Faire face à la nouvelle normalité en protégeant convenablement vos données

2020 est définitivement une année bien étrange. Même si un « retour à la normal » - et au bureau - est souhaité par les entreprises, le rebond de la pandémie de coronavirus demande à nouveau aux entreprises d'être flexibles et de s'adapter. Ce contexte génère de nouvelles préoccupations et de nouvelles problématiques pour les équipes IT auxquelles il est indispensable de trouver des solutions.

Parmi les principaux défis figurent la sécurité des dispositifs face aux logiciels malveillants ou encore la réévaluation des systèmes et processus de sécurité déjà en place. Ces derniers étaient peut-être jugés adaptés avant la pandémie, mais la multiplication des attaques par ransomwares (dont les dernières en date contre Tesla ou encore Orange Business Services) a changé la donne. Les entreprises de toutes tailles et secteurs doivent s'assurer que leurs systèmes, au lieu d'être seulement "suffisamment efficaces", soit totalement résistants et résilients à ce type d'attaque.

Le retour d'un vieil ennemi

Pour les entreprises, la menace d'une cyberattaque est une inquiétude du quotidien. Cependant, avec la démocratisation du télétravail et l'utilisation de nouveaux outils, la cybersécurité est devenue, plus que jamais, un enjeu majeur pour les entreprises. Des entreprises comme Honda et EasyJet ont dues faire face au raz de marée provoqué par de récentes attaques, et ce, alors qu'elles essayaient en parallèle de se maintenir à flot dans un contexte économique difficile. Mais, en matière de risques informatiques, cette période de télétravail n'aura été que la face émergée de l'iceberg, et d'autres vagues d'attaques pourraient suivre.

Si certains employés ont pu retourner au bureau, la possibilité qu'ils aient ramené des dispositifs infectés est un risque à prendre en compte. En effet, une fois que ces dispositifs sont sur le réseau de l'entreprise (et donc derrière le pare-feu), les logiciels malveillants latents peuvent rapidement se propager et causer des dommages considérables pendant une période de récupération critique. De nombreux services IT sont d'ores et déjà dépassés par les évènements, notamment parce qu'ils doivent prendre en charge une nouvelle façon de travailler, beaucoup plus flexible. Si on ajoute à cela un nombre de menaces et de dispositifs grandissant, le contexte pourrait sembler parfait pour la propagation des ransomwares.

La nécessité d'un plan de secours solide

Que ce soit d'un point de vue juridique, financier ou lié à la réputation, le vol des données clients peut avoir de graves conséquences sur les entreprises. L'exemple de Garmin est d'ailleurs assez parlant : l'entreprise a dû payer une rançon de plusieurs millions de dollars pour récupérer ses données après avoir été victime d'une attaque par ransomware en juillet 2020. Pour les entreprises qui cherchent à atténuer ces risques, une solution de sauvegarde des données efficace peut contribuer à éviter la perte de données.

Les attaques par ransomware reposent en grande partie sur le fait que les entreprises ne sont pas en mesure de restaurer les données qui ont été cryptées par les hackers. Ils utilisent cette technique pour s'assurer d'avoir un moyen de pression pour extorquer d'importantes rançons en échange de la

clé de cryptage. Cependant, si les entreprises disposent d'une autre copie fiable des données, stockée en sécurité et en dehors du réseau, les hackers perdent leur moyen de pression.

Grâce à la mise en place d'une solution de sauvegarde des données efficace, les entreprises victimes d'une attaque par ransomware seront en mesure de reprendre leurs activités rapidement et sans avoir à interagir avec les hackers. En effet, elles pourront tout simplement restaurer les données à partir des sauvegardes stockées sur site et dans le cloud dès lors que l'attaque aura été détecté.

Lorsqu'il s'agit de mettre en oeuvre une stratégie efficace de sauvegarde des données, la règle du "3-2-1" s'avère être une bonne méthode. L'entreprise doit avoir 3 copies de ses données : deux d'entre elles doivent être stockées sur différents supports et la troisième en dehors du réseau. Comme les attaques se concentrent généralement sur les serveurs de sauvegarde basés sur site, la nécessité d'isoler physiquement une copie des données de sauvegarde du réseau (connue sous le nom de "air-gapping") s'avère aujourd'hui primordial.

En fin de compte, si les entreprises admettent que le « jamais » n'existe pas en matière de violation de données, le fait d'y être préparé est non seulement intelligent mais rentable.

S'adapter à une nouvelle réalité

Alors que les employés oscillent entre télétravail et journées au bureau, se préparer à d'éventuelles attaques par ransomwares est une priorité, certes, mais de nombreux autres efforts sont également déployés par les équipes IT pour adapter le système aux nouvelles conditions et méthodes de travail liées à la crise du COVID-19.

Beaucoup d'entreprises ont réussi à mettre en place, au pied levé, un dispositif permettant aux employés de travailler depuis chez eux. Toutefois, dans de nombreux cas, cette rapidité d'exécution répond au caractère urgent de la situation plutôt qu'à l'objectif de mettre en place un dispositif préparé en amont. Certains processus (audits, appels d'offres, formation) dont la mise en place aurait nécessité des mois, ont été condensés et déployés en une semaine. De plus, les déploiements technologiques qui auraient pu être confiés à des spécialistes ont souvent dû être mis en place par des talents internes. Par conséquent, les entreprises, pour pouvoir continuer à travailler à distance, ont accepté le compromis d'entrainer des risques à court terme.

Les systèmes et les processus passant d'un statut temporaire à permanent, il devient nécessaire de les réexaminer et de les réviser, et cela n'est pas aussi facile qu'il n'y parait. En fin de compte, il existe de multiples dispositifs, applications et, dans certains cas, systèmes d'exploitation, qui évoluent hors du réseau de l'entreprise et ce, depuis plusieurs mois maintenant. Rien ne garantit que ces appareils aient été utilisés uniquement pour le travail, certains outils comme zoom ayant été mis à profit dans un contexte plus personnel notamment pendant la période de confinement.

Il n'a jamais été aussi important d'avoir une visibilité complète sur l'infrastructure et les environnements de données de l'entreprise. On ne saurait trop insister sur les dangers que courent les entreprises qui ne prennent pas de précautions. Il est important de s'assurer que les données ne restent pas cloisonnées, non classées et non surveillées dans divers environnements (cloud, sur site etc.). Au contraire, elles doivent être accessibles aux employés à partir d'une plateforme connectée supportée par les logiciels de sécurité les plus récents et les plus performants. Ainsi, les entreprises deviennent plus efficaces face aux ransomwares, tant sur le plan préventif que réactif. Une surveillance régulière, voire constante, des données sensibles, qui sont les plus exposées au risque de cryptage, améliorera également la capacité des entreprises à réagir.

De nos jours, les attaques par ransomwares sont inévitables. Les entreprises devraient certainement

mettre en place des mesures de sécurité strictes pour s'en protéger, mais de bons processus de détection pour repérer les attaques, couplés à une solution de protection des données solides, sont tout aussi importants pour pouvoir réagir efficacement. Il n'y a aucune excuse pour ne pas être préparé alors que vous avez déjà été prévenu.