TÉMOIGNAGE CLIENT AKAMAI

L'université d'État choisit Akamai pour protéger la technologie d'exploitation des bâtiments critiques sur 24 campus

Visibilité complète du réseau

Règles de segmentation

Détection des menaces et réponse

Le client

Grande université d'État

Cette grande université d'État accueille plus de 100 000 étudiants, avec plus de 17 000 enseignants et membres du personnel répartis sur ses 24 campus.

L'enjeu

Centralisation de l'infrastructure réseau de plus de 600 bâtiments

Une grande université d'État souhaitait intégrer des systèmes d'automatisation des bâtiments en toute sécurité dans le cadre d'une initiative de campus intelligent à l'échelle de l'État. L'équipe responsable des installations physiques et des systèmes OT de l'université s'inquiétait du manque de segmentation protégeant ces terminaux et applications. Elle était également préoccupée par le réseau informatique de l'université en cas de faille dans les systèmes. En conséquence, l'équipe responsable a entrepris un effort ambitieux pour centraliser ses systèmes d'automatisation des bâtiments et améliorer la sécurité.

Le chef de projet de l'université explique : « Jusqu'à il y a environ deux ans, tous les campus étaient pratiquement livrés à eux-mêmes. Nous hébergions le serveur d'application principal, mais les contrôleurs individuels du campus se trouvaient sur des réseaux informatiques et n'étaient pas toujours segmentés sur des VLAN distincts du reste du trafic du campus. »

Cela signifie qu'une attaque réussie sur les systèmes de contrôle d'un seul bâtiment pouvait facilement se propager au réseau informatique d'un campus ou inversement.

Le projet était également motivé par des raisons économiques. « L'université voulait gérer sa consommation énergétique et voir où nous pouvions réduire les coûts, » a expliqué le chef de projet, « mais nous ne recevions pas de données des campus parce qu'ils fonctionnaient tous à partir de systèmes autonomes.

Nous devions donc les connecter, mais nous devions le faire en toute sécurité. Les connexions entre ces campus distants et notre centre de données pouvaient créer une brèche dans notre réseau, facilitant ainsi une attaque potentielle. »

Large State University

Secteur
Enseignement

Solution
Guardicore Segmentation d'Akamai

Impacts majeurs
- Empêche les mouvements latéraux
- Cloisonne les applications

Akamai

L'ambitieux projet visant à tout intégrer dans une infrastructure de réseau partagée couvrait plus de 600 bâtiments répartis sur 24 campus. L'équipe du département chargée de l'automatisation des installations a été sélectionnée pour prendre en charge le projet.

Toutefois, la complexité même des systèmes d'automatisation de l'université et le nombre de fournisseurs impliqués ont constitué un autre défi de taille.

« Nous gérons les systèmes d'ascenseurs, le chauffage, la ventilation et la climatisation, les systèmes d'analyse des vibrations, l'éclairage, la distribution électrique et les compteurs électriques. Ensuite, nous avons tous nos principaux services collectifs, notamment la production de vapeur, la distribution d'électricité et le traitement des eaux usées. Nous traitons avec plus de 260 sous-traitants qui travaillent sur ces systèmes dans les différentes entreprises. » Tous ces fournisseurs devaient avoir accès au réseau, sans introduire de risques ni interférer avec les systèmes de contrôle des autres.

> “Un système de gestion de pare-feu ne peut pas rivaliser avec [Akamai].
>
> Chef de projet universitaire

Choix d'une solution

Objectif attendu : visibilité du trafic est-ouest et règles centralisées

Tempered Networks, un fournisseur de sécurité spécialisé dans les systèmes de contrôle intelligents et les réseaux de l'Internet des objets, a été sollicité pour gérer les connexions nord-sud entre les campus éloignés et le centre de données principal de l'université. Une fois ce point réglé, l'université devait encore protéger plus de 300 serveurs du centre de données contre les menaces en termes de sécurité.

« Nous avons envisagé des solutions censées gérer le trafic est-ouest, mais aucune ne répondait à nos critères en termes d'efficacité et de simplicité, » se souvient le chef de projet de l'université.

L'équipe a découvert Akamai lorsqu'elle est tombée sur l'outil gratuit de simulation d'attaque et d'intrusion Infection Monkey. Infection Monkey aide les opérateurs de centres de données à évaluer la résilience de leurs environnements face aux attaques post-intrusion et aux mouvements latéraux.

Après avoir téléchargé l'outil et commencé à l'utiliser, l'équipe a réalisé que l'outil Guardicore Segmentation d'Akamai pouvait résoudre les problèmes mis en évidence par Infection Monkey.

Guardicore Segmentation d'Akamai est l'une des rares solutions du marché actuellement axées sur la microsegmentation. Elle permet aux opérateurs de définir, de créer et de déployer facilement des règles de sécurité pour régir les communications entre des applications individuelles ou regroupées logiquement.

Lors de la toute première présentation à l'université, l'équipe d'Akamai a démontré les capacités de visualisation uniques de la plateforme. Grâce à Akamai Guardicore Segmentation, les opérateurs de centres de données peuvent visualiser toutes les applications en cours d'exécution dans leur environnement et cartographier graphiquement les dépendances entre elles.

« Nous avons immédiatement adopté cet outil. Nous savions que c'était exactement ce dont nous avions besoin. »

Guardicore Segmentation d'Akamai

Akamai par rapport aux pare-feu internes

« Avec la gestion centralisée des pare-feu, vous devez toujours configurer les règles pour chaque pare-feu individuellement. Avec [Akamai], nous pouvons créer un groupe d'applications et décider que nous voulons que ces systèmes ne communiquent qu'entre eux. »

Les pare-feu posent également des problèmes de coût, de ressources et de gestion. « La gestion de tous ces pare-feu serait un véritable cauchemar. Nous aurions probablement besoin d'une demi-douzaine de personnes pour déployer le système et s'assurer qu'il n'y a pas de problèmes, et d'au moins deux personnes dédiées à sa gestion. »

En outre, les pare-feu manquent de souplesse pour définir et modifier les règles au niveau de l'application. « Avec [Akamai], nous pouvons écouter pendant un moment et comprendre ce qui se passe entre les systèmes et les raisons de leur besoin de communication. Avec les pare-feu, c'est tout ou rien. Un pare-feu va simplement bloquer les ports, point barre. »

Microsegmentation avec gestion centralisée et facile

La rapidité et la facilité avec lesquelles les membres de l'équipe peuvent créer et déployer des règles ont été citées comme un autre avantage important.

« Le premier jour, nous l'avons installé sur quelques sites, puis nous avons essayé de créer une règle pour empêcher un fournisseur de voir un autre fournisseur. Et c'est ainsi que le premier fournisseur a été bloqué. Cela m'a prouvé que ce produit correspondait à ce que nous recherchions, » a indiqué le chef de projet.

Les outils et la méthodologie de microsegmentation d'Akamai ne nécessitent pas l'intervention d'un expert. « Le fait d'avoir quelque chose d'assez simple pour que n'importe quel membre de notre équipe puisse en tirer parti a été un facteur déterminant pour moi. »

Au-delà de la microsegmentation : détection et réponse

La visibilité acquise grâce à Akamai a eu l'avantage supplémentaire de mettre en évidence les anomalies opérationnelles au sein du centre de données. « Nous avons trouvé un service de spooler d'impression qui se connectait à un réseau qui n'était pas le nôtre, » raconte le chef de projet. « Lorsque nous avons finalement découvert le problème, il s'agissait d'une session de bureau à distance de quelqu'un qui s'était déconnectée sans jamais se terminer et qui essayait continuellement de dialoguer avec le serveur d'impression de son PC. Si ce PC présentait une faille, il pourrait potentiellement constituer un moyen d'accès au serveur d'application. »

Maintenant que l'équipe utilise activement Akamai, l'université envisage déjà d'autres améliorations en termes de sécurité et d'efficacité grâce à la solution.

« À l'avenir, nous prévoyons d'automatiser une grande partie des fonctionnalités du réseau en cas d'incident. Par exemple, si nous avons détecté une adresse MAC ou un point d'accès illicite dans un bâtiment, nous pouvons utiliser [Guardicore Segmentation d'Akamai] pour envoyer une commande à la solution Tempered Networks afin de verrouiller ce bâtiment, puis envoyer une alerte à un opérateur pour qu'il corrige la situation et comprenne ce qui s'est passé. Jusqu'à présent, nous ne disposions pas de cette capacité de détection. »

La plateforme Akamai a permis à l'équipe d'automatisation des installations de l'université d'atteindre le niveau de sécurité souhaité plus rapidement et plus facilement que prévu. « Nous n'avons jamais vraiment disposé d'un outil proactif comme celui-ci, qui surveille tout en permanence, » a expliqué le chef de projet.

Akamai surveillant le trafic est-ouest des centres de données, l'équipe n'a pas à le faire. « Je veux que notre équipe puisse se concentrer sur son travail, qui consiste à aider l'université à économiser de l'énergie et de l'argent. Nous ne pouvons pas nous concentrer sur cet objectif si nous devons nous préoccuper de ce qui se passe dans le centre de données. »

L'équipe de l'université s'est mise à la recherche d'une solution simple de microsegmentation. Avec Akamai, elle a trouvé un outil qui surpasse ses attentes.

« Cette solution tient ses promesses. »

> “Dès que nous l'avons installé, les membres de l'équipe ont été en mesure de l'utiliser, de le déployer et de mettre en place des règles de protection, et ils ont été conquis.
>
> Chef de projet universitaire

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

 | Assistance | Publication : 06/23