Rançongiciel : 6 leçons à tirer de la pandémie pour prévenir les attaques

Alors que le paysage des cybermenaces est constitué de plusieurs types d'attaques, le rançongiciel est l'une des préoccupations majeures des RSSI. Il constitue même le scénario d'attaque informatique le plus redouté des RSSI.

Quoi de pire en effet qu'un incident de sécurité informatique d'envergure publique, qui porte atteinte à la capacité opérationnelle d'une entreprise ?

Une étude récente révélait que 18 % des entreprises françaises ayant répondu à l'enquête, ont été touchées par un rançongiciel et ont payé la rançon en 2020 ; compte tenu de l'ampleur potentielle de l'impact, c'est un chiffre terrifiant. En parallèle, la même étude démontre également que 25 % des entreprises françaises interrogées ont souffert d'une infection par rançongiciel à la suite d'une attaque de phishing réussie.

Si le rançongiciel est une attaque qui effraye le RSSI et l'ensemble de sa hiérarchie, particulièrement les risques liés au coût élevé de l'attaque, 98 % des entreprises qui ont payé la rançon sont parvenues à récupérer leurs données. Cette statistique n'était que de 78 % l'année précédente et suggère une montée en gamme des compétences des cyberattaquants.

En effet, plus la rançon est élevée, plus les lanceurs d'attaques auront de chances de voir leurs victimes payer la rançon avec en contrepartie la récupération des données.

La montée en gamme du niveau de sophistication des attaques a largement été démontrée lors d'une récente attaque qu'a subie une marque de mode. En effet, dans ce cas particulier, l'attaquant avait étudié les données dérobées dans le but de trouver des détails sur la politique de responsabilité et de sécurité informatique de l'entreprise.

L'attaquant aligne le montant de sa rançon avec celui qui est indiqué dans la politique de l'entreprise. C'est ainsi que l'attaquant peut négocier le montant de la rançon directement auprès de la victime déjà en position de faiblesse. Profitant de sa position de force, l'attaquant se base sur l'évaluation de la santé financière de sa proie avant de recevoir le paiement convenu.

Certains cybercriminels vont même jusqu'à pousser le niveau de professionnalisme en proposant un véritable accompagnement de crise aux clients contraints de payer une rançon. En effet, de nombreuses organisations parallèles proposent un niveau d'assistance technique fourni via des plateformes de messagerie instantanée anonymes pour aider les victimes à se rétablir une fois qu'elles ont payé. Et de manière assez ironique, les attaquants pensent à offrir de solides conseils pour sensibiliser les entreprises aux risques des attaques par rançongiciel. Aperçu de leurs conseils qui portaient notamment sur les points suivants :

1. Adopter le filtrage des e-mails

La mise en place du filtrage des e-mails est cruciale. Les statistiques montrent qu'environ 94 % des cyberattaques sont initiées par le biais de l'email, un véritable point d'entrée aux risques pour les entreprises. Bien que les attaques de rançongiciel ont pendant longtemps exploité les ports du protocole de bureau à distance (RDP), une récente étude montre que une augmentation des vagues d'attaques par rançongiciels distribués dans le cadre de campagnes d'email de phishing, ce qui contraste fortement avec les années précédentes, où les acteurs malveillants utilisaient principalement des téléchargeurs comme charge utile initiale.

2. Réaliser des tests d'intrusion et de phishing auprès des employés

Dans les scénarios des attaques distribuées par email, plus de 99 % d'entre elles exigent que l'utilisateur prenne des mesures pour que l'intrusion des attaquants aboutisse, qu'il s'agisse d'exécuter une macro, de communiquer des informations d'identification ou simplement de payer une fausse facture. Les employés contribuent à étendre la surface d'attaque de toute entreprise.

En effet, comme l'humain est le principal maillon faible dans la chaîne d'attaques, il est essentiel qu'il soit sensibilisé et formé à détecter ces menaces. Cette formation doit également être complétée par des tests d'intrusion en continu afin de s'assurer que toute mauvaise configuration du périmètre ou tout dispositif périphérique non corrigé est détecté et corrigé avant d'être exploité par des acteurs indésirables.

3. Revoir la politique de mot de passe d'Active Directory

Un troisième conseil promulgué par les cybercriminels est de s'assurer que la politique de mots de passe est suffisamment robuste. L'un des premiers prérequis est de passer par une authentification multifactorielle (MFA) pour l'accès externe, qui est également étendue à la politique de mot de passe interne. Une partie de la chaîne d'élimination des rançongiciels consiste à étendre les privilèges pour permettre aux attaquants d'accéder à des volumes importants de données critiques et de les supprimer avant le cryptage forcé.

D'où l'importance d'identifier les mots de passe internes faibles, ou d'exploiter simplement un fichier XLS que les administrateurs de bases de données peuvent obtenir afin de répertorier tous les mots de passe clés de leur département.

4. Investir dans une solution de détection et de

réponse (EDR)

Les cybercriminels tendent de plus en plus à déployer des méthodes toujours plus créatives lorsqu'ils conçoivent leurs attaques. Une tendance récente consiste notamment à utiliser des outils installés de manière légitime, comme PowerShell, pour atteindre leurs objectifs. Dans le cadre d'une attaque par rançongiciel, les attaquants utilisent par exemple BitLocker pour chiffrer les appareils.

Quelle leçon tirer de cette méthode ? La détection des logiciels malveillants basée sur les signatures ne suffit plus. Une protection plus intelligente des terminaux, capable de surveiller en permanence les comportements suspects et de permettre la récupération, devient donc primordiale.

5. Protéger le réseau interne et isoler les systèmes critiques

Si les grands réseaux plats sont plus simples à administrer, ils permettent cependant aux attaquants d'atteindre plus facilement leurs objectifs. Avec la présence de couches supplémentaires de segmentation et de contrôle du réseau, entourant les systèmes et les données, une infection par un logiciel malveillant est moins susceptible d'avoir un impact sur les services critiques.

Si les systèmes informatiques d'entreprise sont constamment dans le radar des cyberattaquants, c'est bien parce qu'ils sont reliés à des organisations qui envoient et reçoivent des quantités colossales d'emails en continu. Les systèmes informatiques des entreprises doivent par conséquent, être isolés de l'infrastructure des données les plus sensibles de l'entreprise.

6. Adopter le stockage de données hors ligne et la sauvegarde sur bande

On peut regretter aujourd'hui que le concept de sauvegarde ait presque disparu des pratiques et des débats d'entreprises. Les sauvegardes en ligne déployées aujourd'hui sont pratiques car automatiques et offrent un certain niveau de transparence. Cependant les sauvegardes automatiques ne sont ni imperméables ni épargnées de toutes attaques. Si un attaquant parvient à dérober les identifiants de l'administrateur, il peut supprimer ou endommager l'ensemble d'une sauvegarde, ne laissant aucune chance à l'entreprise de récupérer ses données.

Nous avons certes entamé notre entrée dans l'ère de la transformation digitale, il n'en demeure pas moins qu'il est essentiel d'opter pour un mode de fonctionnement qui intègre les sauvegardes vers un stockage hors ligne afin de les tenir à l'écart des menaces.

Connaître son ennemi est une des règles primordiales pour le combattre. C'est pourquoi les RSSI ont tout intérêt à prendre connaissance de ces conseils inspirés des pratiques professionnelles d'experts en rançongiciel afin de réduire la surface d'attaque de leur entreprise.

L’ensemble de ces conseils permettent de tirer des leçons qui rappellent que la majorité des attaques sont opportunistes et initiées par des attaquants expérimentés capables de créer la moindre brèche afin de s’infiltrer et de causer des dégâts.