opentext™ | Cybersecurity

Positionnement de la solution

Zero Trust : repenser la sécurité

La cybersécurité traditionnelle s'est concentrée sur la lutte contre les intrusions sur les réseaux d'entreprise, un objectif atteint principalement grâce aux pare-feu qui surveillent le trafic entrant et bloquent les paquets de données suspects. Les pare-feu nouvelle génération actuels ont évolué pour offrir des capacités plus avancées, telles que le protocole SSL (Secure Socket Layer) pour protéger les transactions et inspecter minutieusement les paquets avant que les données ne soient livrées à l'entreprise.

Bien que les pare-feu soient toujours un élément essentiel de la cyberdéfense, il est important de se rappeler qu'ils ont été conçus pour protéger un réseau unique. À l'ère du cloud, les informations circulent à une vitesse fulgurante vers et depuis une multitude d'applications, de réseaux de partenaires et des centaines de périphériques distants se connectant à votre réseau via des milliers de points d'accès. Certains de ces périphériques et applications disposent de contrôles de sécurité insuffisants. Un nombre inquiétant ne dispose d'aucun contrôle de sécurité.

L'environnement multi-cloud et multi-périphériques actuel est une aubaine pour les pirates informatiques qui bénéficient d'un nombre croissant de points d'entrée et sont armés d'outils logiciels sophistiqués pour détecter les vulnérabilités sur Internet. Une fois que les pirates sont entrés sur votre réseau, ils sont souvent libres de leurs mouvements et ont accès à vos données clients protégées, à votre propriété intellectuelle ou à vos contrôles réseau.

L'environnement multi-cloud et multi-périphériques actuel est une aubaine pour les pirates informatiques qui bénéficient d'un nombre croissant de points d'entrée et sont armés d'outils logiciels sophistiqués pour détecter les vulnérabilités sur Internet.

Ils peuvent se déplacer librement, car les défenses traditionnelles se sont concentrées sur le renforcement de la barrière entre votre réseau et le monde extérieur, la coquille dure, tout en ignorant pratiquement le « centre névralgique ». Il ne s'agit pas d'un bogue, mais d'une fonction conçue pour permettre aux utilisateurs internes à l'entreprise de se déplacer plus facilement et de trouver ce dont ils ont besoin. Une fois que quelqu'un a saisi un mot de passe, voire un second facteur d'authentification, il obtient facilement ce qu'il veut.

Mais, dans le monde d'aujourd'hui, l'authentification multi-critères à elle seule ne suffit pas à empêcher les intrus d'entrer. De plus, les employés disposant d'un accès illimité aux données de l'entreprise, une fonction courante des applications héritées, facilitent encore davantage le travail des pirates informatiques, tout en offrant des tentations aux utilisateurs internes mécontents.

Selon le rapport d'enquête 2019 sur les violations de données (Data Breach Investigations Report) de Verizon, 34 % des violations de données sont commises par des utilisateurs internes. Cette proportion atteint 60 % dans le secteur de la santé et 36 % dans le secteur des services financiers, des secteurs contenant des informations particulièrement précieuses pour les voleurs. Selon le Ponemon Institute, le coût moyen d'une violation est passé à 3,92 millions de dollars.

Les enjeux étant plus élevés que jamais, il est temps d'adopter une nouvelle approche de la cybersécurité, une approche basée sur la réalité actuelle du multi-cloud et de l'accès à tout moment et en tout lieu. Cette approche est appelée Zero Trust.

Qu'est-ce que l'approche Zero Trust ?

Vous avez probablement déjà entendu le terme « Zero Trust », mais sa signification peut vous paraître floue. En effet, il ne s'agit pas d'une technologie unique (même si elle est parfois décrite comme telle), mais d'un ensemble d'activités qui agissent ensemble pour vous offrir la meilleure protection possible lorsque vos informations transitent entre des périphériques, des applications et des emplacements dans le monde entier.

Voici un résumé de quelques-unes des caractéristiques les plus importantes d'un système Zero Trust. Il n'est pas nécessaire de disposer de toutes ces technologies ni de les adopter toutes simultanément. Gardez simplement à l'esprit qu'elles fonctionnent mieux de concert, il est donc important de tout synchroniser au fur et à mesure.

Contrôles d'accès rigoureux

Le concept le plus fondamental de l'approche Zero Trust est peut-être le contrôle d'accès, non pas sur la base générale d'un utilisateur interne versus un utilisateur externe, mais en fonction des besoins spécifiques des utilisateurs. C'est ce que l'on appelle le principe du privilège minimal : donnez uniquement accès aux outils dont les employés, partenaires, sous-traitants et autres personnes utilisant votre réseau ont besoin pour travailler, ni plus ni moins. Le système d'accès doit être géré de manière centralisée et dynamique, car les personnes et les organisations changent.

Si Greg commence en tant que comptable, il aura besoin d'accéder aux transactions de l'entreprise. S'il est promu au poste de contrôleur, il aura besoin d'un accès plus large aux données financières et aura besoin de consulter le travail des personnes qu'il supervise. S'il est affecté au bureau de Londres, il aura besoin d'informations différentes et une grande partie de son ancien accès devra être révoqué. Lorsqu'il prendra sa retraite, il aura encore besoin de consulter ses prestations, mais tout autre accès devra lui être interdit immédiatement.

Avec l'approche Zero Trust, toutes ces actions sont basées sur des règles et automatisées pour garantir une mise en oeuvre immédiate. En effet, un accès non autorisé peut semer le chaos.

Demandez simplement à Target, qui a perdu 162 millions de dollars américains après que les références d'un sous-traitant CVCA ont été utilisées pour voler les numéros de carte de crédit et les informations personnelles de 41 millions de clients. Ou à Home Depot, où les références d'un fournisseur ont été utilisées pour récupérer 56 millions de numéros de carte de débit et de crédit, ce qui a coûté 180 millions de dollars américains à l'entreprise.

Il n'y a pas que les sous-traitants qui sont à tenir pour responsables. Dans une étude réalisée par Dell, 72 % des employés ont admis qu'ils partageraient des informations sensibles, confidentielles ou réglementées sur l'entreprise avec des personnes extérieures si un responsable leur demandait, s'ils pensaient que cela les aiderait à faire leur travail ou pour une autre raison. Alors que certains estimaient avoir le devoir de protéger les informations confidentielles, l'évolution des directives de sécurité de leur entreprise les a fait douter de la méthode pour y parvenir.

L'accès des anciens employés peut également entraîner une catastrophe pour de nombreuses entreprises. Une récente étude a révélé qu'un tiers des anciens employés ont toujours accès aux dossiers et aux documents de leur ancienne entreprise. Sans un contrôle et une automatisation centralisés, il est très facile pour un service informatique surchargé de négliger ce problème.

Une seule personne mal intentionnée peut semer le chaos, voler de la propriété intellectuelle ou supprimer des comptes administratifs et des documents protégés.

Vous avez probablement déjà entendu le terme « Zero Trust », mais sa signification peut vous paraître floue. En effet, il ne s'agit pas d'une technologie unique (même si elle est parfois décrite comme telle), mais d'un ensemble d'activités qui agissent ensemble pour vous offrir la meilleure protection possible lorsque vos informations transitent entre des périphériques, des applications et des emplacements dans le monde entier.

Pour enfoncer le clou, votre entreprise peut être tenue responsable. Au Royaume-Uni, après qu'un ancien employé a publié des informations sur les salaires de près de 100 000 employés sur un site Web de partage de fichiers, un juge a statué que même si l'entreprise n'avait pas mal géré les données elle-même, elle était responsable par procuration de la violation.

Protéger les informations essentielles relève de la responsabilité de l'entreprise et avec tous les canaux par lesquels transitent vos données aujourd'hui, personne ne peut les suivre manuellement. Un système automatisé de gestion des identités et des accès sur mesure constitue la base de toute sécurité et est l'un des préceptes au coeur de l'approche Zero Trust.

Protéger les informations essentielles relève de la responsabilité de l'entreprise et avec tous les canaux par lesquels transitent vos données aujourd'hui, personne ne peut les suivre manuellement. Un système automatisé de gestion des identités et des accès sur mesure constitue la base de toute sécurité et est l'un des préceptes au coeur de l'approche Zero Trust.

Gestion rigoureuse des privilèges

Un autre élément crucial de l'approche Zero Trust est la gestion rigoureuse des comptes privilégiés, ceux qui peuvent accéder à vos informations les plus sensibles ou apporter des modifications aux systèmes et données importants.

Étant donné que ces comptes gèrent les clés du royaume, ils sont particulièrement attrayants pour les cybercriminels. Selon Forrester, 80 % des violations de sécurité impliquent l'utilisation de références de comptes privilégiés.

Bien entendu, les pirates peuvent dès le départ échouer à compromettre l'un de ces précieux comptes. Mais si les contrôles d'accès internes sont insuffisants, ils peuvent se frayer un chemin jusqu'au sommet.

C'est pourquoi un compte privilégié doit exiger des facteurs d'authentification supplémentaires au fur et à mesure que l'importance des informations auxquelles il accède augmente. Lorsqu'un compte privilégié traite les données sensibles des clients, résout un problème de réseau ou se livre à une activité potentiellement dangereuse, l'utilisateur doit être surveillé en temps réel et ne doit jamais se voir accorder d'autorisations générales. Dans certains cas, les mots de passe pour une tâche spécifique doivent être révoqués dès que cette dernière est terminée.

Ces précautions supplémentaires garantissent non seulement que les titulaires de comptes privilégiés se comportent correctement, mais elles permettent également d'empêcher les pirates informatiques de se déplacer dans l'entreprise. La plupart des criminels recherchent des cibles faciles, si leurs attaques sont déjouées à chaque fois, ils seront contrariés et passeront à autre chose.

Monitoring des activités

En coordonnant votre système de gestion des identités et des accès, votre centre de sécurité peut détecter des activités suspectes en se basant non seulement sur le trafic réseau, mais aussi sur l'identité, le périphérique, l'emplacement et le comportement des utilisateurs internes, en émettant des alertes ou en coupant l'accès si, par exemple, un employé travaillant à New York se connecte inopinément depuis Moscou.

Les outils de machine learning d'aujourd'hui vont encore plus loin. Ils détectent si les employés visitent des sites Web étranges à des heures irrégulières, téléchargent des informations sensibles qu'ils n'utilisent pas en temps normal, ou tapent selon un schéma différent de leur rythme habituel. La création d'alertes automatiques pour les événements anormaux vous permet de répondre beaucoup plus rapidement à ces événements, d'éviter une violation ou d'en limiter sa portée.

Selon le Ponemon Institute, plus vite une violation est détectée, moins elle crée de dégâts. Le temps moyen nécessaire pour identifier et contenir une violation est de 279 jours, mais celles qui sont arrêtées en moins de 200 jours coûtent 37 % moins cher que les autres violations.

Le Ponemon Institute affirme que les logiciels de sécurité dotés de contrôles automatisés sont particulièrement efficaces. Le coût des violations pour les entreprises ne disposant pas d'une sécurité automatisée était 95 % plus élevé que celui des entreprises dotées de systèmes automatisés entièrement déployés.

Les logiciels d'IA s'améliorent constamment et certains des derniers produits peuvent vous protéger quasiment en temps réel.

En plus de surveiller le comportement des utilisateurs, un centre de sécurité Zero Trust protège en permanence l'entreprise des dernières menaces et fournit des alertes pour corriger les vulnérabilités, aidant ainsi les organisations à éviter des attaques spectaculaires comme l'attaque du logiciel de rançon WannaCry.

Classification des données significatives

La classification complète des données est fondamentale pour l'approche Zero Trust. Ce n'est que lorsque vous savez ce que vous détenez et où cela se trouve que vous pouvez élaborer les bonnes politiques pour le protéger.

Pour bien comprendre vos informations, vous ne pouvez pas vous contenter de balises META, en particulier pour les données non structurées telles que les vidéos, les e-mails, les enregistrements audio, les images et les présentations PowerPoint.

Les balises sont simplement des raccourcis créés par des individus pour les aider à trouver ce dont ils ont besoin, mais elles peuvent ne pas fonctionner pour d'autres personnes recherchant les mêmes données à d'autres fins. Par exemple, un responsable marketing peut étiqueter une présentation « Campagne des guerriers de la route », ne laissant aucun indice sur les informations qu'elle contient concernant les produits de l'entreprise.

Les logiciels d'intelligence artificielle et de machine learning peuvent afficher le contenu des données non structurées, leur donner un sens et les classer en fonction de leur signification et de leur valeur en matière de sécurité. En plus d'aider chacun à trouver ce dont il a besoin, ils identifient les données sensibles non protégées qui se cachent dans des emplacements inattendus et les transfèrent vers un emplacement plus sûr.

Le marquage logiciel facilite également la mise en conformité, en révélant instantanément aux auditeurs des informations qu'ils passeraient autrement des heures à rechercher.

Les logiciels d'IA s'améliorent constamment et certains des derniers produits peuvent vous protéger quasiment en temps réel. À titre expérimental, un magasin a installé une caméra à l'extérieur de son entrée, filmant les curieux qui passaient devant. La caméra était dotée d'une technologie de reconnaissance faciale, mais le magasin ne pouvait l'utiliser que sur les personnes qui avaient donné leur accord. Lorsque les gens s'approchaient, on leur demandait la permission d'utiliser leurs images, la technologie de reconnaissance vocale répondant à leurs réponses. En fin de compte, la caméra a réussi à flouter les images des 99 % qui n'avaient pas donné leur consentement dès la diffusion de la vidéo.

Les logiciels de reconnaissance d'images apportent également une valeur métier en temps réel. Ils peuvent être utilisés pour surveiller un chantier afin de détecter les activités dangereuses et les infractions, ou pour avertir une usine chimique si un camion non autorisé s'approche.

La confiance à l'ère du cloud

Les services cloud sont extrêmement précieux, mais ils ouvrent également la voie à un nouvel ensemble de vulnérabilités. Télécharger vos données sur une application basée sur le cloud signifie que vous devez faire confiance à une entreprise tierce. Quel que soit le degré de fiabilité et d'éthique du fournisseur, il est possible qu'il soit piraté et que vos précieuses informations privées soient perdues.

Adopter une approche Zero Trust permet de tirer pleinement parti des services cloud sans renoncer à vos informations les plus sensibles. Grâce au chiffrement avec conservation du format, vous pouvez remplacer les noms de clients ou d'employés, les adresses, les numéros de carte de crédit et autres données sensibles par de fausses informations. Vous l'envoyez ensuite à l'application pour analyse. Tant que les informations sont saisies dans les champs appropriés et au bon format, l'application ne fait pas la différence. Vous obtenez toutes les analyses détaillées que vous souhaitez sans avoir à communiquer vos informations personnelles à l'application, même si vous pouvez toujours voir ces informations dans les résultats.

À mesure que la technologie de sécurité évolue, les chercheurs mettent au point d'autres techniques sophistiquées, comme la création de fausses applications et de faux serveurs pour attirer les attaquants, étudier leurs méthodes et les prendre sur le fait.

Alors que l'utilisation du cloud se développe et que les avancées technologiques créent de nouvelles vulnérabilités à grande échelle, la sécurité basée sur la protection d'un seul réseau n'a plus de sens. L'approche Zero Trust est un ensemble de procédures prospectives conçues pour identifier vos utilisateurs et vos informations avec la plus grande précision, vous aidant ainsi à préserver vos ressources tout en protégeant vos actifs les plus précieux, et ce, automatiquement et en temps réel.

Le meilleur des mondes de l'IoT

L'Internet des objets est à nos portes, et il s'accompagne d'un nombre stupéfiant de nouveaux points de lancement pour les cyberattaques. Les fabricants de produits IoT grand public courants, tels que les télévisions intelligentes, les webcams, les thermostats, etc., ont été négligents en matière de sécurité, ce qui facilite le piratage de ces appareils. Il n'a pas fallu longtemps pour que les pirates informatiques s'en rendent compte.

Au début, leur exploit le plus courant était de créer des armées d'appareils domestiques pour créer des botnets et organiser des attaques par déni de service sur les sites Web des entreprises. Le botnet le plus tristement connu est le botnet Mirai, qui a fait disparaître plusieurs sites Web à fort trafic en même temps, dont CNN, Twitter et Netflix.

Les attaques DDoS n'étaient que le début. Les pirates informatiques ont attaqué et pris le contrôle de tout, des voitures aux pompes à insuline, en passant par les stimulateurs cardiaques et les défibrillateurs, les babyphones et même les jouets.

Leur prochaine cible pourrait être les données d'entreprise. Gartner prédit qu'en 2020 il y aura 5,8 milliards d'entreprises et de produits automobiles connectés à Internet en circulation.

L'année dernière, des chercheurs ont créé un scénario montrant comment des pirates informatiques pouvaient exécuter une attaque latérale de l'IoT d'une entreprise en compromettant les caméras de sécurité et un routeur, une tâche relativement simple. À l'aide d'outils logiciels, ils pourraient alors théoriquement zoomer par-dessus les épaules des employés pour voir et enregistrer leurs informations de connexion. D'autres chercheurs ont découvert des vulnérabilités dans des imprimantes de bureau qui pourraient permettre aux voleurs de dérober des documents et des mots de passe.

L'IoT crée un nouvel univers de problèmes de sécurité. Ces problèmes ne sont pas uniquement dus au grand nombre de nouveaux périphériques de connexion. Ils sont également dus à la technologie qui rend leur fonctionnement possible. Bien que la technologie 5G offre un meilleur chiffrement et une meilleure vérification du réseau que la 4G, sa vitesse ultra-rapide signifie que les pirates informatiques qui accèdent à votre réseau parviendront à se déplacer en un rien de temps, à moins que vous ne disposiez de contrôles d'accès automatisés pour les arrêter.

Alors que l'utilisation du cloud se développe et que les avancées technologiques créent de nouvelles vulnérabilités à grande échelle, la sécurité basée sur la protection d'un seul réseau n'a plus de sens. L'approche Zero Trust est un ensemble de procédures prospectives conçues pour identifier vos utilisateurs et vos informations avec la plus grande précision, vous aidant ainsi à préserver vos ressources tout en protégeant vos actifs les plus précieux, et ce, automatiquement et en temps réel.

L'avantage d'OpenText Cybersecurity

Grâce à des décennies d'expérience dans le domaine de la sécurité des entreprises, OpenText™ dispose d'une connaissance approfondie de tous les aspects de l'approche Zero Trust. Nous pouvons jeter une nouvelle lumière sur vos collaborateurs et vos données, en vous présentant les meilleurs moyens de les protéger tout en travaillant avec vos solutions existantes pour les intégrer à un ensemble cohérent, actualisé et fonctionnel.

Pour en savoir plus, rendez-vous sur :
www.microfocus.com/fr-fr/cyberres

À propos de NetIQ par OpenText

NetIQ par OpenText fournit des solutions de sécurité qui aident les entreprises à gérer les identités et les accès des employés et des utilisateurs à l'échelle de l'entreprise. En fournissant un accès sécurisé, une gouvernance efficace, une automatisation évolutive et des informations exploitables, les clients OpenText peuvent renforcer la confiance dans leur stratégie de sécurité informatique sur les plates-formes cloud, mobiles et de données.

Pour en savoir plus, visitez la page d'accueil NetIQ par OpenText à l'adresse **www.cyberres.com/netiq**. Regardez des vidéos de démonstration sur notre chaîne YouTube NetIQ Unplugged à l'adresse **www.youtube.com/c/NetIQUnplugged**.

NetIQ fait partie de Cybersecurity, une ligne de produits d'OpenText.

Communiquez avec nous
www.opentext.com

opentext™ | Cybersecurity

OpenText Cybersecurity fournit des solutions de sécurité complètes pour les entreprises et les partenaires de toutes tailles. De la prévention à la détection, en passant par la réponse, la récupération, l'enquête et la conformité, notre plate-forme unifiée de bout en bout aide les clients à développer leur cyber-résilience via un portefeuille de sécurité global. Grâce à des informations exploitables issues de nos renseignements en temps réel et contextuels sur les menaces, les clients d'OpenText Cybersecurity bénéficient de produits hautement efficaces, d'une expérience conforme et d'une sécurité simplifiée pour les aider à gérer les risques métiers.

762-FR0021-005 | O | 12/23 |