Ressource de Petri IT Knowledgebase
Une propriété de BWW Media Group

Document technique de Petri
9 août 2022

Les plus grands défis pour les professionnels de la sécurité informatique en 2022

Survol

La cybersécurité est LA priorité pour les professionnels de l'informatique depuis déjà plusieurs années. Malgré cela, nous observons une augmentation fulgurante de la fréquence des attaques par maliciel, du piratage, et des failles de cybersécurité qui visent des cibles importantes.

Chaque année, les cyberattaques deviennent de plus en plus sophistiquées, dommageables et – vous l'aurez deviné – coûteuses. Protéger les données sensibles des organisations contre ces attaques constitue donc la priorité nº 1 pour les professionnels informatiques en ce moment. Examinons en détail quelques-uns des plus grands défis auxquels sont confrontés les professionnels de la sécurité des TI d'aujourd'hui.

Rançongiciel

Les rançongiciels constituent sans l'ombre d'un doute un des plus grands dangers pour la sécurité informatique des entreprises, quels que soient leur taille et leur secteur d'activité. Ceux-ci peuvent paralyser une entreprise en chiffrant ses données et services essentiels, les rendant ainsi inutilisables jusqu'au paiement d'une rançon ou jusqu'au moment où l'entreprise en question est en mesure de réhabiliter ses données.

Avec le temps, les rançongiciels gagnent en sophistication, en efficacité et en accessibilité pour les pirates. Les cybercriminels profitent désormais de fournisseurs RaaS pour créer des rançongiciels avec très peu de connaissances techniques ou d'expertise.

Une étude menée par la firme de sécurité Sophos a révélé que **66 % des organisations ont été affectés par un rançongiciel en 2021. Il s'agit d'une hausse de 37 % par rapport à 2020.** L'étude a également démontré que les montants extorqués ont augmenté durant la même période. En effet, la rançon moyenne avoisine les 812 360 $ US, soit une augmentation de 480 % par rapport à 170 000 $ US en 2020.

Même si une organisation décide de ne pas payer, l'attaque entraîne tout de même des coûts substantiels. Les coûts moyens associés à l'interruption des opérations et la perte de revenus s'élèvent à 1,4 M$. La durée moyenne pour se remettre sur pied à la suite d'une attaque de rançongiciel est d'un mois.

L'hameçonnage et le piratage psychologique

L'hameçonnage et le piratage psychologique sont deux des méthodes les plus utilisées pour disséminer des rançongiciels. Elles sont particulièrement efficaces puisqu'elles exploitent des faiblesses humaines, plutôt que matérielles. Des données de l'entreprise Veeam révèlent que 44 % des infections par rançongiciel proviennent de courriels d'hameçonnage et de liens malicieux trouvés sur des sites Web. Il est effectivement beaucoup plus facile de duper des gens pour qu'ils cliquent sur des liens infectés que de tromper un système de sécurité doté de plusieurs niveaux de défense.

Qui est vulnérable?

Une protection efficace contre les rançongiciels doit comporter :

1. De la formation pour les utilisateurs finaux
2. Des mises à jour logicielles régulières
3. Des procédures de sauvegarde de données fiables et sécuritaires
4. Une protection des comptes privilégiés

La formation des utilisateurs finaux contribue à réduire les risques d'exposition en informant les utilisateurs à propos des dangers à éviter.

La restauration de sauvegardes s'avère être la solution la plus efficace de se remettre d'une attaque par rançongiciel. Le rapport Sophos State of Ransomware 2022 indique que 73 % des organisations ont employé cette méthode pour restaurer leurs données chiffrées. Les professionnels de la sécurité informatique doivent non seulement s'assurer que leurs sauvegardes sont actualisées et fonctionnelles, mais aussi qu'elles sont inaltérables, protégées et incorruptibles par les rançongiciels.

Les mises à jour sont cruciales pour la protection des entreprises contre les failles connues.

Et pour finir, la dissémination des attaques par rançongiciel peut être endiguée en protégeant et en **limitant l'accès aux comptes privilégiés.**

Vulnérabilités de chaînes d'approvisionnement

Avant 2022, les vulnérabilités de chaînes d'approvisionnement n'étaient pas encore considérées comme un facteur de risque important pour la sécurité. Cependant, à la suite des attaques sur SolarWinds en décembre 2020 et sur Kaseya en juin 2021, les professionnels de la sécurité informatique ont définitivement pris conscience des dégâts que peuvent causer les vulnérabilités de chaînes d'approvisionnement.

Ces incidents prouvent que les attaques très sophistiquées deviennent monnaie courante. L'attaque sur SolarWinds fut menée par des acteurs étatiques qui ont exploité une vulnérabilité d'un système populaire d'analyse de performances TI nommé ***SolarWinds Orion.*** En utilisant une porte dérobée du nom de Sunburst, les cybercriminels ont pu accéder aux systèmes de **plus de 30 000 clients et partenaires de SolarWinds** (incluant les départements de la trésorerie, du commerce et de la sécurité intérieure des États-Unis, en plus d'autres grandes entreprises telles que : Intel, VMware et Cisco).

SolarWinds a dû créer un correctif pour réparer la faille avant d'entreprendre une refonte importante de ses mesures de sécurité afin d'empêcher ce genre d'attaques à l'avenir.

Kaseya VSA

La brèche de Kaseya a entraîné des conséquences similaires à la suite de l'attaque sur le logiciel de gestion TI Kaseya VSA (Administrateur Système Virtuel). Le VSA est utilisé pour gérer des réseaux, des systèmes et des infrastructures TI. Il est également populaire chez les fournisseurs de services gérés (*managed service providers ou MSP*) qui s'en servent pour gérer à distance des systèmes TI pour leurs clients.

Le marché des fournisseurs de services gérés a explosé durant la pandémie de Coronavirus, en même temps que le travail à distance. **Les failles que comportent les outils des MSP sont difficilement détectables et défendables pour leurs clients.** Une vulnérabilité permettant de contourner l'authentification dans Kaseya VSA a permis à la bande de cybercriminels REvil de distribuer des charges malveillantes par l'intermédiaire d'hôtes gérés par le logiciel. Cette charge a ensuite déversé des rançongiciels aux points de terminaisons des clients.

Selon Kaseya, l'impact de cette brèche s'est étendu à plus de 50 clients directs ainsi qu'à entre 800 et 1500 autres entreprises. Par la suite, les gouvernements russes et américains ont travaillé à ce que les sites Web de REvil disparaissent de l'Internet. Kaseya a ensuite annoncé qu'un correctif était déjà conçu pour le logiciel VSA et que l'entreprise disposait maintenant d'un outil de déchiffrement universel qu'elle avait utilisé pour restaurer les données de ses clients.

Mise en lumière des vulnérabilités des chaînes d'approvisionnement

Des attaques ambitieuses visant des acteurs importants ont aidé à exposer les vulnérabilités des chaînes d'approvisionnement. Ce type d'attaque peut être difficile à détecter et la protection contre de telles menaces nécessite l'apport de plusieurs entreprises. Vous devez faire en sorte que tous vos partenaires et fournisseurs se conforment à des pratiques de sécurité optimales, en plus de mettre tous vos logiciels à jour avec les derniers correctifs de sécurité.

Gestion des accès à distance

La gestion des accès à distance a toujours été une grande préoccupation des professionnels de la sécurité informatique. Le protocole RDP est un service standard disponible avec toutes les versions de Windows. Il permet aux utilisateurs ainsi qu'aux administrateurs et professionnels TI de se connecter à un poste à distance, lui-même connecté sur un réseau.

Il en va de même pour les systèmes de connexion à distance Linux qui, eux, emploient souvent VNC ou un de ses dérivés en source libre tels que RealVNC, TightVNC ou TigerVNC pour fournir ce type d'accès.

RDP et VNC ont toujours été couramment utilisés pour la gestion à distance. En revanche, l'augmentation du travail à distance engendrée par la pandémie a poussé l'usage de ces technologies à un niveau supérieur. Malheureusement, les services d'accès à distance sont souvent ciblés pour des attaques sur le périmètre réseau. Les serveurs accessibles via Internet, qu'ils fonctionnent avec Windows ou Linux, sont souvent confrontés à des tentatives d'attaque par force brute (une tactique souvent associée avec les rançongiciels).

Mouvement latéral utilisant des identifiants de comptes compromis

Les mots de passe faibles ainsi que les identifiants compromis font partie des méthodes les plus utilisées par les pirates et les cybercriminels pour infecter vos technologies d'accès à distance. Une fois votre réseau infecté, les pirates peuvent se servir des technologies d'accès à distance pour accéder aux autres systèmes sur le réseau.

Une solution de gestion des accès à distance, telle que ***Remote Desktop Manager*** de Devolutions, dispose de fonctionnalités de gestion de mots de passe, de la sécurité et des accès à distance avec RDP ou VNC. Elle vous permet d'unifier, de centraliser et de contrôler l'accès à tous les systèmes de votre réseau.

Les solutions de gestion des accès à distance améliorent la sécurité et la protection du périmètre réseau grâce à :

- **Leur politique de mots de passe forts** - La sécurité commence par s'assurer que tous vos utilisateurs se servent d'un mot de passe fort. Les mots de passe forts difficiles à deviner constituent la première ligne de défense pour vos données sensibles, en plus d'offrir une protection robuste contre les attaques par force brute et pulvérisation de mot de passe.

- Les outils comme ***Remote Desktop Manager (RDM)*** de Devolutions font en sorte que les mots de passe de vos bureaux à distance soient solides en appliquant des politiques de longueur, de complexité, et d'historique de réutilisation des mots de passe. Un générateur et un analyseur de mots de passe facilitent la création de mots de passe forts pour les utilisateurs.

- **Leur gestion centralisée des mots de passe** - les outils de gestion des accès à distance stockent de manière sécuritaire tous les mots de passe de vos connexions à distance au même endroit. Qui plus est, ils empêchent les utilisateurs d'inventer leurs propres méthodes farfelues de stockage de mots de passe. RDM peut stocker tous les mots de passe d'une entreprise dans une base de données chiffrée sur place. Ce faisant, les utilisateurs bénéficient d'un accès rapide à leurs identifiants de connexion ainsi que d'une façon de partager de l'information entre équipes. Les usagers de RDM n'ont donc plus besoin de stocker leurs mots de passe et leurs identifiants de connexion dans des fichiers non sécurisés ou sur des petits bouts de papier.

- **Leurs sessions à distance sécurisées sur demande** - Les connexions à distance peuvent être chiffrées, ce qui les protège contre les attaques de « l'homme du milieu ». Vous pouvez régler la sécurité des connexions RDP sur ***élevée***. Les VNC peuvent être réglés sur 256-bit AES dans les paramètres de configuration du serveur VNC.

- **Leur suivi des sessions en temps réel** - Lorsqu'il est question d'accès à distance, il est crucial pour la sécurité et le respect des normes de pouvoir garder un œil sur qui accède à quoi, quand et pour combien de temps. Une surveillance régulière permet de détecter les activités suspectes telles que les tentatives de connexion non autorisées. Une solution de gestion des accès à distance offre également une vision centralisée de toutes les activités de bureau à distance de votre entreprise. RDM peut effectuer un suivi du système de connexion, des dates, du temps, des utilisateurs et des postes pour toutes les connexions à distance.

Accès privilégiés

La gestion des accès privilégiés et la réduction des risques associés aux comptes privilégiés sont deux des enjeux les plus importants pour les professionnels de la sécurité des TI. Selon le rapport de Verizon (DBIR) de 2022, ***« 82 % des brèches de l'année incluaient une interaction humaine. Qu'il s'agisse d'identifiants compromis, d'hameçonnage, d'abus ou simplement d'erreur, le facteur humain continue de jouer un rôle de premier plan dans les brèches et les incidents de cybersécurité ».***

La protection des identifiants est essentielle pour assurer la défense de vos réseaux et systèmes, surtout lorsque ces informations permettent d'accéder à des comptes privilégiés. Les cybercriminels exploitent la vulnérabilité des accès aux comptes privilégiés pour infiltrer des réseaux, accéder à des systèmes sensibles et dérober des informations confidentielles.

Les comptes privilégiés peuvent causer des dégâts plus importants aux entreprises que ceux qui ne disposent que de droits d'utilisateur standards ou d'accès pour invités externes. En plus des données, les comptes privilégiés peuvent accéder aux services et aux configurations système.

D'après Microsoft, **les accès privilégiés devraient être LA priorité de sécurité de toutes les organisations.** L'implémentation du principe de moindre privilège, selon lequel les comptes ne disposent que des droits nécessaires à leurs fonctions, constitue une des manières les plus efficaces de limiter l'exposition des comptes privilégiés.

Gestion des accès privilégiés

Les solutions de gestion des accès privilégiés (PAM) telles que ***Devolutions Server*** limitent les risques en protégeant l'accès à des ressources vitales. En effet, les solutions PAM surveillent et contrôlent les accès à des comptes hautement privilégiés. En plus de réduire l'incidence de cybermenaces externes, les solutions PAM peuvent également empêcher les menaces internes comme des abus – accidentels ou non – de comptes privilégiés.

Pour vous défendre de ce type de menaces, les solutions de gestion des accès privilégiés vous permettent de limiter, révoquer et surveiller les accès.
Une solution PAM protège les identifiants d'un compte dès sa création. Une solution de stockage des identifiants ou un système de gestion des mots de passe sert à stocker les informations d'authentification des comptes privilégiés afin d'empêcher les vols ou la mauvaise gestion de ces derniers.

Pour accéder à ces comptes privilégiés, les utilisateurs PAM doivent utiliser leur solution PAM pour s'identifier. À chaque fois que quelqu'un se connecte à un de ces comptes, les solutions PAM enregistrent la session et effectuent un suivi des actions.
Un rapport détaillé d'un accès à un compte privilégié inclut :

- le nom de l'utilisateur;
- le moment du début de la session;
- la durée de la session;
- et les opérations effectuées avec ces identifiants.

Les solutions PAM fournissent aussi des informations à propos de vos comptes privilégiés qui pourraient vous surprendre. Par exemple : vous pourriez découvrir combien de comptes privilégiés n'expirent jamais, ou encore combien d'entre eux existent toujours alors qu'ils auraient dû être supprimés.

Bien que certaines entreprises considèrent que les solutions PAM sont compliquées et difficiles à implémenter, elles facilitent la gestion et la surveillance des utilisateurs privilégiés. La gestion des accès privilégiés garantit la sécurité des segments les plus importants de votre infrastructure TI, et ce, malgré leur évolution constante.

Les nouveaux défis pour les années à venir

En plus des défis auxquels sont confrontés les professionnels de la sécurité informatique en 2022, de nombreuses nouvelles épreuves vont certainement prendre de l'ampleur dans les prochaines années. **L'IdO (Internet des objets) se transforme rapidement en un des plus grands défis pour la sécurité informatique pour les années à venir.** Toutes sortes d'appareils IdO sont rapidement déployés pour combler des besoins informatiques tels que la vérification de procédé, le calcul en périphérie de réseau et même la domotique.

L'Internet des objets

Les appareils IdO ne nécessitent pas d'interventions humaines pour leur fonctionnement. Ils utilisent des capteurs pour collecter, analyser et traiter l'information. Cependant, cette automatisation peut entraîner des risques importants pour la sécurité puisque les appareils IdO peuvent être compromis et passer inaperçus. Les données, serveurs et services (incluant les services infonuagiques) sont bien souvent partagés entre appareils IdO, ce qui augmente les risques de sécurité de façon exponentielle.

Puisque les appareils IDO sont autonomes par nature, il est important d'effectuer les dernières mises à jour de sécurité et du système d'exploitation pour s'assurer que ces appareils demeurent sûrs. Il est également primordial d'utiliser des mots de passe forts ou un processus d'authentification multifacteur dès que possible pour tous les appareils connectés.

La sécurité pour Mac et Linux

Certains problèmes de sécurité pour Mac et Linux vont inévitablement se présenter. Bien que l'omni-présence des systèmes Microsoft en fasse des cibles de choix pour les maliciels, les cybercriminels se concentrent de plus en plus sur les systèmes Linux et Mac.

Un rapport de Crowdstrike traitant les données sur les cyberattaques recueillies en 2021, **enregistre une augmentation des attaques visant les systèmes Linux de 35 % par rapport à 2020.** L'utilisation d'ordinateurs Mac dans les entreprises est également plus répandue, surtout en raison de l'adoption généralisée de portables. Selon IDC, les **appareils macOS étaient utilisés par 23 % des entreprises américaines en 2021.** Cette augmentation de 17 % par rapport à 2019 signifie qu'ils constituent désormais une cible plus alléchante pour les pirates.

Encore une fois, des mises à jour logicielles régulières et des mots de passe forts doivent être considérés comme des mesures de base pour la sécurité de ces plateformes. La protection de tous les comptes privilégiés limite l'exposition à de potentielles attaques sur Linux et Mac.

La sécurité est prioritaire pour les professionnels de l'informatique

Il ne fait aucun doute que la sécurité demeurera l'une des plus grandes préoccupations des professionnels de l'informatique pour un bon moment. Affronter les épreuves relatives aux rançongiciels, aux attaques sur les chaînes d'approvisionnement, à la gestion des accès privilégiés ainsi qu'aux accès privilégiés nécessite un habile mélange de formation, de pratiques optimales et de solutions de sécurité telles que Devolutions Remote Access Management et le support PAM de Devolutions Server. La gestion de l'accès à distance fait en sorte que vos utilisateurs aient des mots de passe forts gérés de façon sécuritaire et centralisée. Les solutions PAM, quant à elles, servent à protéger l'accès à vos comptes privilégiés qui disposent des niveaux d'accès les plus profonds de l'infrastructure de votre entreprise.

Informations supplémentaires

Pour plus d'informations concernant les enjeux et les solutions qui touchent les PME, veuillez consulter le Portrait de la cybersécurité dans les PME pour 2020-2021.

Devolutions