Battez-vous pour vos données

La lutte pour tenter de remporter les données des entreprises va commencer. À gauche, le ransomware, qui a coûté aux entreprises près de 20 milliards de dollars l'année dernière, se prépare à attaquer les data centers. À l'autre extrémité, le spectre de l'erreur humaine, souvent sous-estimé, fait son retour en force. Qui va porter le coup fatal qui pourrait mettre l'entreprise au tapis ?

Tout dirigeant espère qu'aucun de ces deux problèmes n'enverra son organisation dans les cordes. En réalité, tous deux représentent une menace majeure pour l'intégrité des données et la continuité des activités. Cependant, alors que les risques liés au ransomware commencent heureusement à être pris plus au sérieux, les entreprises accordent rarement la même attention et le même soin à prévenir l'erreur humaine.

Ransomware VS erreur humaine : lequel est le plus risqué ?

Selon une récente étude, une entreprise aurait en moyenne déjà subi 1,87 attaque par ransomware en France. Le risque est donc réel et s'intensifie car la fréquence des attaques par ransomware aurait augmenté de près 255% en 2020. Les attaques sont de plus en plus sophistiquées et les hackers s'organisent pour cibler certains types d'entreprises ou de données de grande valeur. En plus des techniques habituelles, les hackers trouvent également de nouveaux moyens de faire pression sur leurs victimes pour qu'elles paient, en paralysant par exemple l'intégralité des systèmes informatiques ou en menaçant de divulguer les données sensibles volées. En France, les entreprises sont malheureusement bonnes payeuses : 63% des entreprises ont déjà payé partiellement ou intégralement une rançon.

Beaucoup pourraient penser que les hackers qui utilisent des ransomwares ont gagné le combat. Cependant, l'erreur humaine reste la cause la plus fréquente de perte de données. L'être humain n'est tout simplement pas infaillible et aucun utilisateur ne peut se prétendre à l'abri d'une erreur de manipulation d'autant plus dans un contexte où le télétravail est beaucoup plus répandu qu'il y a quelques mois. Même si les entreprises forment l'ensemble de leur personnel au respect des politiques relatives aux données, celles-ci ne seront respectées, finalement, que par une faible proportion des collaborateurs. De plus, les partenaires, sous-traitants, ainsi que l'ensemble des tiers intervenant sur la chaîne d'approvisionnement font également peser une menace sur la conformité des données.

Alors, l'intérêt grandissant et la démocratisation de l'utilisation des ransomwares par les hackers, l'erreur humaine reste la raison première de la compromission des données d'entreprises.

Quelles sont les leçons à tirer ?

Si les motivations et les circonstances derrière ces deux types de menaces diffèrent fortement, les solutions à mettre en place peuvent tout de même présenter des similarités. Voici donc cinq enseignements à prendre en compte pour préserver vos données des ransomwares et des erreurs humaines :

1. Partir du principe que les violations de données sont inévitables

Les entreprises ont bien compris qu'essayer de protéger le périmètre de leur réseau contre une attaque entrante par ransomware revient à essayer de combler les trous d'une passoire : finalement, il y aura toujours un risque de fuite. C'est pourquoi il leur est nécessaire de prévoir le pire des scénarios afin d'être prêt à réagir dans n'importe quelle situation.

2. Trois sauvegardes valent mieux qu'une

Si vous n'avez qu'une seule copie de vos données et qu'elles vous sont confisquées par un ransomware, vos chances de les récupérer sont très limitées. Il en va de même si une donnée unique est accidentellement supprimée ou écrasée. En revanche, vos chances de restaurer ces données sont d'autant plus grandes si vous disposez d'une copie de sauvegarde. Deux copies valent mieux qu'une et l'idéal est de prévoir trois copies dont l'une est stockée hors ligne et donc inatteignable.

3. Garder un oeil sur vos données

Surveiller leurs données permet aux entreprises d'être en mesure de détecter toute modification importante des fichiers, de repérer rapidement une attaque par ransomware et de réagir suffisamment tôt. Cette surveillance peut également aider à identifier si des fichiers ont été supprimés accidentellement. De manière générale, des moyens permettant de remédier à un incident existent, et le fait de repérer rapidement les changements sera avantageux pour les entreprises.

4. La formation, la communication et la confiance des employés sont essentielles

En raison de la sophistication des méthodes de phishing, les employés peuvent facilement devenir le point d'entrée des hackers qui utilisent des ransomwares. C'est pourquoi, beaucoup d'entreprises forment l'ensemble du personnel sur la meilleure façon de réagir : elles encouragent les collaborateurs à se manifester s'ils pensent être à l'origine d'une violation de données tout en insistant sur le fait qu'ils ne seront pas pénalisés. Cette méthode n'est que peu mise en place au sein des entreprises. Pourtant, elle aiderait les entreprises à identifier les problèmes, à surveiller les risques et à agir en conséquence.

5. Les données de sauvegarde sont aussi vulnérables que les autres données

S'il n'est pas repéré à temps, un ransomware peut facilement finir par atteindre les données de sauvegarde. De même, les erreurs commises lors des sauvegardes des données peuvent avoir des répercussions sur les sauvegardes. Il est alors essentiel de mettre en place les politiques et les technologies adéquates pour s'assurer que les données de sauvegarde sont disponibles à tout moment.

Qui l'emporte ?

Finalement, qui est le plus susceptible de mettre à mal une entreprise : le ransomware ou l'erreur humaine ? La réalité est qu'ils s'attaquent tous deux aux données et qu'il est presque impossible de ne pas être frappé par les deux. Selon la loi des probabilités, l'erreur humaine survient plus fréquemment, mais un ransomware finit aussi par survenir, et tous deux sont dévastateurs. Les entreprises doivent être prêtes à protéger et à détecter toute menace pouvant peser sur leurs données, quelle qu'elle soit, puis à réagir et à récupérer leurs données. Celles qui se battent intelligemment se préparent contre ces deux menaces.