okta

Checklist pour lutter contre les ransomwares

Trois étapes pratiques pour protéger votre entreprise des attaques de ransomware grâce à une approche Zero Trust centrée sur l'identité.

Commencer

Bien que les ransomwares ne datent pas d'hier, la transition rapide et généralisée vers une nouvelle culture du travail hybride qui s'étend au-delà du périmètre se traduit par une plus grande vulnérabilité des entreprises face aux attaques.

Selon le **rapport d'enquête de Sophos L'état des ransomwares 2021**, 37 % des entreprises ont déjà été victimes d'un ransomware cette année, tandis que le coût total moyen de la récupération après une attaque de ransomware a plus que doublé, passant de 761 106 dollars en 2020 à 1,85 million en 2021. Mais comment s'explique cette augmentation spectaculaire ?

En règle générale, on considère qu'une solution de sauvegarde efficace et une procédure de restauration bien rodée peuvent permettre de ne pas payer la rançon. Bien évidemment, nous avons tous entendu parler de cas où les sauvegardes elles-mêmes étaient infectées, mais ces cas restent marginaux. Les gangs spécialisés dans les ransomwares redoublent de créativité pour contourner les mesures de sécurité et rentabiliser leurs efforts.

SOPHOS
Cybersecurity evolved.

À présent, il n'est pas rare que les données soient volées avant d'être chiffrées, ce qui permet au cybercriminel de faire pression sur sa victime en la menaçant de divulguer publiquement ses informations. Une fois compromis, l'accès à un réseau peut être vendu à d'autres cybercriminels via un courtier d'accès, conduisant à d'autres attaques pour des motivations diverses. En cas d'attaque de ransomware sur la chaîne logistique, les cybercriminels peuvent exercer une pression sur les clients d'un fournisseur ciblé afin qu'eux-mêmes demandent à la victime de céder au chantage pour restaurer rapidement ses services.

L'information sur le lancement d'une attaque peut également être vendue à des courtiers financiers, qui pourraient vendre à découvert des actions de l'entreprise ciblée avant que le marché ne prenne connaissance de l'attaque. Aujourd'hui, avec le Ransomware-as-a-Service (RaaS), plus besoin d'une maîtrise technique approfondie. Ces plateformes mettent des technologies malveillantes complexes à la portée d'un public de cybercriminels plus large, pour des sommes relativement faibles. Le ransomware est donc devenu une entreprise criminelle agile, capable de s'adapter et offrant de nombreux débouchés pour quiconque souhaite tirer profit des failles technologiques. Alors, quelle est la solution ?

S'il n'existe pas de formule magique pour protéger votre entreprise des attaques de ransomware, ce guide explique comment une stratégie de sécurité Zero Trust axée sur l'identité peut vous aider à réduire les brèches de données exploitées par les cybercriminels.

Étape 1

Neutraliser les attaques de ransomware grâce à une authentification multifacteur adaptative performante

Lorsqu'il s'agit d'exposer les vulnérabilités de réseaux IT d'entreprise, les cybercriminels ont généralement l'embarras du choix. Les noms d'utilisateur et les mots de passe faibles sont facilement compromis par des techniques telles que le credential stuffing ou le password spraying, et font office de points d'entrée rapides pour les auteurs d'attaques de ransomware. Pourtant, les noms d'utilisateur et les mots de passe forts sont eux aussi vulnérables, en particulier lorsqu'ils sont la cible d'attaques de phishing intelligentes qui incitent les victimes à divulguer volontairement leurs identifiants.

Heureusement, **l'authentification multifacteur adaptative (Adaptive MFA)** est l'une des manières les plus efficaces de prévenir le piratage de comptes. Avec cette technologie, les accès sont octroyés selon des politiques d'accès contextuelles qui distinguent les comportements normaux et anormaux ainsi que les actions à faible risque et à haut risque des utilisateurs. Ces signaux sont souvent les premiers indicateurs d'une activité malveillante.

Si l'AMFA peut donc contribuer à bloquer l'accès initial des auteurs d'attaques de ransomware, une architecture holistique Zero Trust protège l'entreprise des éventuels déplacements latéraux des cybercriminels sur le réseau.

Euro Garages

Euro Garages* a récemment élaboré une nouvelle stratégie pour simplifier ses processus IT et offrir à ses 4 000 collaborateurs et 1 000 partenaires externes un accès fluide et sécurisé à toutes les applications professionnelles dont ils ont besoin pour travailler à distance. Grâce aux solutions Okta Single Sign-On et Okta Adaptive Multi-Factor Authentication, l'entreprise est parvenue à implémenter rapidement un modèle de sécurité Zero Trust pour protéger ses données au niveau individuel, tout en laissant les équipes libres d'utiliser les terminaux de leur choix. En plus d'augmenter la productivité des collaborateurs et de leur donner la possibilité de travailler où ils le souhaitent, les fonctionnalités de gestion des identités et des accès (IAM) de pointe d'Okta ont également aidé Euro Garages à éliminer totalement les brèches de données.

* Source

Étape 2

Optimiser votre architecture Zero Trust centrée sur l'identité

Au début de leur parcours de sécurité Zero Trust, la plupart des entreprises se retrouvent avec différentes applications on-premise et cloud non intégrées, ce qui oblige les équipes IT à gérer des identités disparates dans plusieurs systèmes, ainsi que les nombreux services et applications utilisés sans connaissance des enjeux informatiques.

La disparité des contrôles d'accès augmente ainsi la fragmentation et les vulnérabilités dont les auteurs d'attaques de ransomware peuvent tirer profit. Les utilisateurs finaux, quant à eux, ont généralement besoin de plusieurs noms d'utilisateur et mots de passe (souvent non sécurisés) faciles à pirater. Sans visibilité ni maîtrise de ces identités fragmentées, les équipes IT et sécurité se retrouvent avec des fenêtres de vulnérabilité potentiellement larges, que les cybercriminels mettent à profit pour accéder aux systèmes.

En adoptant une approche où l'identité est le nouveau périmètre de sécurité de votre entreprise, la gestion des identités et des accès (IAM) devient le point de contrôle central des utilisateurs, des terminaux, des données et des réseaux. Cette stratégie de sécurité axée sur l'identité est considérée par **Gartner** comme l'une des principales tendances de 2021 en matière de sécurité et de réduction des risques, car elle offre une visibilité et un contrôle accrus sur les utilisateurs ayant accès aux différentes ressources. En adoptant un modèle de sécurité axé sur l'identité, votre entreprise peut réduire les attaques de ransomware qui exploitent des identifiants compromis, un provisioning incorrect ou une authentification inadéquate grâce à l'implémentation du Zero Trust aux stades suivants :

Au stade 1, votre entreprise doit commencer à créer un écosystème unifié de gestion des identités et des accès (IAM) et éliminer les mauvaises pratiques liées aux mots de passe en implémentant **l'authentification unique (SSO)** et **l'AMFA** pour contrôler l'accès des collaborateurs aux ressources stratégiques.

Au stade 2, votre entreprise peut adopter de nouvelles pratiques de sécurité en étendant les contrôles d'accès à d'autres ressources (telles que les API) et en s'appuyant sur le contexte et d'autres facteurs pour améliorer la prise de décisions d'authentification.

Au stade 3, votre entreprise aura adopté une approche d'authentification Zero Trust entièrement basée sur les risques, avec notamment des solutions d'accès sans mot de passe et itératives.

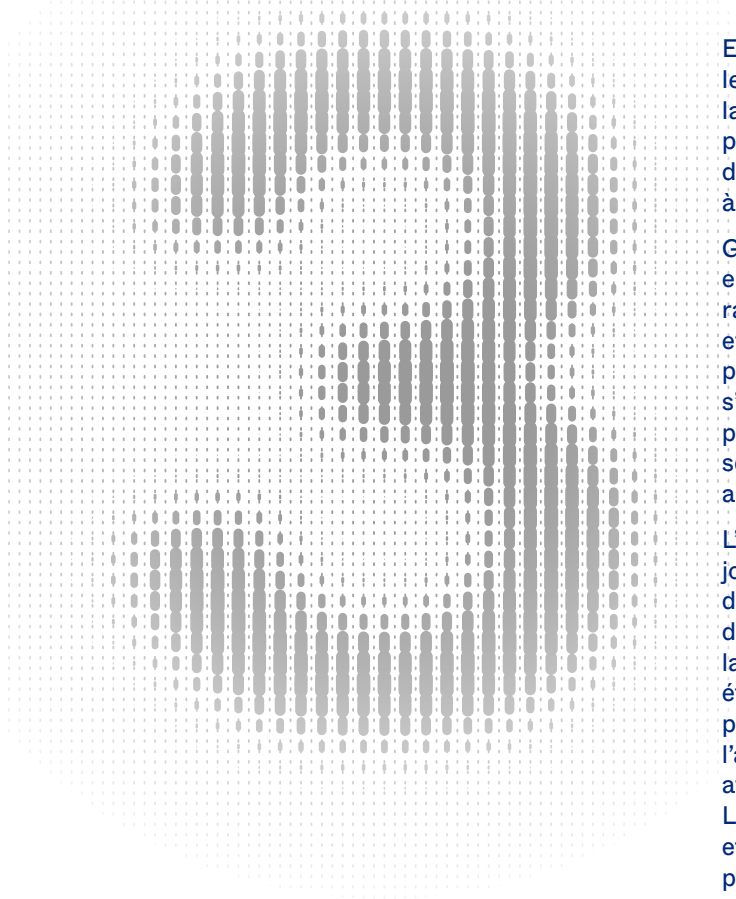
مطارات دبي
DUBAI AIRPORTS

Okta a accompagné **Dubai Airports*** dans la mise en œuvre d'une stratégie de sécurité Zero Trust. En prenant des décisions de sécurité sur la base des utilisateurs individuels et du contexte de leurs demandes d'accès, l'entreprise a ainsi réduit sa surface d'attaque. Cette approche Zero Trust axée sur l'identité a permis à Dubai Airports de protéger les données au niveau individuel, tout en laissant les collaborateurs libres d'utiliser les terminaux de leur choix. Grâce à Okta Adaptive Multi-Factor Authentication qui protège les applications cloud et on-premise, les 4 000 collaborateurs de Dubai Airports et les 100 000 personnes actives sur le site peuvent travailler en toute sécurité, sans risquer d'exposer leurs données à des menaces externes.

* Source

Étape 3

Centraliser la gestion des accès pour vos applications et ressources stratégiques



En plus de nuire à l'expérience utilisateur et de ralentir les opérations pour les responsables IT et sécurité, la nécessité de mémoriser plusieurs mots de passe pour différentes applications complique le processus d'authentification et augmente le risque d'exposition à des tiers.

Grâce à l'implémentation d'outils tels que le SSO, votre entreprise peut bloquer de nombreuses menaces de ransomware en offrant une solution SSO sécurisée et centralisée pour chaque plateforme et application professionnelle. Les utilisateurs peuvent ainsi s'authentifier rapidement, et vos équipes IT et sécurité peuvent gérer les accès de manière bien plus efficace et sécurisée, ce qui leur permet d'isoler et de bloquer toute activité suspecte avant qu'elle ne fasse des dégâts.

L'intégration d'**Okta Lifecycle Management** peut jouer un rôle déterminant dans le renforcement des défenses de votre entreprise contre les auteurs d'attaques de ransomware. Selon ce **rapport de CRN**, la tristement célèbre attaque de ransomware dont a été victime Colonial Pipeline est survenue lorsque des pirates ont infiltré un compte inactif qui n'utilisait pas l'authentification multifacteur (MFA). Même si le MFA avait pu empêcher des tiers d'accéder au compte, Okta Lifecycle Management aurait supprimé le compte et/ou ses privilèges. En automatisant le processus de provisioning à toutes les étapes du cycle de vie des utilisateurs (arrivées, transferts et départs) avec Okta Lifecycle Management, les utilisateurs n'ont accès qu'aux applications appropriées au moment opportun, et les comptes inactifs ne peuvent plus être utilisés par les pirates pour prendre le contrôle de votre réseau IT.

En plus de tirer parti des mots de passe faibles et des comptes inactifs, les auteurs d'attaques de ransomware sont connus pour cibler délibérément des entreprises dotées d'architectures d'ancienne génération difficiles à visualiser et d'intégrations mal conçues. La réduction de la surface d'attaque de ces vastes réseaux complexes peut toutefois représenter un défi de taille pour les responsables IT et engendre de nombreuses failles pouvant être exploitées par les cybercriminels.

Okta Integration Network permet à votre entreprise de tirer parti de plusieurs milliers de préintégrations et repose sur des protocoles modernes tels qu'OpenID Connect, qui limitent les risques de prolifération des mots de passe et permettent de définir des politiques d'accès contextuelles cohérentes et dynamiques pour l'ensemble de vos ressources, tout en améliorant l'expérience utilisateur.

Les solutions de sécurité réseau et CASB se servent également des modèles de trafic cloud et d'utilisation des applications pour renforcer la conformité, la protection contre les menaces et la prévention des pertes de données. Parallèlement, l'analyse de la sécurité élargit votre horizon aux systèmes cloud, mobiles et on-premise pour multiplier les opportunités de corrélation et d'application.

Vos équipes IT et sécurité peuvent ainsi déployer facilement les dernières applications en date, centraliser la gestion de vos utilisateurs et automatiser les workflows d'accès au niveau des applications cloud, on-premise et mobiles en toute simplicité.

Vinted

Pour soutenir son plan de croissance à long terme, **Vinted*** avait besoin d'une plateforme capable d'automatiser les tâches manuelles et de renforcer la sécurité, sans pour autant créer davantage de points de friction pour les utilisateurs. En fournissant une intégration SSO prête à l'emploi pour 95 % des 394 applications utilisées par Vinted, Okta a permis à l'entreprise de déployer rapidement un écosystème d'identités avancé sur son réseau, tout en gagnant du temps et en faisant des économies. La facilité d'intégration avec Okta a permis à Vinted d'identifier un grand nombre d'applications non validées (Shadow IT), telles que des abonnements et services redondants, p. ex. trois ou quatre applications remplissant les mêmes fonctions. L'entreprise a donc décidé de créer son propre annuaire d'utilisateurs et d'applications à l'aide d'Okta Universal Directory. Pour la première fois, Vinted disposait d'une liste exhaustive et centralisée lui permettant de déterminer qui utilisait ses applications et comment.

* Source

Pourquoi choisir Okta ?

Les cybercriminels ne vous laissent aucun répit. C'est pourquoi il est essentiel d'opter pour un fournisseur IDaaS capable de protéger votre entreprise 24 h/24 pour garder une longueur d'avance sur les menaces et lutter contre les ransomwares.

En plus d'être **la plateforme d'identité n° 1**, systématiquement nommée dans la catégorie des leaders par les plus grands cabinets d'analyse et utilisée par plus de 13 000 clients à travers le monde, Okta possède le plus vaste portefeuille d'applications préintégrées du marché, avec plus de 7 000 applications cloud, on-premise et mobiles prêtes à l'emploi disponibles via l'Okta Integration Network.

En plus de notre suite phare de solutions d'identité de pointe, nous avons conçu une architecture cloud globale et évolutive offrant un taux de disponibilité moyen de 99,99 %, ce qui fait de notre plateforme d'identité l'une des **solutions les plus fiables du marché**.

Regardez la démonstration MFA
Dans cette démonstration, découvrez comment configurer une authentification multifacteur performante pour renforcer la sécurité du réseau et consolider les défenses de votre entreprise contre les ransomwares.

Regarder la démo

Prêt à essayer Okta ?
Démarrez votre essai gratuit de 30 jours dès aujourd'hui.

Démarrer l'essai