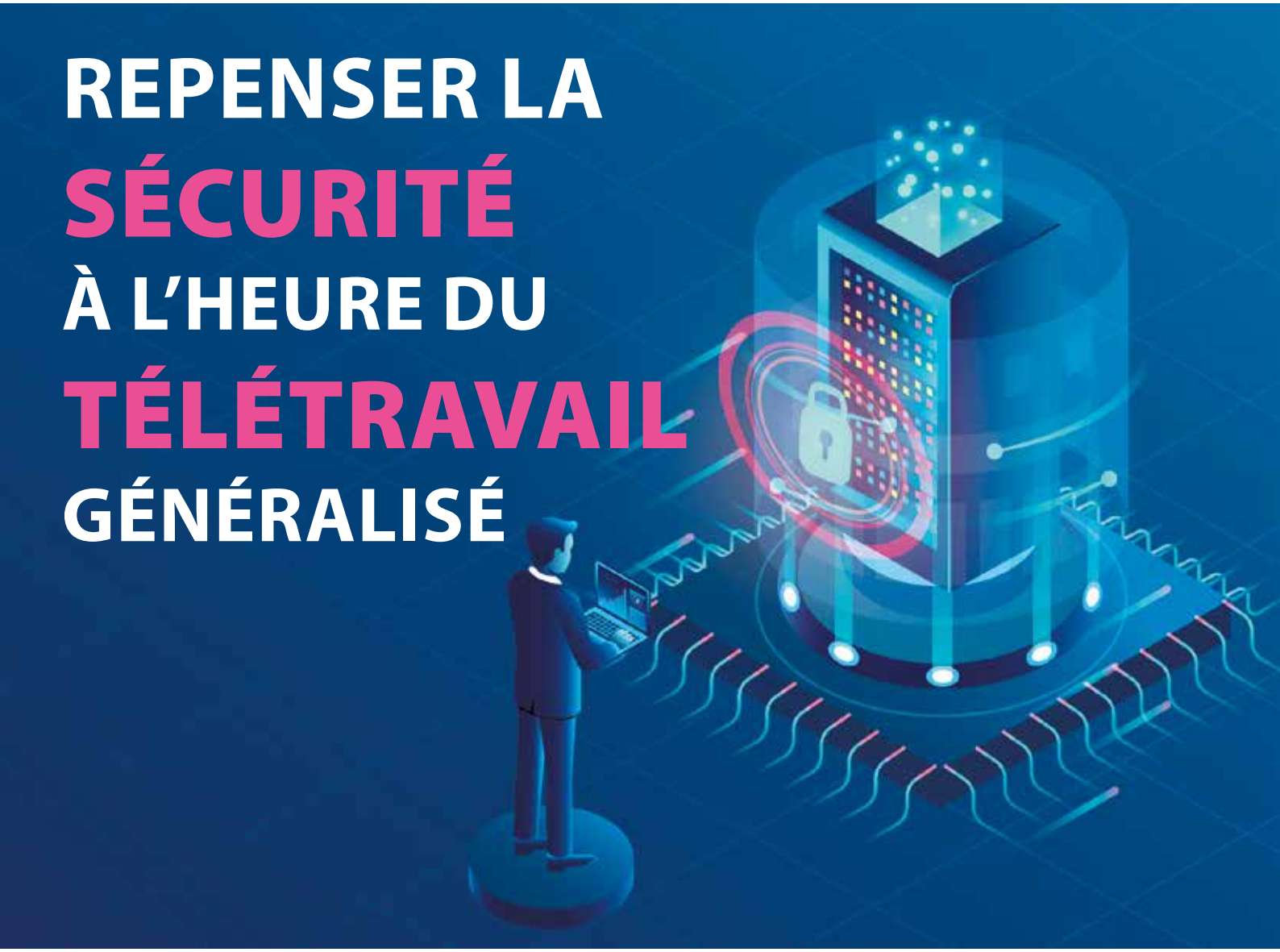
REPENSER LA SÉCURITÉ À L'HEURE DU TÉLÉTRAVAIL GÉNÉRALISÉ



Le développement du travail à distance suppose de revoir les modèles traditionnels de protection. Cela passe autant par de nouvelles parades techniques que par des changements organisationnels.

Opportunistes, les cybercriminels profitent à, chaque crise, de la faiblesse passagère de leurs proies. La pandémie de la Covid-19 n'échappe pas à la règle. Avec le recours généralisé au télétravail, les entreprises ont ouvert davantage leur système d'information afin d'accueillir un grand nombre d'accès distants.

En dépit des précautions prises – VPN, virtualisation du poste de travail – elles ont mécaniquement élargi leur surface d'exposition aux risques.

De leur côté, les télétravailleurs ne disposent pas à leur domicile du même niveau de protection qu'abrités derrière le pare-feu de leur entreprise. Isolés, les salariés sont aussi plus vulnérables aux compagnes d'hameçonnage et de malwares d'autant que les hackers ont su les personnaliser. Trend Micro a ainsi bloqué 8,8 millions de menaces se référant au Covid-19 au cours du premier semestre 2020.

Aussi, pour faire face à tous ces changements et évolutions, DIB-France vous recommande 5 axes à ne pas négliger.

1 Encadrer le BYOD

La menace est d'autant plus grande que, selon une récente étude de Trend Micro, un peu plus d'un tiers des télétravailleurs français (38%) utilisent leur propre équipement. Des smartphones, tablettes et autres ordinateurs personnels dont le niveau de protection est disparate en termes de patching ou de mise à jour du système d'exploitation et qui sont autant de portes d'entrée vers le réseau d'entreprise.

A défaut d'enrayer ce phénomène du BYOD (Bring Your Own Device), la DSI peut le limiter en privilégiant, lors du renouvellement de son parc informatique, l'acquisition d'ordinateurs portables utilisables au bureau comme au domicile.

Elle peut ensuite sécuriser une flotte de terminaux mobiles en passant par une solution d'EMM (Enterprise Mobility Management). Celle-ci comprend différents modules : le MDM (Mobile Device Management) prend en charge la partie hardware, le MAM (Mobile Application Management) gère les applications installées et le MCM (Mobile Content Management) contrôle l'accès aux données sensibles.

2 Sensibiliser les collaborateurs

La période est propice pour rappeler aux utilisateurs les règles élémentaires de sécurité comme choisir un mot de passe robuste et en changer régulièrement ou ne pas transférer de fichiers sur une clé USB. Une approche plus ludique à base de mises en situation, de vidéos, de quizz ou de serious games offre un surplus d'engagement.

Une simulation de cyberattaque permet, elle, d'évaluer le pourcentage d'utilisateurs qui, sans information préalable, se sont laissé piéger par une fausse campagne de phishing à base d'e-mail avec pièce jointe infectée ou de lien invitant à saisir ses identifiants en ligne. Le message auprès de ces salariés peu vigilants passera d'autant mieux.

La campagne doit être aussi personnalisée afin de répondre aux menaces spécifiques du télétravail comme le phishing sur mobile ou l'installation d'applications grand public sur un terminal à usage professionnel.

Un guide des bonnes pratiques du télétravail rappellera comment paramétrer correctement la sécurité d'un réseau wifi domestique ou une solution de visioconférence.

3 Faire la chasse au shadow IT

Basculant du jour au lendemain dans le travail à distance, les équipes métiers ont recouru à un ensemble hétérogène de solutions de collaboration à distance pour poursuivre leur activité. Certaines, grand public et/ou gratuites, n'offraient pas toutes les garanties de sécurité attendues.

Si elle a pu les fermer les yeux faute de mieux, la DSI doit aujourd'hui imposer les outils qu'elle a référencés en communiquant sur leur existence. Des tutoriels vidéo ou des guides d'utilisation peuvent faciliter leur appropriation.

Il s'agit aussi de cartographier les applications installées sous le radar de la DSI, d'évaluer leur criticité puis d'engager un dialogue avec les utilisateurs afin d'envisager des solutions alternatives plus sécures.

4 Repenser la gouvernance de l'information

La collaboration à distance suppose un échange permanent d'informations entre collègues, pour certains en télétravail, d'autres basés en entreprise. Ce mode d'organisation d'hybride suppose de repenser le circuit d'information, l'utilisation massive de tunnels VPN ayant montré ses limites.

Le confinement a aussi mis en évidence de mauvaises pratiques. Des télétravailleurs ont stocké des fichiers sensibles en local puis les ont partagés en pièces jointes dans leurs courriels, à partir de leurs espaces personnels de stockage en ligne ou directement depuis les plateformes de visioconférence.

Autant de méthodes qui ne garantissent pas le contrôle des accès ou le chiffrement des données.

L'entreprise doit aujourd'hui rappeler quels sont les outils de collaboration à distance référencés par la DSI et quel canal - chat, mail, visioconférence… - utiliser pour quel usage. Le concept de digital workplace qui réunit dans un espace unifié et sécurisé l'ensemble de ces briques est à privilégier.

5 Changer d'approche en matière de cybersécurité

Avec la généralisation de la collaboration à distance, le modèle de sécurité périmétrique dit du château fort où l'entreprise se retranche derrière ses murs, vole en éclats. La dissémination de l'information à la fois dans le cloud et dans les terminaux physiques invite à repenser différemment la sécurisation et l'accès au réseau et aux applications.

Comme son nom l'indique, le concept de « Zero Trust » consiste à exercer un contrôle strict et continu de l'utilisateur. Toujours dans le domaine de la gestion des identités se pose la question de l'authentification multifacteurs. Soit un mot de passe couplé à un SMS à usage unique, une carte à puce ou une clé cryptographique.

Enfin, la « cloudification » du SI incite à recourir à une solution de CASB (Cloud Access Security Broker) qui permet à une entreprise d'étendre sa politique de sécurité aux services cloud.