Ransomwares : compliquer et ralentir leur progression grâce à la visibilité

Selon le rapport d'activité publié par la plateforme française d'assistance et de prévention en sécurité numérique, Cybermalveillance, en 2021 les demandes d'assistance contre la menace ransomware ont connu une hausse de 95 % en 2021 en France avec 1 633 demandes émanant des entreprises. Ce type d'attaque se classe une nouvelle fois en tête des principales cybermenaces qui visent les organisations ; il s'agit de l'une des plus lucratives, avec une progression attendue en 2022.

L'omniprésence et la recrudescence des ransomwares ont poussé les entreprises à repenser leur approche de la sécurité au cours des dernières années. Elles ne peuvent plus se permettre de zones d'ombres dans leurs systèmes. Elles doivent à présent envisager les vecteurs d'attaque de manière globale. Bénéficier d'une visibilité claire sur leurs actifs et d'une connaissance absolue de leurs faiblesses, afin d'être en mesure de garder une longueur d'avance qui est devenu incontournable.

La lutte contre les ransomwares évolue continuellement avec les utilisateurs et leurs pratiques. Dans des environnements de plus en plus complexes, aucun système n'est aujourd'hui capable de bloquer les ransomwares. Tout comme pour l'antivol d'un deux roues, le but est de compliquer et ralentir au maximum la progression de l'attaquant pour limiter les dégâts et protéger ainsi les actifs de l'entreprise.

Penser comme un attaquant, anticiper la menace

L'usage hybride des terminaux mêlant autant d'activités professionnelles que personnelles, combiné au fait que les données sont désormais majoritairement hébergées dans le cloud, constitue un facteur de risque important pour les entreprises. Or, trop nombreuses sont encore celles qui estiment que si leur cloud public est chiffré, elles sont protégées, et n'accordent pas suffisamment d'attention aux risques qu'elles encourent.

En outre, elles comptent sur les équipes IT pour rétablir tous les fichiers à une version antérieure, et ce, sans conséquences sur l'activité. Si c'est le cas parfois, ce n'est cependant pas une généralité : les pertes peuvent être bien plus importantes qu'escompté et avoir un impact financier non négligeable.

C'est pourquoi une approche proactive est indispensable pour faire face à une potentielle attaque. L'anticipation des risques permet de mettre en place des plans de prévention et de récupération avant même que l'attaque n'ait eu lieu. On dit depuis longtemps que la question n'est pas « si » mais « quand » une entreprise sera attaquée, et il est plus que jamais nécessaire de se mettre à la place de l'attaquant pour parer à toute éventualité.

En cas d'attaque ransomware, il suffit en effet parfois d'un clic de la part d'un utilisateur pour que tout le réseau s'arrête : par exemple, si 10 % des employés d'une entreprise de 1 500 personnes

cliquent sur un lien malveillant, cela représente 150 chances pour un attaquant de pénétrer dans le réseau et de mener sa mission à bien !

Or, au-delà de la question du paiement de la rançon, les entreprises doivent être en mesure de restaurer leurs systèmes aussi rapidement que possible, que leurs données aient été chiffrées, perdues ou mises hors ligne à la suite d'un incident technique. Mais cela ne s'arrête pas là car une fois remises en ligne, il n'est pas exclu que l'attaquant ait également exfiltré des données sensibles ou privées – et que l'entreprise reste vulnérable. En d'autres termes, se préparer au pire aide à limiter les dégâts en cas d'attaque.

Evolution vers des systèmes de récupération basés sur le cloud

Le processus de rétablissement est l'un des parents pauvres de la sécurité, en ce sens qu'il s'agit souvent de la dernière chose à laquelle les équipes pensent lorsqu'elles élaborent une stratégie de sécurité. A tort.

La reprise après sinistre et la continuité des activités (DRBC) constituent probablement le problème le plus difficile à résoudre et, reste malheureusement souvent le plus ignoré. Or, pour une organisation dans le secteur de la santé ou un opérateur d'importance vitale (OIV), une infrastructure critique ou un système de contrôle

industriel (ICS) les interruptions de service peuvent entraîner des conséquences désastreuses. Dans certains cas, comme par exemple en santé, assurer la continuité des activités peut sauver des vies, ce qui requiert un délai de rétablissement immédiat.

Aujourd'hui, les solutions hébergées dans le cloud prennent des captures instantanées des données en temps réel. C'est la raison pour laquelle le stockage dans le cloud offre un DRBC beaucoup plus rapide que les solutions existantes, qui restent figées dans une logique de serveurs et d'appareils physiques. Pour garder une longueur d'avance sur les ransomwares, les entreprises doivent donc passer à la vitesse supérieure et adopter une stratégie DRBC de nouvelle génération basée sur le cloud.

Par ailleurs, l'une des principales raisons pour lesquelles de nombreuses organisations n'ont pas franchi cette étape cruciale tient au fait qu'elles s'inquiètent encore de la sécurité de ces environnements cloud ; ce que confirme la Cloud Security Alliance (CSA), dans sa dernière étude indiquant que la sécurité demeure une préoccupation majeure en matière d'adoption du cloud pour 58 % des personnes interrogées.

Cependant, cette crainte fait naître un autre type de risque. Cela peut notamment ralentir une reprise et impacter ainsi la continuité des opérations après une panne invalidante. Force est donc de constater, qu'à l'heure où le cloud peut offrir une meilleure visibilité et un contrôle renforcé des données que ne le feraient des serveurs en datacenter physique, les entreprises peuvent accélérer leur délai de rétablissement et améliorer leur temps de fonctionnement.

On ne peut pas sécuriser ce que l'on ne voit pas

Une stratégie de préparation aux attaques ransomwares consiste, in fine, à assurer une visibilité complète des données, afin de les classifier et de mettre en place des politiques destinées à garantir que les informations sensibles ne quittent jamais l'organisation. Cela permet aussi de bloquer l'entrée de fichiers qui les enfreignent (à l'instar de ransomwares stockés dans le cloud par exemple), en fonction de leur classification. Il est ainsi possible de conserver les bons éléments à l'intérieur et de laisser les mauvais à l'extérieur.

Actuellement, en cas d'attaque ransomware, le fichier infecté n'a plus besoin de pénétrer physiquement dans le réseau ; il suffit au cybercriminel de le distribuer en périphérie. Pour pallier ces nouvelles pratiques, une architecture SASE (Secure Access Service Edge) combinée à des capacités de prévention des pertes de données (DLP), permet de protéger les utilisateurs dans les environnements que les équipes IT maîtrisent et qui sont déployées dans l'entreprise.

Or, le problème se pose avec les outils et plateformes susceptibles d'être installés et utilisés en parallèle. Ce « shadow IT » échappe à l'attention et au contrôle des équipes informatiques, lesquelles ne peuvent pas pleinement protéger les systèmes de l'entreprise.

Cette situation s'est amplifiée depuis le début de la pandémie, avec la mobilité accrue, les politiques de BYOD, les applications SaaS et la recrudescence des télétravailleurs. Il est donc plus que jamais nécessaire d'avoir de la visibilité et des contrôles basés sur des politiques afin d'empêcher le téléchargement de fichiers malveillants sur tout appareil autorisé à recevoir les données des utilisateurs.

Par conséquent, étendre la visibilité de la sécurité au-delà des seules données pour disposer également d'une vue globale des utilisateurs, des dispositifs et des applications est plus que jamais indispensable. Plus les équipes en savent sur les environnements réseau étendus, mieux elles seront en mesure de protéger les utilisateurs, les appareils, les applications et les données contre les perturbations.

Il n'existe aujourd'hui aucun remède contre les attaques ransomware, aucune solution de sécurité capable de les stopper ; mais il existe des moyens de les anticiper, de les ralentir, voire de s'en prémunir avec une visibilité claire sur les actifs et les données, une compréhension de l'environnement et des mesures de prévention et d'anticipation pour qu'en cas d'attaques les conséquences soient les plus minimes possibles et offrir aux entreprises la possibilité de ne pas payer une rançon.