TÉMOIGNAGE CLIENT AKAMAI

Un fournisseur d'infrastructure de communications

stoppe net les ransomwares avec Akamai

Prévention des pertes potentielles d'un million de dollars

Prévention de l'informatique fantôme potentielle

Visibilité du trafic est-ouest

Le client

Ce fournisseur d'infrastructure de communications américain permet aux entreprises et aux résidents de rester connectés dans le monde d'aujourd'hui en constante évolution. Il est en charge d'un vaste réseau d'antennes relais et de fibres optiques sur lesquelles les clients comptent au quotidien.

Les enjeux

Contrôle et visibilité limités des points de terminaison

Sachant qu'il y a plus de 6 000 ordinateurs portables déployés dans l'entreprise, l'équipe de sécurité informatique s'inquiétait de plus en plus des risques que présentait le parc pour l'environnement informatique plus large. En outre, il était nécessaire de résoudre les problèmes persistants liés à l'activité informatique fantôme de certains utilisateurs expérimentés de l'entreprise.

Bien que certaines mesures de sécurité aient été mises en place par l'équipe informatique des utilisateurs finaux, elles étaient limitées. Aucune ne pouvait contrôler de manière granulaire l'accès au système pour les utilisateurs ou limiter la communication P2P pour empêcher efficacement la propagation des programmes malveillants, ce dernier point étant une préoccupation importante de l'entreprise.

Pour combler ces lacunes, les parties prenantes souhaitaient renforcer la sécurité de l'entreprise en adoptant une solution visant à étendre la visibilité et les contrôles de segmentation granulaires aux terminaux des employés. Elle leur permettrait en outre de mieux observer et prévenir les mouvements latéraux non autorisés.

Un fournisseur d'infrastructure de communications

Localisation
États-Unis

Secteur
Infrastructure de communications

Solution
Akamai Guardicore Segmentation

Impacts majeurs
- Prévention des ransomwares
- Contrer l'informatique fantôme
- Visibilité du trafic est-ouest

Choix d'une solution

Les décisionnaires en matière de sécurité s'intéressaient depuis un certain temps à Akamai Guardicore Segmentation, en raison de sa multitude de cas d'utilisation de cybersécurité. L'organisation a décidé d'adopter une approche graduelle afin d'observer le potentiel dans la visibilité granulaire et le processus direct de création de règles.

Étant donné que les politiques de segmentation logicielles d'Akamai ne sont pas liées à l'infrastructure sous-jacente, le fournisseur a eu la possibilité de s'attaquer à un certain nombre d'initiatives de sécurité. Cependant, le parc d'ordinateurs portables des employés étant identifié comme à haut risque, l'équipe a accordé la priorité au déploiement d'agents Akamai au niveau de ses points de terminaison.

Akamai Guardicore Segmentation

Une fois le projet lancé, l'agent Windows rationalisé d'Akamai a rapidement été déployé sur les ordinateurs de l'organisation. Cela a étendu la visibilité au niveau des processus à l'accès des utilisateurs et à l'activité des ordinateurs portables.

L'équipe de sécurité informatique a ensuite pu créer et gérer des contrôles de sécurité pour ces points de terminaison de manière centralisée, tous basés sur des données environnementales précises. Elle a ensuite pu rapidement mettre en place plusieurs stratégies, notamment une alerte pour les activités spécifiques du protocole RDP (Microsoft Remote Desktop Protocol), y compris les tentatives de connexion ratées.

Visibilité granulaire en action

Peu de temps après le déploiement, la règle configurée pour signaler une activité anormale liée au protocole RDP a généré une série d'alertes. Il est rapidement apparu évident qu'un acteur malveillant tentait une attaque en force, car chaque tentative de connexion échouait.

L'équipe de sécurité informatique a surveillé de près la situation et, alors que les attaquants progressaient, elle est passée à l'action et a bloqué le RDP sur chaque point de terminaison avec un agent Akamai. En seulement quelques clics, elle a créé et appliqué une nouvelle règle de segmentation qui a désactivé le RDP, mettant ainsi un terme à l'attaque avant qu'un seul point de terminaison ne soit compromis.

Une attaque ransomware arrêtée en plein élan

Au cours de l'analyse rétrospective, l'équipe de sécurité s'est rapidement rendu compte que tous les indicateurs pointaient vers un acteur majeur et bien connu de la menace ransomware.

Si la campagne avait réussi, les attaquants auraient probablement déployé leur tactique habituelle, qui consiste à crypter tout ce qui est à leur portée avant de demander une rançon. En raison de la taille du fournisseur et des tendances actuelles, la demande des acteurs malveillants aurait certainement dépassé le million de dollars. Cela aurait entraîné des perturbations et des temps d'arrêt supplémentaires importants si des actifs critiques pour l'entreprise, tels que le système ERP, avaient été compromis.

Cependant, grâce à Akamai et à l'équipe de sécurité qui a su agir rapidement, la tentative d'attaque n'a pas eu d'impact sur l'organisation.

Contrer l'informatique fantôme

En plus de stopper les menaces externes, la plateforme a également permis à l'équipe de relever les défis internes. Avant Akamai, la visibilité limitée sur les points de terminaison permettait à certains utilisateurs de contourner plus facilement les processus officiels, en exécutant de leur propre chef des activités qui étaient non conformes aux politiques de l'entreprise. Cette nouvelle visibilité et la capacité à appliquer des contrôles de sécurité sur les points de terminaison ont permis à l'équipe de sécurité informatique d'endiguer l'informatique fantôme. Il s'agissait notamment d'empêcher les membres de l'organisation DevOps de créer de nouvelles ressources de leur propre chef sans passer par les canaux officiels pour obtenir une autorisation.

Protection étendue avec Akamai

Pour le fournisseur d'infrastructure de communications, la protection des points de terminaison ne constitue qu'une première étape. Il prévoit en effet d'explorer de nouvelles fonctionnalités, de déployer Akamai dans son centre de données, de sécuriser son environnement Citrix et d'appliquer des contrôles d'accès tiers pour les fournisseurs externes.

Grâce à la nature flexible de la plateforme, l'équipe est certaine de pouvoir étendre la protection contre les menaces avancées partout dans l'environnement, quelle que soit l'évolution future de la stratégie des fusions et acquisitions, ou des initiatives de transformation digitale.

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