Télétravail et cybersécurité : comment gérer les risques

Depuis le début de la pandémie, les entreprises font face à de nouvelles cybermenaces du fait de l'adoption du travail à distance. Or, selon une étude menée par Bodet Software, 93% des télétravailleurs souhaiteraient prolonger la pratique du télétravail après la crise, au moins de manière occasionnelle. Les organisations doivent donc mesurer l'importance de la gestion des risques liés aux environnements de travail hybrides, en particulier vis-à-vis des fournisseurs et sous-traitants.

Impact du COVID-19 sur l'entreprise

L'obligation de télétravailler en mars 2020 a pris de court une majorité d'organisations, qui n'étaient pas habituées ou préparées à ce format. Ainsi, des industries entières ont dû adopter le cloud pour centraliser les informations et créer un flux de travail plus modulaire. En outre, les technologies basées sur le cloud favorisent naturellement un télétravail plus efficace, facilitant la connexion et la collaboration entre les employés. Ce déploiement s'est cependant accompagné de l'octroi d'accès à distance, pour des ressources parfois très sensibles ; telles que des données à caractères personnelles, de la propriété intellectuelle, ou encore des informations financières. Si ces actifs sont critiques pour le maintien des opérations d'une entreprise, il s'agit aussi de cibles privilégiées pour les cybercriminels, car ils peuvent les vendre à un bon prix à des concurrents ou à d'autres hackers, ou même les utiliser lors de futures campagnes malveillantes.

Les accès distants à ces données doivent par conséquent être sécurisés et étroitement surveillés. Sans compter que ces ressources ne sont pas seulement utilisées par les équipes internes, mais aussi par des fournisseurs, dont les stratégies de cybersécurité peuvent être différentes. Or, selon nos recherches, seulement deux entreprises sur cinq (42 %) ont mis en place des méthodes d'authentification forte pour gérer les accès à distance de leurs employés et tiers en 2020. Si le télétravail a pu sembler temporaire à l'époque, ce modèle s'est pourtant installé de manière plus durable. Et malgré un retour en présentiel autorisé depuis le 9 juin en France, de nombreuses entreprises ont prévu de proposer des formats hybrides et plus flexibles, entre présentiel et distanciel, à la demande de leurs équipes.

Télétravail et cyber-risques inhérents

Plus le nombre de processus opérés à distance augmente, plus il est important de mettre en place des garanties pour protéger les informations qui circulent entre serveurs et points d'accès. Mais nos recherches révèlent que seulement 26 % des entreprises ont mis en place des procédures pour garantir que seuls les appareils autorisés puissent se connecter à leurs réseaux internes. Cela signifie que plus de 70 % des entreprises ne disposaient d'aucune procédure pour contrôler les appareils accédant aux réseaux de l'entreprise. En outre, seules 15 % des organisations ont mis en place un processus de contrôle sur les appareils des télétravailleurs avant de les autoriser à se connecter à leurs réseaux. La majorité des entreprises ne contrôlent donc pas les risques que présente un accès non surveillé au réseau.

Selon l'ANSSI, il y a eu trois fois plus de piratages en France en 2020 que l'année précédente. En effet, les cybercriminels tirent parti de la confusion, des changements de processus et des nouvelles formes de communication pour exploiter les vulnérabilités des organisations. Les attaques peuvent

prendre diverses formes ; les plus nombreuses en 2020 étant les tentatives de phishing, les ransomwares et les attaques de déni de service distribué (DDoS).

Afin de faire face à ces menaces, les entreprises doivent donc veiller à la formation régulière de leur personnel aux politiques et processus de cybersécurité à mettre en place. L'adoption de services et systèmes basés sur le cloud oblige les entreprises à s'assurer également que les fournisseurs de ces technologies respectent leurs propres normes de cybersécurité, disposent d'une architecture IT sécurisée, d'un plan de réponse à incidents, ou encore, chiffrent les données sensibles. Seulement, malgré la hausse des attaques, notre étude dévoile que seules 25 % des organisations évaluent sérieusement le cyber-risque présenté par leurs fournisseurs.

Modifier le processus de gestion des risques

Une des premières mesures à déployer est la sécurisation des accès distants ; et ce pour les employés, mais aussi pour les fournisseurs et partenaires. En parallèle, les appareils non autorisés ne doivent en aucun cas pouvoir se connecter aux réseaux internes, et l'activité sur les réseaux est à surveiller étroitement afin de repérer rapidement toute activité suspecte. En outre, quelle que soit la stratégie de cybersécurité qu'une entreprise décide de déployer, elle doit viser à contrôler que sa supply chain déploie les mêmes exigences. Pour ce faire, des questionnaires déclaratifs ne sont pas suffisants car ils ne donnent pas un niveau de confiance suffisant. Il faut donc y préférer des audits plus avancés, pour lesquels les parties tierces doivent justifier leur cyber-hygiène via des documents et preuves concrètes. Si des vulnérabilités sont alors notées, il est possible de proposer un plan d'amélioration avec des dates butoirs, dans l'objectif d'accompagner et de réévaluer ultérieurement la cybersécurité de cette organisation.

Alors que les environnements de travail hybrides deviennent la norme, il devient urgent pour les entreprises de prendre en compte le risque cyber, et en particulier celui lié aux fournisseurs et partenaires. En effet, les cybercriminels ont bien conscience que la meilleure porte d'entrée vers leur cible se fait via ses parties tierces, dont le niveau de cybersécurité est encore trop rarement évalué. La stratégie d'une organisation pour faire face aux menaces actuelles doit donc se montrer davantage holistique, afin de prendre en compte tout l'écosystème dans lequel elle évolue, pour se protéger de manière optimale.