamental de mettre en place des systèmes attractifs, simples et non contraignants permettant de contrôler que les supports amovibles utilisés sont réellement de confiance. On comprend donc que le rôle des stations blanches est stratégique.

En ce sens, un premier travail consiste à identifier les zones de risques et à y déployer des dispositifs en « libre-service » où les utilisateurs internes et externes pourront connecter les clés USB et autres supports amovibles. Imaginons l'accès à des salles de réunion, les couloirs, les guichets d'accueil… Autant de lieux qui sont à définir précisément avant de mettre en place tel ou tel dispositif. Une fois les différents endroits identifiés, il faudra ensuite raisonner sur le format des bornes à déployer : Stations, Totems, dispositifs plus compacts… Tout dépendra des usages et de la configuration des lieux.

L'espace de travail en mutation que nous connaissons va donc continuer sa mue pour offrir une réponse pertinente aux nouvelles attentes exprimées par les collaborateurs. En ce sens, il est fondamental que ces environnements de travail soient conçus dans une logique globale qui intègre les différentes composantes du volet cybersécurité. Sur ce point, la sécurisation des périphériques amovibles se positionne comme un must have.

Par Christophe BOUREL, CEO de Kub Cleaner