Les attaques de ransomware sont de plus en plus sophistiquées.

Votre entreprise peut-elle faire face à cette menace en toute sérénité ?

PRÉSENTATION

Les auteurs d'attaques de ransomware deviennent plus sophistiqués et ciblent de plus en plus d'entreprises en leur demandant des rançons toujours plus importantes. Ces attaques fortement perturbatrices peuvent entraîner l'arrêt des systèmes informatiques et opérationnels. Beaucoup d'entreprises découvrent que leur système de défense est insuffisant pour garder le contrôle lors de l'attaque d'un ransomware.

Comme CSO.com le remarque, « Les attaques de ransomware se sont développées avec les années en adoptant des techniques plus discrètes et sophistiquées, tout en corrigeant la plupart des problèmes de mise en œuvre de leurs précédentes tentatives ». En résumé, ces attaques ne sont pas vouées à disparaitre.

« Les auteurs de ransomwares ont développé leurs compétences et leurs attaques deviennent plus complexes, plus créatives et plus ciblées sur les entreprises », déclare Alex Restrepo, employé Veritas en marketing solutions.

Dans la mesure où les entreprises privées ne sont pas toujours légalement obligées de divulguer qu'elles ont été victimes d'un ransomware, l'impact de ces attaques sur ces entreprises est difficile à quantifier en terme de coût et de fréquence. Il est également difficile de savoir combien de victimes décident de payer la rançon, même si on peut affirmer que beaucoup le font, puisque les cybercriminels ont continué à investir dans la conception de formes avancées de ransomware.

HAUSSE DES PERTES DUES AUX RANSOMWARES

Dans une publication parue en octobre dernier, l'Internet Crime Complaint Center (IC3) du FBI alerte « Depuis le début de l'année 2018, la fréquence des campagnes de ransomware menées à large échelle et au hasard a énormément diminué. Cependant, les pertes dues à ces attaques ont largement augmenté, selon les plaintes reçues par l'IC3 et les information du FBI. »

> « Les auteurs de ransomwares ont développé leurs compétences et leurs attaques deviennent plus complexes, plus créatives et plus ciblées sur les entreprises. »
>
> ***— déclare Alex Restrepo, employé Veritas en marketing solutions***

Le cas le plus connu de ransomware est probablement l'attaque NotPetya, survenue en 2017. Le géant des transport Maersk a dû suspendre ses opérations dans 17 terminaux portuaires, ce qui a créé d'immenses files d'attentes de cargos destinés à être chargés et un cauchemar logistique qui a pris des mois à être réglé. Il a été estimé que l'incident a coûté plus de 10 milliard de dollars à l'entreprise.

Dans un rapport publié en août dernier sur l'évolution des ransomwares, l'entreprise de sécurité Malwarebytes indique que, « Cette menace dangereuse mais dernièrement en retrait est redevenue active de façon spectaculaire, passant de campagnes de consommateurs de masse à des attaques artisanales et hautement ciblées sur les entreprises ».

DÉVELOPPER UNE STRATÉGIE EFFICACE POUR PROTÉGER, DÉTECTER ET RÉCUPÉRER DES DONNÉES

De nombreuses entreprises ont investi dans des solutions de sécurité de pointe dont l'objectif est de prévenir les attaques de ransomware. Mais avec les constantes modifications et mises à jour des configurations système et des accès utilisateur, il est pratiquement impossible de maintenir une barrière impénétrable qui peux stopper 100 % des attaques.

Les criminels ont démontré leur persistance à constamment creuser dans les défenses pour identifier les faiblesses d'un système et ils se sont montrés aptes à trouver et chiffrer n'importe quelles données accessibles, y compris les fichiers de sauvegarde accessibles sur le réseau.

« Certaines entreprises pensent à tord que les ransomwares vont juste pirater leurs messages électroniques ou leurs documents, et elles supposent qu'elles pourront les récupérer simplement avec leurs sauvegardes », déclare Restrepo. « Mais les attaques de ransomware sont devenues extrêmement efficaces pour découvrir toutes les connections au sein des systèmes d'une entreprise, donc même si vos documents ne sont pas sauvegardés à un seul endroit, il n'y a aucune garantie qu'ils soient en sécurité ».

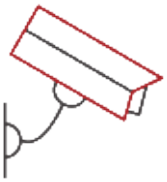
Comme le rapporte l'article de CSO.com, « Dans certains cas, les entreprises ont décidé ou ont étés forcées de payer la rançon car leurs sauvegardes ont été corrompues ou le processus de restauration aurait pris trop de temps ».

Même si les bonnes pratiques en matière de sauvegarde ont prouvé leur efficacité dans la récupération après une attaque de ransomware, elles ne sont qu'un élément d'une stratégie globale visant à protéger une entreprise contre une attaque de ransomware.

Lorsqu'on parle de ransomware, les entreprises peuvent prendre de nombreuses mesures préventives pour contenir la menace. Veritas conseille l'adoption d'une stratégie à trois niveaux :

1 PROTÉGER SES DONNÉES DE FAÇON ANTICIPÉE

En plus de disposer d'une solution de sécurité de pointe, la mise en œuvre de mesures de renforcement est essentielle pour protéger l'intégrité des données. Les démarches qui consistent à conserver plusieurs copies des données, notamment la sauvegarde de copies sur un stockage isolé et immuable, permettent de s'assurer que les sauvegardes fonctionneront lorsqu'on en a besoin.



2 MAINTENIR LA CONNAISSANCE DES DONNÉES ET DES INFRASTRUCTURES.

Les outils et processus de détection et de prévention des risques peuvent assurer une réponse appropriée en cas d'intrusion. Cela nécessite une visibilité de bout en bout au sein de l'infrastructure informatique avec des outils de surveillance et de rapport pour s'assurer que les données sont accessibles et gérées seulement par des partis de confiance et que les changements dans l'accès aux données et dans les données de références sont détectées et signalées.

3 GARANTIR UNE RÉCUPÉRATION RAPIDE ET EFFICACE

Un ransomware qui infecte et corrompt un appareil peut rapidement devenir incontrôlable et compromettre la totalité du datacenter en raison des infrastructures multicloud hybrides modernes. Un processus de récupération automatique et organisé est requis pour reprendre le contrôle après une attaque, idéalement complété par la possibilité d'effectuer des tests et répétitions.

La plateforme Veritas Enterprise Data Services fournit un ensemble complet de technologies qui soutiennent la protection des systèmes informatiques, la détection des activités anormales du système et certaines stratégies de récupération en cas d'attaque.

Pour plus d'informations sur comment garder le contrôle d'une entreprise lors d'une attaque de ransomware, rendez-vous sur www.veritas.com/ransomware.