Anatomie d'une violation

De quelle manière les utilisateurs malveillants s'introduisent-ils et comment peut-on les repousser

Une attaque virtuelle peut coûter des millions à votre société. Disposez-vous du bon plan pour résister à une violation, la contrecarrer et en réparer les conséquences ?

Microsoft

TABLE DES MATIÈRES

Introduction

Les quatre étapes d'une violation

Les quatre étapes d'une violation

En matière de sécurité, les menaces sont incessantes. Avant même que vous ne vous en rendiez compte, une attaque virtuelle peut faire des dégâts évalués à plusieurs millions de dollars, tant au niveau de votre société en elle-même qu'à celui de sa réputation. Êtes-vous au courant des menaces potentielles pour votre société ? Disposez-vous du bon plan pour résister à une violation, la contrecarrer et en réparer les conséquences, lors de ses quatre étapes de déploiement ?

Poursuivez la lecture pour en savoir plus sur chaque étape et examiner certains exemples issus de vraies entreprises, ainsi que le type de dégâts infligés par les utilisateurs malveillants à chaque stade. Vous découvrirez également comment formuler une stratégie de défense basée sur les failles potentielles pour vous protéger vous et votre société.

Étape 1 :
Obtention d'un point d'appui initial

Étape 2 :
Obtention d'un contrôle élevé
(réaffectation locale de privilèges)

Étape 3 :
Développement dans le réseau
(Réaffectation de privilèges Active Directory)

Étape 4 :
Installation pour une présence à long terme

Étape 1 : Obtention du point d'appui initial

L'ouverture la plus petite peut permettre à un utilisateur malveillant d'obtenir un point d'appui dans votre entreprise. Que ce soit via une station de travail compromise, un serveur non protégé accessible sur Internet ou un appareil mal configuré géré par un tiers, un utilisateur malveillant peut utiliser et utilisera tout ce dont il dispose pour percer les défenses d'une société et obtenir l'accès à son réseau. Une fois dans le système, il peut effectuer les tâches de reconnaissance nécessaires pour identifier et cibler les informations ou ressources précieuses de votre entreprise.

Termes courants :

Hameçonnage : méthode visant à amener les utilisateurs à communiquer des informations personnelles, financières ou spécifiques à l'entreprise, qui peuvent être utilisées pour obtenir un accès non autorisé à une infrastructure interne. Les utilisateurs malveillants peuvent utiliser de faux sites web ou e-mails qui semblent venir d'un contact fiable (par exemple : fournisseurs tiers ou autres collaborateurs internes) pour inciter les utilisateurs à cliquer sur des liens web, des documents malveillants ou d'autres sources d'infection.

Attaque de point d'eau : site web que les utilisateurs malveillants ont identifié comme étant fréquemment visité par leur cible visée. L'utilisateur malveillant place des liens vers des programmes malveillants sur le site dans l'espoir que la cible soit infectée lorsqu'elle s'y rend.

Programmes malveillants : ces programmes effectuent des actions indésirables sur votre PC, comme le vol d'informations, le verrouillage de votre PC jusqu'à ce que vous payiez une rançon, ou l'utilisation de votre PC pour envoyer du courrier indésirable. Virus, vers et chevaux de Troie sont trois types de programmes malveillants. (Ce document se concentre sur ce que l'on appelle fréquemment des « programmes malveillants ciblés », un type de programme conçu pour infiltrer un secteur ou une organisation spécifique.)

Code malveillant exploitant une faille de sécurité : élément de code qui utilise des vulnérabilités logicielles pour accéder à des informations sur votre PC ou installer des programmes malveillants.

Vulnérabilité Zero day : attaque logicielle qui a été divulguée ou corrigée par le fournisseur logiciel.

Profil sectoriel : Secteur de la santé

Le secteur de la santé a enregistré une consolidation au cours des dernières décennies, à mesure que les hôpitaux fusionnent. Bien que ce processus ait été fructueux du point de vue des soins de santé, une fusion s'accompagne souvent de défis technologiques pour le personnel. Les hôpitaux nouvellement associés peuvent décider de réduire leurs investissements globaux dans les technologies de l'information en centralisant les services IT au sein d'un même service.

Le processus de fusion des réseaux, infrastructures et logiciels peut conduire à une défaillance s'il n'est pas effectué correctement. Les utilisateurs malveillants commencent généralement par s'introduire sur le réseau dont le niveau de sécurité est le plus faible. Après quoi, ils peuvent exploiter les failles de sécurité internes pour avoir accès au réseau plus sécurisé. Dans un scénario réel, un attaquant a pu accéder à un réseau avant d'utiliser un réseau social par e-mail pour s'introduire sur le réseau d'un autre hôpital. L'hôpital s'est rendu compte qu'il y avait un problème lorsqu'une mise à niveau a provoqué des problèmes de stabilité sur ses serveurs. Des enquêteurs ont découvert qu'un programme malveillant se trouvait depuis longtemps sur le réseau et qu'il compromettait ce dernier.

De nombreux facteurs ont contribué à la défaillance globale. L'hôpital ne sépare pas son réseau de celui d'autres organisations, ce qui permet aux utilisateurs malveillants de pénétrer le réseau le moins protégé. Des identifiants communs ont été utilisés sur l'ensemble du réseau, ce qui a permis aux utilisateurs malveillants d'accéder plus facilement aux différentes zones après s'être introduits. En outre, des applications héritées développées en interne fonctionnaient avec des privilèges trop laxistes. Plusieurs années ont été nécessaires pour repenser et reconstruire le réseau, avec la nécessité d'un changement culturel pour en avoir la pleine maîtrise.

Lorsqu'un point d'appui est établi, la tâche d'un utilisateur malveillant est facilitée. Pénétrer un réseau à l'aide de l'une de ces méthodes permet à un utilisateur malveillant de découvrir les identifiants plus efficaces, ce qui lui ouvre la voie vers des zones plus sensibles du réseau.

Un soupçon de prévention...

Des mesures de sécurité plus efficaces, incluant la formation du personnel et la mise en œuvre d'une solution de technologie adaptée, peuvent aider des hôpitaux à garder la forme.

Nous conseillons les mesures préventives suivantes :

Intégrez une base solide de critères de sécurité sectoriels : séparez les réseaux, intégrez des exigences sévères en matière de mots de passe forts, adoptez une démarche de séparation des privilèges et exigez des mots de passe individuels pour chaque réseau ou zone d'accès. Ces mesures s'imposent notamment pour des appareils hérités susceptibles d'être attaqués sans qu'ils puissent être protégés.

Mise à niveau des réseaux : gardez l'infrastructure réseau à jour pour veiller à conserver un niveau de sécurité optimal

Utilisez des solutions avec garantie intégrée : Le Health Insurance Portability and Accountability Act de 1996 (HIPAA) s'applique à toutes les sociétés de soins de santé aux États-Unis et prévoit des exigences pour l'utilisation, la divulgation et la protection d'informations de santé individuellement identifiables. Les services cloud de Microsoft sont compatibles avec le HIPAA et la fonctionnalité de protection avancée contre les menaces de Windows 10. Par ailleurs, Office 365 analyse automatiquement tous les liens et les pièces jointes dans les e-mails entrants, à la recherche de menaces potentielles. Le contenu douteux n'a pas l'autorisation d'atteindre les utilisateurs finaux, ce qui limite les menaces de piratage psychologique sur votre réseau.

Étape 2 : Obtention d'un contrôle élevé

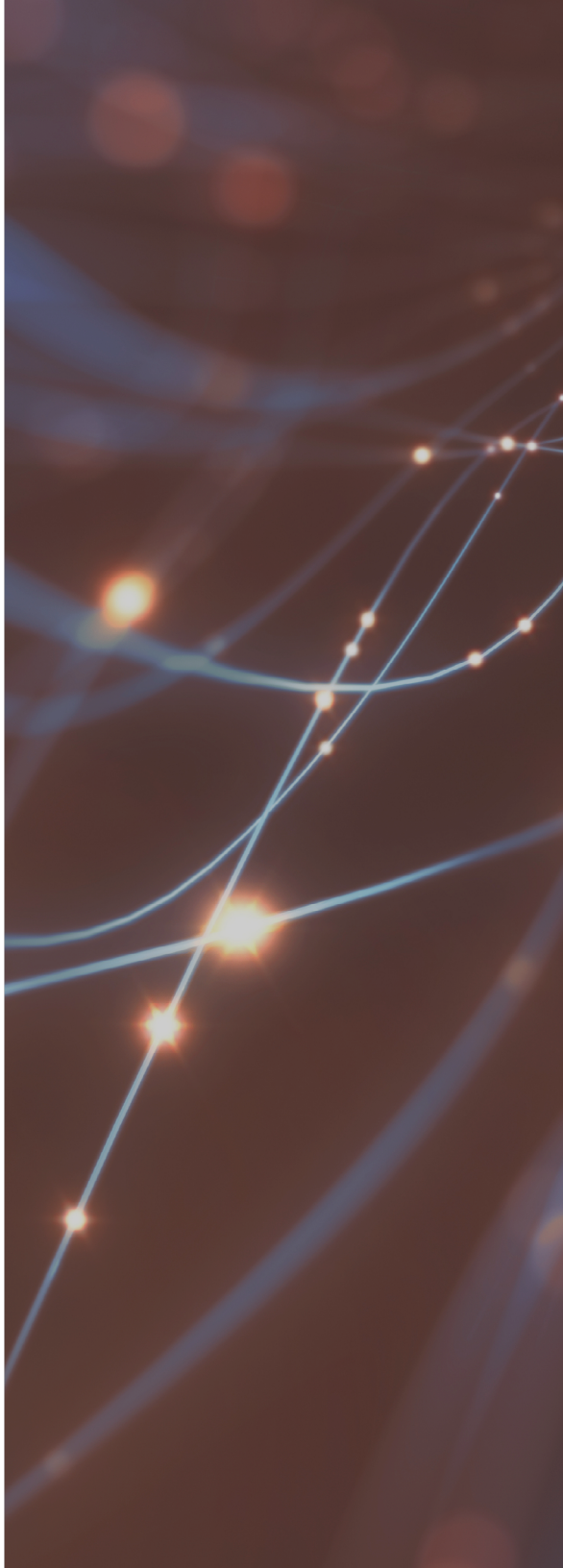
Après qu'un utilisateur malveillant a pénétré une organisation, l'étape suivante est la réaffectation locale de privilèges. Les attaquants recherchent généralement une méthode pour conserver leur contrôle du système local ou ciblent un autre système qui présente une probabilité de réussite plus élevée pour l'obtention de privilèges administratifs ou d'un accès plus étendu à des données précieuses. L'objectif de l'utilisateur malveillant est d'identifier les comptes d'utilisateur responsables de la gestion du système afin d'imiter la capacité de ces comptes à gérer, mettre à jour et consulter les ressources système. Ensuite, en utilisant des outils intégrés et téléchargés, l'utilisateur malveillant tente d'identifier d'autres systèmes d'intérêt et ressources réseau, et de capturer des noms d'utilisateur et des mots de passe. En règle générale, ces actions ne peuvent pas être accomplies par un utilisateur normal.

Termes courants :

Enregistreurs de frappes : programmes malveillants qui enregistrent les frappes d'un utilisateur. L'enregistrement de frappes permet aux utilisateurs malveillants de collecter les noms d'utilisateur et mots de passe afin de se connecter au réseau de l'entreprise ciblée.

Attaques Pass-the-hash : technique selon laquelle un utilisateur malveillant utilise le hash (code) du mot de passe d'une victime pour se faire passer pour cet utilisateur. L'attaquant ne doit pas connaître les identifiants réels pour s'authentifier auprès d'un serveur/service distant.

Analyse de réseau : les attaquants utilisent cette technique de reconnaissance pour répertorier les systèmes auxquels ils ont accès, tels que des machines hôtes, des services et des ressources actives sur le réseau. Les attaquants créent ensuite une liste cible de systèmes intéressants auxquels ils tenteront d'accéder avec leurs identifiants administratifs récemment acquis.



Profil sectoriel : Média de divertissement

Prenez un secteur très en vue, ajoutez-y du contenu controversé, et voilà une cible parfaite pour les utilisateurs malveillants. Les attaques ciblant les organisations de médias et de divertissement sont souvent menées dans le but de marquer le coup et de subtiliser des informations. Les anciennes attaques d'utilisateurs malveillants ont provoqué le chaos en dévoilant des informations sensibles d'une société ou en prenant le contrôle des sites web de celle-ci.

Dans un tel cas de figure, une société était victime d'une violation qui ne se contentait pas d'en perturber le fonctionnement ; des données sensibles relatives aux collaborateurs, aux clients et à la propriété intellectuelle étaient en outre subtilisées. Bien que les circonstances de la survenue de cette violation ne soient pas tout à fait claires, des cas similaires se sont présentés avec d'autres vecteurs d'attaque bien connus, tels que le piratage psychologique, des vulnérabilités non protégées ou de simples erreurs de configuration.

Pour une société de médias, les dégâts peuvent être considérables. L'étendue et l'impact potentiel de cette violation, tant sur le plan financier que géopolitique, sont inouïs. Outre les frais non négligeables associés à la recherche et à l'élimination de l'attaque réelle, le coup le plus sévère est porté à la réputation de la société : elle doit désormais consacrer du temps et de l'argent à la réhabilitation des relations, des moyens qui auraient pu être consacrés au développement de nouveaux projets.

Une solution de réseau efficace

Le développement d'une stratégie de sécurité renforcée peut empêcher des attaques dévastatrices et constitue un élément fondamental de la gestion intégrale des risques. Cela implique de maîtriser les ressources dont vous disposez, les risques potentiels pour ces ressources, l'impact pour la société si ces ressources s'échappent, ainsi que les contrôles en place pour protéger ces ressources. Il est également essentiel de pouvoir déterminer le moment où un problème se produit, de pouvoir le contenir et de répondre efficacement aux conséquences. Ces approches doivent être considérées comme un élément du cycle de vie en matière de sécurité au sein d'une organisation, où le risque est évalué sur une base régulière et où les enseignements tirés servent au bon fonctionnement du système.

Nous recommandons de miser sur ces mesures de sécurité :

Protection, détection, réaction : cette approche vous permet de créer une infrastructure de sécurisation des systèmes. Elle fait partie des approches que Microsoft et d'autres sociétés adoptent pour comprendre le risque, faire face à une violation éventuelle et y remédier, ainsi que pour en tirer des enseignements.

Mettez en œuvre l'accès avec séparation des privilèges : définissez vos contrôles d'accès au réseau en vous basant sur les rôles plutôt que sur les méthodes de travail individuelles, puis limitez l'accès au minimum pour effectuer des tâches attribuées. Si une personne n'a pas besoin d'un accès à un réseau ou à une ressource pour son travail, ne lui en attribuez pas. Il s'agit d'une méthode commune pour enrayer toute violation.

Security Development Lifecycle : ce processus de développement de logiciels aide les développeurs à créer des logiciels plus sécurisés et à répondre à des exigences en matière de conformité et de sécurité tout en réduisant les coûts de développement.

Et la mise en œuvre des outils suivants :

Solutions LAPS (Local Administrator Password Solutions) : cette solution peut être utilisée pour définir un mot de passe aléatoire différent sur chaque ordinateur d'un domaine. Ensuite, les contrôleurs de domaine peuvent l'utiliser pour déterminer quels utilisateurs (p. ex. : administrateurs du helpdesk) ont l'autorisation de lire des mots de passe.

Windows 10 Credential Guard : cette sécurité basée sur la virtualisation et introduite dans Windows 10 Entreprise isole les informations secrètes afin que seuls les logiciels système dotés de privilèges puissent y accéder.

Microsoft Advanced Threat Analytics (ATA) : vous permet d'identifier les menaces et les violations de sécurité à l'aide d'une analyse du comportement, sécurise les logiciels et satisfait aux exigences de conformité en matière de sécurité tout en réduisant les coûts de développement.

Profil sectoriel : Industrie agroalimentaire

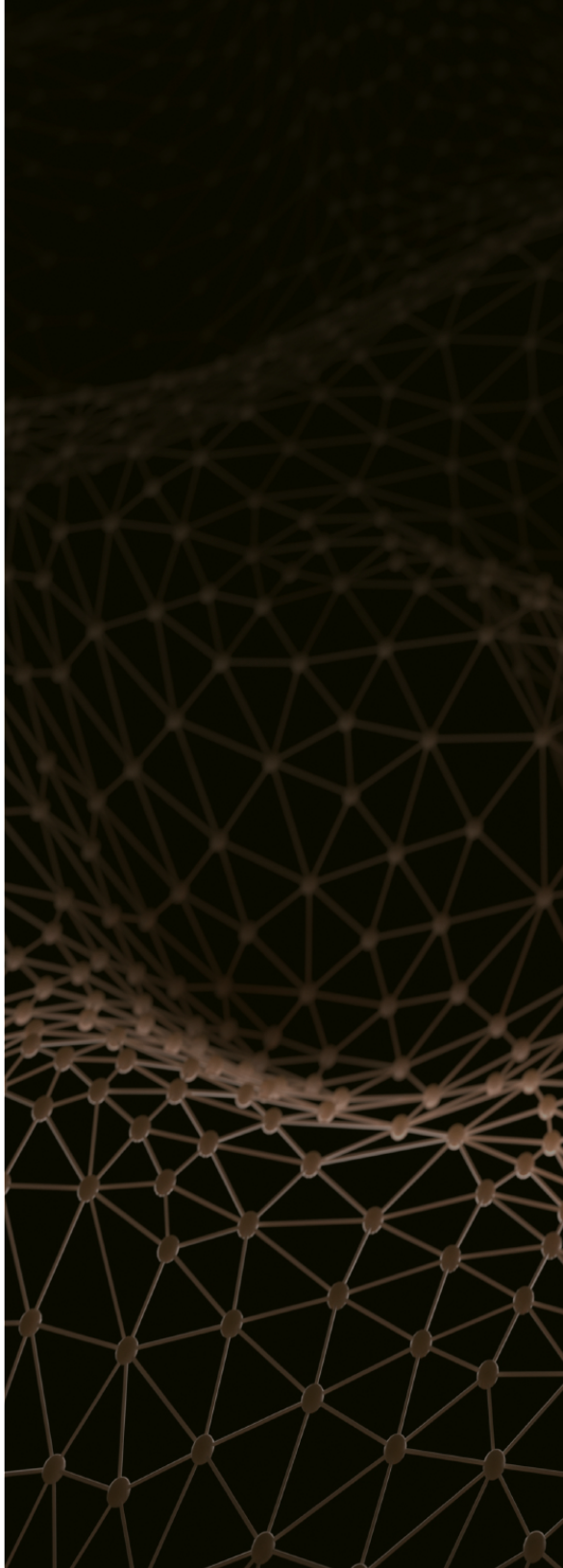
Une grande entreprise spécialisée dans la fabrication de boissons avait conscience qu'elle devait faire un effort pour améliorer la sécurité du réseau tout en réduisant les frais relatifs à l'IT, sans toutefois savoir par où commencer. Elle a décidé d'externaliser ses activités IT et de se concentrer sur sa spécialité : fabriquer des boissons rafraîchissantes. Externaliser la tâche vers une société IT devait améliorer la sécurité des données de la société. Au lieu de cela, le fabricant s'est fait avoir. La société n'est pas parvenue à suivre les processus de diligence raisonnable lors de la protection des comptes critiques des clients. De même, elle n'a pas pu conserver une intégrité élevée avec les comptes à valeur élevée des clients qui accédaient à des serveurs du même ordre.

En l'occurrence, comme le fournisseur IT n'a pas séparé les comptes de la société des activités normales du fournisseur, ces comptes étaient exposés à des attaques normales, telles que le piratage psychologique via la messagerie des collaborateurs et le hasard de la navigation sur le web. Après que l'utilisateur malveillant s'était emparé des comptes de la société, il a pu gérer la société à distance, comme peut le faire le fournisseur IT. Pour corser le tout, le fabricant a dû réagir via le fournisseur IT, étant donné que les systèmes principaux du client n'étaient plus gérés localement. Cela a rendu les efforts de coordination des enquêtes et de résolution des problèmes plus difficiles jusqu'à ce que les comptes critiques soient de nouveau aux mains de l'équipe en charge de la résolution des problèmes.

Certaines scénarios d'usage critiques peuvent être externalisées tandis que le fabricant de boissons conserve l'accès à ses données et à ses systèmes principaux au sein de l'organisation. Les coûts peuvent être réduits sans externalisation, en déplaçant des systèmes professionnels vers le cloud (p. ex. : en remplaçant un déploiement de messagerie sur site par une solution hébergée et gérée telle qu'Office 365), tout en concentrant les flux de travail internes sur la fabrication en tant que telle. Une solution hébergée permet de réduire la charge de travail des collaborateurs, génère des coûts mensuels prévisibles, préserve le contrôle de la société et exploite l'expérience du fournisseur de services.

Si l'environnement inclut de nombreux systèmes avec une capacité importante, la société doit songer à les déplacer vers un service cloud de confiance. Le cloud permet de disposer d'une plateforme, d'une infrastructure et de services complets sans qu'il soit nécessaire de configurer et d'entretenir tous les systèmes et datacenters. La société ne doit pas gérer la protection et l'administration des systèmes d'exploitation et du matériel.

Il est toujours important de poser des questions, qu'il s'agisse d'un fournisseur externe ou d'un fournisseur de services cloud, à propos de ses pratiques et stratégies en matière de sécurité des données, de confidentialité, de contrôle, de conformité et de transparence. Si le fabricant avait identifié l'ensemble des risques dans les pratiques de sécurité de la société responsable de l'externalisation, elle aurait peut-être pris une décision plus avisée pour déterminer à qui accorder sa confiance.



Le secret de la réussite

L'externalisation des fonctions IT peut être une solution attrayante pour réduire les frais généraux. Toutefois, il est nécessaire de déterminer si l'externalisation IT fournira les défenses idéales pour les données et la propriété intellectuelle de votre entreprise. Vous devrez ensuite choisir un fournisseur ou fournisseur de services dont les stratégies et pratiques sont dignes de votre confiance. Comme le fabricant de boissons a pu le découvrir, les avantages de l'externalisation doivent être mis en perspective avec le risque qu'implique la gestion de la sécurité des données par une entreprise tierce.

Nous vous conseillons de poser les questions suivantes avant de rechercher un fournisseur :

- **Quels types de services devons-nous externaliser ?**
- **Quel niveau d'accès devons-nous externaliser ?**
- **Comment peut-on utiliser le cloud pour réduire les coûts IT (plutôt que d'externaliser vers un tiers) ?**

Après vous être penché sur votre situation, il se peut que vous déterminiez que la meilleure solution est de faire appel à un fournisseur externe ou à un fournisseur de services cloud. Assurez-vous d'analyser, de contrôler et de surveiller de près le fournisseur potentiel, avec toute l'assiduité nécessaire. Posez-lui des questions et déterminez s'il semble digne de confiance en cas de catastrophe.

Posez les questions suivantes à vos fournisseurs potentiels :

- **Suivez-vous les pratiques idéales de Enhanced Security Administrative Environment (ESAE) ?**
- **Imposez-vous des restrictions quant à déterminer où les comptes de l'administrateur de domaine (AD) et l'administrateur d'entreprise (AE) peuvent se connecter ?**
- **Utilisez-vous Privileged Identity Management pour Azure Active Directory ?**

Étape 3 : Développement dans le réseau

À l'étape 3, l'utilisateur malveillant obtient un accès plus large à votre réseau en s'étendant depuis une station de travail ou un serveur individuel vers le plus de systèmes possible. L'utilisateur malveillant peut ensuite installer une porte dérobée permanente ou un mécanisme alternatif pour profiter d'un accès à long terme aux systèmes.

L'attaquant utilisera des outils, dont certains peuvent être des programmes malveillants (appelés implants). Certaines méthodes peuvent sembler plus légitimes, comme la création de faux comptes et l'obtention d'un accès distant, si bien que l'utilisateur malveillant dispose de plusieurs moyens pour accéder de nouveau au réseau, mais aussi pour se cacher dans l'environnement et accéder à de nombreuses ressources. En règle général, lorsqu'ils utilisent des implants et des robots, les utilisateurs malveillants disposent d'une console de commande et de contrôle pour l'ensemble des ressources qu'ils contrôlent. Ils utilisent cette console pour veiller à garder une mainmise correcte sur le réseau. S'ils se rendent compte que l'un des accès qu'ils contrôlent est systématiquement déconnecté, ils savent que quelqu'un les traque et ils peuvent tenter de rétablir leur accès et d'échapper à toute détection.

Termes courants :

Robots : petits programmes cachés installés sur votre PC par un utilisateur malveillant sans que vous le sachiez.

Botnet : système malveillant dans lequel de nombreuses copies d'un robot sont installées sur de nombreux PC et contrôlées par un utilisateur malveillant, qui peut les utiliser pour des attaques de grande envergure.

Commande et contrôle : les serveurs et l'infrastructure utilisés pour contrôler de nombreux ordinateurs via des commandes centralisées, telles qu'un botnet. L'utilisateur malveillant black hat qui exécute une console de commande et de contrôle de botnet est appelé un contrôleur ou un botmaster.

Profil sectoriel : Institution publique

Cette institution publique a fait les bons choix à presque tous les niveaux. Le logiciel a été protégé dans des délais raisonnables, un nombre relativement restreint d'utilisateurs finaux disposaient de droits d'administration, et des contrôles de sécurité réguliers étaient effectués (analyses). Une mention spéciale peut également être formulée pour le maintien de stations de travail administratives dédiées pour une utilisation par l'administrateur de domaine (AD) et par l'administrateur d'entreprise (AE). (Les AD et AE régulent tous les autres comptes de l'organisation. Très peu de personnes dans l'entreprise doivent disposer d'un tel niveau d'accès. L'attribution d'informations d'identification de type AD ou AE doit être strictement contrôlée.)

L'erreur fatale commise par cette organisation a été d'utiliser le même mot de passe administratif local pour toute l'entreprise, sur tous les ordinateurs des services RH, comptabilité et IT. Comment des dirigeants sensés disposant de ressources publiques ont-ils pu commettre cette erreur ?

L'usage de mots de passe administratifs locaux est une pratique répandue dans de nombreuses organisations qui ne comprennent pas les risques associés. Il arrive que la configuration initiale des systèmes ne fonctionne pas comme prévu avec les comptes restreints. Pour résoudre ce problème, les administrateurs attribuent davantage de droits à ces comptes, jusqu'à ce que l'application fonctionne. Si le problème n'est toujours pas résolu, l'administrateur peut décider de maintenir ces droits supplémentaires afin de pouvoir contourner l'erreur. Dans d'autres situations, des comptes locaux sont parfois utilisés en cas d'urgence, puis demeurent sur le système pour être utilisés ultérieurement. Dans ces deux cas, le système est alors vulnérable aux attaques. Ces comportements IT révèlent une stratégie de sécurité axée sur le local, qui ne fournit pas de protection adéquate contre les menaces inhérentes à l'ère de l'Internet toujours actif et toujours connecté.

Dans le cas de cette agence publique, un pirate a pu s'introduire sur le réseau lorsqu'un autre utilisateur a accédé à un document infecté ou cliqué sur un lien vers un site Web contenant du code malveillant. (Le moment exact de la contamination n'est pas connu.) Étant donné que l'organisme utilisait le même mot de passe administratif local pour tous ses services, le pirate a pu explorer le réseau et récupérer les informations d'identification AD et AE. Ces données étaient un véritable sésame : l'utilisateur malveillant a pu implanter un code dans les datacenters, les serveurs et sur Microsoft Exchange, provoquant une contamination du réseau entier qui a coûté des millions de dollars.

Les coûts directs de ce piratage comprenaient la reconstruction des systèmes, la création de nouveaux mots de passe et les enquêtes publiques sur le vol de données et la cause du piratage. Quant à la perte de la confiance des victimes du piratage, elle ne peut être quantifiée par un prix.

Une stratégie de défense complète

L'institution publique a fait beaucoup de choix judicieux, mais pour bloquer efficacement les attaques, il faut surtout adopter une approche complète.

Nous conseillons les mécanismes de défense suivants :

Trousse à outils EMET (Enhanced Mitigation Experience Toolkit) : cet utilitaire empêche l'exploitation des vulnérabilités logicielles.

Microsoft Office 365 : cette suite de produits est conçue pour répondre aux besoins de votre organisation en matière de sécurité, notamment l'utilisation des données selon des normes juridiques, réglementaires et techniques.

Enhanced Security Administrative Environment (ESAE) : cet outil s'appuie sur des technologies avancées et des pratiques recommandées pour garantir des stations de travail et un environnement administratifs protégés par des systèmes de sécurité avancés.

Privileged Identity Management pour Active Directory : vous permet de gérer, de contrôler et de surveiller vos identités privilégiées et leurs droits d'accès aux ressources sur Azure Active Directory et d'autres services en ligne de Microsoft (p. ex. Office 365 et Microsoft Intune).

Microsoft Advanced Threat Analytics (ATA) : utilise l'analyse du comportement pour surveiller les utilisations anormales de comptes et d'informations d'identification.

Operations Management Suite (OMS) : solution de gestion IT basée dans le cloud qui vous aide à surveiller les utilisateurs malveillants, à les alerter et à suivre leurs actions.

Étape 4 : Installation pour une présence à long terme

L'étape 4 consiste pour l'utilisateur malveillant à s'installer pour une présence durable en déployant des processus discrets et continus, comme l'utilisation de programmes malveillants pour exploiter les vulnérabilités et la surveillance ainsi que l'extraction de données, tout en évitant d'être repéré pendant la plus longue durée possible. Les utilisateurs malveillants créent des comptes pour eux-mêmes afin de garantir leur présence sur le réseau. Ils modifient également les mots de passe afin d'échapper aux outils de détection.

Tout comme à l'étape 3, les pirates utilisent des implants ou des robots pour créer et maintenir plusieurs possibilités d'accéder au réseau et de se dissimuler dans l'environnement. Ils utilisent un serveur de commande et contrôle pour conserver leur point d'appui et parcourir les ressources et les canaux via le réseau comme bon leur semble. S'ils pensent avoir été détectés, ils disposent des moyens et des ressources nécessaires pour s'échapper et récupérer leur accès.

Termes courants :

Menace avancée persistante (APT) : une attaque ciblée contre une entité spécifique dans le but d'éviter la détection et de dérober des informations sur une période donnée.

Failles potentielles : il s'agit d'une approche stratégique. Pour les dirigeants d'entreprise et les responsables de la sécurité informatique, cette approche implique de se pencher davantage sur la détection, la réaction et la récupération en cas de problèmes de sécurité, plutôt que sur des mesures de sécurité purement préventives.

Profil sectoriel : Industrie High-Tech

Les utilisateurs malveillants sont capables de redoubler de patience. Après avoir infiltré un réseau, ils peuvent rester cachés pendant des centaines de jours. Pendant cette période, ils reconstruisent les systèmes, écrasent les fichiers journaux et mettent à jour leurs outils de piratage. Une entreprise spécialisée dans l'industrie High-Tech a laissé un intrus accéder à son réseau pendant au moins un an et demi avant de s'apercevoir du piratage. Pendant cette période, le pirate est parvenu à implanter des logiciels malveillants avancés sur le serveur du lecteur de base d'un client qui contenait absolument toutes les données d'un client théoriquement protégées par la propriété intellectuelle.

L'utilisateur malveillant avait désormais à sa disposition les présentations PowerPoint, documents, échéanciers de projets et procédures détaillées de fabrication du client, qu'il pouvait utiliser à tout moment. Un nombre incalculable d'informations de recherche et de développement ont été dérobées à différents emplacements du réseau du client avant que celui-ci ne détecte la violation.

Mise en place d'une sécurité plus efficace

Personne ne sait comment le pirate est parvenu à s'introduire sur le réseau du client du fabricant. La nature de l'attaque nous indique que les pirates ont trouvé un moyen de s'octroyer l'accès afin d'implanter le logiciel malveillant.

Dans l'optique d'empêcher ce type de faille, nous recommandons les outils suivants :

Protection avancée contre les menaces : cette fonctionnalité intégrée à Office 365 analyse automatiquement toutes les pièces jointes et liens figurant dans les e-mails reçus afin de détecter les menaces potentielles. Le contenu douteux n'a pas l'autorisation d'atteindre les utilisateurs finaux, ce qui limite les menaces de piratage psychologique pour votre réseau.

Multi-factor authorization (MFA) : exige une vérification supplémentaire de la part des utilisateurs, sans se contenter d'un nom d'utilisateur et d'un mot de passe. Par exemple, l'utilisateur peut confirmer son identité via un appel téléphonique ou un SMS.

Azure Rights Management (Azure RMS) : cette solution de protection des informations utilise des stratégies de chiffrement, de gestion des identités et d'autorisation pour vous aider à garantir la sécurité de vos fichiers et e-mails. Elle fonctionne sur plusieurs appareils, notamment les téléphones, tablettes et PC.

Microsoft OneDrive : cette solution de stockage dans le cloud offre diverses possibilités de protection des fichiers. Les fichiers stockés sur OneDrive ne sont jamais partagés avec d'autres utilisateurs, à moins d'être enregistrés dans un dossier public ou d'être partagés volontairement. Pour encore plus de sécurité, vous pouvez créer un mot de passe fort, ajouter des paramètres de sécurité à un compte Microsoft existant (par exemple, une autre adresse de messagerie ou une question de sécurité) et utiliser la vérification en deux étapes.

Datacenters Microsoft : Microsoft s'appuie sur des décennies d'expérience dans le domaine des logiciels professionnels et des services en ligne mondiaux pour créer des technologies et pratiques sécurisées et fiables. Nos datacenters sont construits, gérés et surveillés de façon physique au moyen de barrières, de gardes, de contrôles en arrière-plan, de systèmes d'authentification biométrique, de formations sur la sécurité et d'un outil de destruction de disque dur semblable à une déchiqueteuse, permettant de supprimer des serveurs. Tous les datacenters font l'objet d'une surveillance permanente, sont soumis à une authentification multifacteur (y compris des scans biométriques) et sont associés à un réseau interne séparé de l'Internet public.

Profil sectoriel : Entreprise de vente au détail sur Internet

Notre dernier exemple provient d'Internet.

Vous avez sans doute entendu parler de certaines violations majeures dans des systèmes de vente au détail en ligne. Dans ce cas, l'utilisateur malveillant tente d'obtenir des données client pour les utiliser à des fins illégales. Les détaillants en ligne offrent généralement un accès réseau distant, assorti de très peu de restrictions, à leurs fournisseurs principaux, comme les services de carte de crédit. (Dans certains cas, ces fournisseurs ont pratiquement les mêmes droits d'accès que les employés). Il s'agit là du premier signal d'alarme. Le deuxième est un manque de séparation entre les composantes du réseau. En d'autres termes, lorsqu'un utilisateur accède au réseau, il peut explorer facilement les serveurs de l'organisation qui ont été piratés.

Nous avons connaissance de plusieurs cas dans lesquels les pirates ont accédé à distance aux serveurs de l'entreprise ciblée grâce à leurs contacts auprès des fournisseurs. Une fois dans le système, le pirate tente de se faire passer pour un fournisseur, se familiarise avec les systèmes et tente de pirater les plus critiques d'entre eux qui renferment les données financières ou les comptes ayant accès à ces données. Autrement dit, les utilisateurs malveillants ont piraté une entreprise pour accéder aux données de l'un de ses partenaires.

Le stock des entreprises de vente au détail victimes de telles attaques peut subir une importante perte de valeur dans la semaine qui suit la violation. Par ailleurs, les entreprises mises en danger sont parfois condamnées par l'État à payer de lourdes amendes, s'élevant parfois à des milliards d'euros, principalement dans les secteurs d'activité régulés (et donc soumis à des obligations de conformité). En outre, les amendes et procès peuvent être utilisés au détriment d'une entreprise considérée comme le maillon faible qui a permis l'attaque. Certaines entreprises souscrivent des assurances couvrant les failles de sécurité.

Achat de solutions de protection

Le meilleur moyen d'éviter les piratages via une connexion à distance est d'interdire, purement et simplement, tout accès distant. Toutefois, cette démarche reste impensable pour de nombreuses entreprises, notamment dans les secteurs des services en ligne et de la vente au détail.

Voici quelques options plus sécurisées pour autoriser vos fournisseurs à accéder à votre réseau :

Publication via Azure : déplacez certains scénarios d'usage internes, comme l'accès à l'interface web et les bases de données principales, vers une solution PaaS (platform as a service) fiable dans le cloud. Le scénario d'usage dans le cloud peut être conservé sur le réseau interne, mais soumis à un niveau d'accès minimal, où seules les données nécessaires sont accessibles. Cette méthode permet de restreindre à la fois le nombre d'utilisateurs disposant d'un accès direct au réseau d'un client et les droits d'accès d'un utilisateur au sein du réseau en limitant l'accès aux ressources PaaS uniquement.

Multi-factor authorization (MFA) : exige une vérification supplémentaire de la part des utilisateurs, sans se contenter d'un nom d'utilisateur et d'un mot de passe. Par exemple, l'utilisateur peut confirmer son identité via un appel téléphonique ou un SMS.

Migration depuis un serveur de connexion Bureau à distance (CBD) vers des machines virtuelles dans Azure : l'utilisation de machines virtuelles vous permet de conserver des mots de passe uniques pour les différentes parties du serveur et de contrôler ainsi l'accès aux informations.

Conclusion

Protection, détection, réaction

Protection, détection, réaction

Êtes-vous prêt à améliorer la sécurité de votre entreprise ? Nous vous recommandons une approche exhaustive. Essayez de comprendre comment les utilisateurs malveillants arrivent généralement à leurs fins. Vous ne devez plus voir les attaques comme une éventualité, mais comme une certitude. Les failles à long terme dans la sécurité des systèmes de l'entreprise ne sont pas rares ; détectez-les et prenez les mesures nécessaires pour réduire le risque. Sachez comment réagir rapidement et efficacement à une attaque ciblée.

Nous avons subdivisé notre stratégie en trois étapes :

Étape 1 : Protection.
Adoptez une approche favorisant la gestion des risques et la séparation des privilèges. Posez-vous les questions suivantes :

- Cette personne a-t-elle réellement besoin d'accéder à ces données ?
- Quel est l'emplacement exact de mes données ?
- Quels sont les utilisateurs qui y ont accès ?
- Les règles de conformité applicables sont-elles toutes respectées ?
- Mes logiciels sont-ils à jour ?

Étape 2 : Détection.
Partez du principe que vous allez être victime de violations. Soyez méfiant. Posez-vous les questions suivantes :

- Comment la faille sera-t-elle détectée ?
- Disposons-nous des outils nécessaires pour détecter une défaillance ?
- Disposons-nous des outils nécessaires pour analyser une défaillance ?

Étape 3 : Réaction.
Vérifiez que vous avez établi une procédure de réaction configurée selon les bons éléments déclencheurs. Posez-vous les questions suivantes :

- Quelle sera notre réaction en cas de violation ?
- Comment allons-nous gérer les préjudices subis par nos ressources et notre réputation ?
- Avons-nous établi un plan de communication avec les clients ?
- Quels enseignements faut-il tirer d'un tel événement ?

Microsoft s'engage à protéger la sécurité et la confidentialité de vos données et systèmes. Pour en savoir plus sur les bonnes pratiques en matière de cybersécurité, de protection des données, de contrôle et de conformité au sein de votre entreprise, consultez le site www.microsoft.com/trustedcloud.

L'équipe Plateforme de confiance souhaite remercier Bruce Cowper, Kasia Kaplinska, Matt Kemehar, IB Terry et Yvette Waters pour le temps, les connaissances et le talent qu'ils ont consacré à l'élaboration du présent livre blanc.