TÉMOIGNAGE CLIENT AKAMAI

Une grande entreprise de services financiers sécurise son accès à distance avec Akamai après une attaque par ransomware

Visibilité complète du réseau

Mise en œuvre rapide des règles

Personnel en télétravail sécurisé

Le client

Une grande entreprise de services financiers basée au Brésil.

L'enjeu

Un accès à distance accru

À l'instar de nombreuses entreprises, en raison de la pandémie de COVID-19, les besoins de ce fournisseur de services financiers en matière d'accès à distance ont évolué, et une grande partie du personnel informatique de la banque a commencé à travailler à domicile sur des terminaux gérés par l'entreprise. Lorsque les utilisateurs ont commencé à accéder aux données et aux applications dont ils avaient besoin dans le cadre de leurs fonctions principalement hors du réseau sécurisé de l'entreprise, cette dernière a vu sa surface d'attaque s'accroître rapidement.

Un incident de ransomware réussi

Peu de temps après la transition vers un modèle de travail à domicile, une base de données Oracle Cloud critique de la banque a été victime d'une attaque réussie de ransomware, dont ils ont découvert plus tard qu'elle provenait d'un environnement VDI. Les équipes informatique et de sécurité savaient qu'elles devaient prendre des mesures rapidement pour limiter la perte de données financières sensibles. De plus, elles avaient conscience que si elles ne parvenaient pas à déterminer et à sécuriser le vecteur d'attaque d'origine, le ransomware risquait de se propager latéralement aux serveurs de sauvegarde et à l'environnement de production de l'entreprise. La banque aurait alors subi d'importantes pertes financières et de données.

Choix d'une solution

La solution Akamai Guardicore Segmentation était déjà très utilisée dans d'autres secteurs de la banque. Avant l'attaque par ransomware, la plateforme était chargée de gérer et d'appliquer les règles de segmentation de plus de 23 000 serveurs avec des charges de travail couvrant des infrastructures sur site, virtuelles, dédiées physiques et VDI, ainsi que des environnements de conteneurs Azure et OpenShift.

Large Financial Services Company

Secteur
Services financiers

Solution
Akamai Guardicore Segmentation

Impacts majeurs

- Empêche les ransomwares de se propager via des mouvements latéraux
- Offre une visibilité granulaire des flux réseau
- Protège l'accès à distance en segmentant les environnements VDI
- Assure une réponse rapide aux incidents

Akamai

La banque avait déjà utilisé cette solution de segmentation logicielle dans le cadre de plusieurs initiatives de sécurité et de conformité, notamment pour la gestion de l'accès des administrateurs aux jump box et la segmentation d'applications Swift. Connaissant les capacités de la plateforme à assurer une excellente visibilité et une rapide mise en œuvre des règles, l'équipe de réponse aux incidents s'est empressée d'exploiter les fonctionnalités d'Akamai Guardicore Segmentation pour neutraliser la violation.

Avantages d'Akamai Guardicore Segmentation

Visibilité au niveau des processus

À l'aide de la plateforme, les membres de l'équipe de réponse aux incidents de la banque ont étudié les flux de communication historiques. Ils sont remontés à l'origine du ransomware, à savoir la connexion VDI distante d'un administrateur de base de données communiquant avec une base de données Oracle Cloud.

Mise en œuvre rapide des règles

Après avoir identifié le vecteur d'attaque, accélérer la segmentation de l'infrastructure VDI est devenu une priorité de l'équipe. Le processus de planification des règles a commencé un samedi, en utilisant les fonctionnalités de visibilité d'Akamai Guardicore Segmentation pour définir les besoins potentiels en matière de règles. Le mardi suivant, la banque avait mis en place des règles applicables pour les plus de 3 000 connexions VDI à Oracle Cloud.

Récupération après attaque par ransomware

L'équipe a déployé des agents Akamai sur les applications de sauvegarde et configuré le cloisonnement des applications, définissant ce qui pourrait communiquer avec la ressource, jusqu'au niveau des processus. Elle a poursuivi le déploiement dans la zone attaquée, empêchant ainsi le ransomware de se propager davantage, grâce à des règles de refus au niveau mondial.

Afin de réduire les risques supplémentaires liés à l'accès des travailleurs à distance, des règles ont également été définies pour les deux solutions VDI utilisées par les employés des centres d'appels, empêchant ainsi tout mouvement latéral non autorisé entre les points de terminaison de la banque.

Le fait d'avoir appliqué les règles de segmentation en seulement trois jours a permis à cette entreprise de services financiers de réduire considérablement l'impact de l'incident de ransomware et de renforcer la sécurité de l'accès à distance à l'avenir.

> La visibilité offerte par [Akamai Guardicore Segmentation] nous a permis d'y voir plus clair !
>
> Responsable de la sécurité de l'infrastructure d'une grande entreprise de services financiers

Pour plus d'informations, consultez le site akamai.com/guardicore.