Comment protéger votre entreprise contre les attaques par rançongiciel

Un rapport spécial de Tunde Odeleye, directeur des services de tests de pénétration à Insight

Principaux points à retenir :

- Les attaques par rançongiciel sont fréquentes, il est donc justifié de mettre en place des mesures de sécurité spécifiques.
- Il est important de choisir des technologies d'entreprise efficaces et sécurisées, correctement gérées et maintenues.
- Utilisez des outils tels que l'authentification multifactorielle, car les mots de passe ne permettent pas une protection suffisante.
- Il convient également de vérifier et de mettre à jour régulièrement les processus de sauvegarde afin d'éviter tout risque de prise en otage de données.

J'ai récemment eu l'occasion de fournir mon aide à quatre entreprises qui ont été victimes d'attaques vicieuses par rançongiciel. Malgré la panoplie de solutions de sécurité disponibles, la fréquence et l'impact de ces attaques continuent de toucher aussi bien les grandes que les petites entreprises.

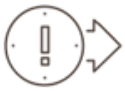
En intervenant dans ces entreprises et en tirant profit de mon expérience dans la réalisation de tests de pénétration, j'ai acquis des connaissances précieuses. Ces stratégies simples, mais efficaces peuvent aider votre entreprise à réduire les risques et la gravité des attaques par rançongiciel.

1. Choisissez la bonne solution de sécurité des terminaux.

Il n'y a pas de manière simple de dire cela, mais la vérité est que tous les produits de sécurité des terminaux ne sont pas créés égaux.
Il est important de s'assurer que vous avez choisi un produit fiable qui fonctionne correctement. Il n'a pas besoin d'être le meilleur, mais il doit répondre efficacement aux besoins et exigences uniques de votre entreprise. En outre, il est essentiel de veiller à ce que la solution de sécurité des terminaux soit correctement déployée dans l'ensemble de l'organisation.

La plupart des solutions de sécurité des terminaux protègent contre les menaces automatisées et manuelles en misant sur les fonctionnalités clés suivantes :

Détection et prévention des menaces entrantes (pré-exécution)



Détection et prévention des menaces basées sur l'exécution (lors de l'exécution)

Analyse continue et correction après l'infection (post-exécution)

La triste vérité est que les solutions de sécurité des terminaux disponibles sur le marché ne possèdent pas le même niveau d'informations sur les menaces et n'offrent pas une efficacité de correction similaire.

Lorsque tous les autres moyens échouent - et cela arrivera inévitablement - votre solution de point de terminaison sera votre ultime ligne de défense. Alors, choisissez judicieusement. Si vous n'êtes pas certain de la solution à adopter, je vous recommande vivement de faire appel à une personne qui comprend votre système informatique et vos exigences en matière de sécurité, et qui peut vous aider à prendre la bonne décision.

2. Surveillez vos modifications Active Directory.

Dans chacun des engagements de rançongiciel récents que j'ai dirigés, j'ai remarqué que le client ne surveillait pas de manière proactive ses modifications Active Directory® (AD), en particulier les stratégies de groupe.

À chaque fois, les attaquants ont modifié une stratégie de groupe existante pour créer une tâche planifiée qui exécuterait un programme malveillant à une date ultérieure. C'est incontestablement la méthode la plus rapide et la plus simple pour diffuser une attaque dans un environnement.

La surveillance des changements dans l'Active Directory, en particulier en dehors des heures de travail et pendant les week-ends, est un moyen extrêmement efficace de repérer les signes précurseurs d'une attaque avant qu'elle ne devienne incontrôlable.

3. Mettez en œuvre une stratégie d'isolation des postes de travail.

Je considère que cela représente la stratégie la plus efficace pour atténuer les mouvements latéraux des attaquants malveillants dans n'importe quel environnement.

La posture de sécurité par défaut de la plupart des organisations permet aux postes de travail situés sur le même sous-réseau - et dans certains cas sur l'ensemble du réseau de l'entreprise - de communiquer entre eux. À bien y penser, est-ce qu'un poste de travail doit réellement communiquer avec un autre poste de travail? La réponse est généralement « non », étant donné que la majorité des communications réseau surviennent entre des clients (c.-à-d. des postes de travail ou des serveurs) interagissant avec des serveurs (c.-à-d. localisés sur place ou dans le nuage).

En conséquence, si nous réduisons la communication entre les postes de travail, un poste de travail compromis (le patient Zéro) ne serait pas à même de nuire à d'autres postes de travail, limitant ainsi les risques d'attaques potentielles. Le patient Zéro ciblerait alors uniquement les ressources des serveurs, ce qui devrait faciliter la détection de toute tentative d'attaque si des contrôles techniques adéquats et des mesures de renforcement sont mis en place.

En fait, la plupart des environnements ont déjà accès à une solution parfaitement adaptée grâce au pare-feu Windows® Defender, gérable au sein des stratégies de groupe AD. Cela pourrait faire partie d'une stratégie globale de renforcement des terminaux que de nombreuses entreprises n'ont pas encore entrepris. L'isolation des postes de travail est une stratégie de sécurité très efficace, mais presque jamais utilisée dans la plupart des environnements que j'ai vus.

4. Mettez en œuvre un programme de gestion des vulnérabilités.

Remarquez que je n'ai pas employé le mot « patch » ou « correctif ». Même si elle est extrêmement importante, la correction ne suffit pas.

En y réfléchissant bien, l'objectif des correctifs consiste à combler les failles de sécurité des logiciels. Cependant, il ne s'agit pas là des seules vulnérabilités auxquelles il faudrait prêter attention.

Vos failles de sécurité peuvent également être liées à la configuration. Vous pouvez avoir les systèmes et les applications les plus récents du marché, mais si vos systèmes internes utilisent des protocoles non sécurisés, tels que NTLMv1, des problèmes majeurs peuvent survenir.

Je recommande donc aux organisations de mettre en place un programme de gestion des vulnérabilités, incluant une analyse régulière des actifs externes et internes, ainsi qu'une hiérarchisation des correctifs, en fonction de la gravité des vulnérabilités identifiées, qu'elles soient ou non liées aux correctifs. Ensuite, il convient de procéder aux corrections nécessaires.

5. Mettez en place l'authentification multifactorielle.

Nous avons tous été sensibilisés à l'importance d'utiliser des mots de passe robustes, mais en réalité, les mots de passe à eux seuls ne suffisent pas.

Dans chaque incident auquel j'ai été confronté, l'AMF (authentification multifactorielle) ne figurait pas parmi les mesures de sécurité mises en place. Le recours exclusif à des mots de passe, même s'il s'agit de mots de passe complexes, expose votre système à des risques. En revanche, l'exigence d'une seconde forme d'authentification contribue à garantir l'identité de l'utilisateur en question, ce qui est généralement plus difficile à obtenir pour un attaquant.

,

Si la transformation numérique a une orientation externe, alors l'AMF est un impératif pour tout le monde.

Si elle est orientée vers l'intérieur, l'AMF est un impératif pour tous les comptes d'administrateur.

Ceci est en fin de compte basé sur la tolérance au risque de l'entreprise, cependant, les règles susmentionnées sont un bon point de départ.

6. Effectuez régulièrement des sauvegardes hors ligne.

Les sauvegardes doivent être complètes et réalisées régulièrement, avec des copies hors ligne. Cela signifie que les copies hors ligne ne sont pas constamment accessibles à partir des réseaux de production.

Lors d'un incident, les attaquants ont complètement supprimé la solution de sauvegarde de l'entreprise du client. Cependant, les sauvegardes hors ligne stockées dans le nuage ont permis au client d'économiser littéralement plusieurs milliers de dollars en évitant de payer une rançon. Dans un autre cas, le client a été contraint de payer plusieurs centaines de milliers de dollars en raison du caractère critique des systèmes d'entreprise cryptés, car il n'avait pas d'autre choix.

Il existe de nombreuses autres mesures pour se protéger contre les rançongiciels qui n'ont pas été abordées dans cet ouvrage. L'objectif était ici de présenter quelques stratégies simples et efficaces pouvant être rapidement mises en place pour lutter contre ces attaques. J'espère que ces informations vous aideront à empêcher votre entreprise de devenir la prochaine victime, car votre entreprise ne mérite pas le stress, les coûts et les dommages à la réputation qui en découlent.

Si vous avez des questions sur ces stratégies, ou si vous souhaitez discuter de la posture de sécurité de votre organisation avec nos experts, nous serons heureux de vous aider.

Contactez-nous pour parler avec notre équipe de sécurité.

En savoir plus sur nos services de sécurité.

Explorez notre approche et nos capacités.

Favoriser l'innovation avec la transformation numérique.

Chez Insight, nous accompagnons nos clients dans leur quête de stimulation de l'innovation avec une approche holistique qui englobe les personnes, les processus et les technologies. Nous sommes convaincus que le chemin le plus direct vers la transformation numérique est une approche intégrative, réactive et proactivement alignée sur les demandes de l'industrie. Notre approche centrée sur les clients propose des solutions qui comprend une gamme complète de services personnalisables, tels que le lieu de travail numérique, les applications modernes, les infrastructures modernes, l'intelligence de périphérie, la cybersécurité, ainsi que les données et l'IA.

Pour en savoir plus :

ca.insight.com/ransomware-defense

Insight.

ca.insight.com