

TÉMOIGNAGE CLIENT AKAMAI

Université Tunghai

Secure Internet Access Enterprise d'Akamai améliore la sécurité de l'université Tunghai et réduit le temps de gestion des incidents

Akamai aide l'université à libérer des ressources au sein de l'équipe de sécurité et à réduire les notifications de sécurité externes

Les entreprises contemporaines sont confrontées à des cybermenaces complexes, à l'heure où les pirates utilisent des méthodes toujours plus sophistiquées pour contourner les défenses de sécurité. Comment trouver un équilibre entre la nécessité d'une protection proactive contre de telles attaques et le besoin de flexibilité et de liberté dans une importante population universitaire internationale ?

C'est le défi auquel l'équipe du centre informatique de l'université Tunghai était confrontée. L'université a adopté l'apprentissage digital et a conçu un campus intelligent qui offre aux étudiants et au personnel un accès haut débit sans fil gratuit à Internet à l'intérieur comme à l'extérieur du campus. Au début de chaque année universitaire, les étudiants arrivent et connectent leurs ordinateurs portables au réseau de l'université.

Cependant, comme la politique de l'université en matière d'informatique n'a pas imposé l'installation d'antivirus sur les ordinateurs des étudiants, de nombreux ordinateurs portables ont été infectés par des logiciels malveillants. Ces terminaux infectés ont entraîné une défaillance des réseaux à l'intérieur et à l'extérieur du campus, une consommation excessive de bande passante et un trafic de botnets malveillants. De plus, les logiciels malveillants se sont déplacés latéralement sur des ordinateurs gérés par l'université, qui a reçu des notifications du centre régional du réseau de Taichung indiquant que le réseau de l'université Tunghai avait été attaqué et faisait l'objet de connexions anormales.

« Le centre informatique a dispensé une formation à la sécurité informatique et a exhorté les étudiants et le personnel enseignant à ne pas cliquer sur les liens suspects dans les e-mails ou sur des pages Web », explique Chien-Hui Ou, directeur de la technologie réseau. « Mais les hackers ont continué à avoir recours à des tactiques de plus en plus détournées, ce qui fait que les utilisateurs pouvaient difficilement reconnaître les cybermenaces de manière immédiate, ce qui a finalement conduit les utilisateurs à être victimes de ces attaques. »

« Les logiciels antivirus traditionnels et les solutions de sécurité informatique qui s'appuient sur l'analyse et l'identification des codes malveillants ne sont pas



Université Tunghai
Taichung, Taiwan
eng.thu.edu.tw

Secteur
Secteur public

Solution
[Secure Internet Access Enterprise](#)

Impacts majeurs

- Sécurité renforcée et réduction du temps de gestion de la sécurité et de résolution des incidents
- Blocage proactif du trafic du serveur de commande et contrôle provenant de terminaux infectés et réduction des mouvements latéraux
- Réduction du volume de notifications de sécurité externes
- Optimisation du budget de sécurité en passant directement des investissements dans des actifs physiques à des coûts d'exploitation



suffisamment rapides. Si un nouveau logiciel malveillant entre en scène et que les fournisseurs d'antivirus n'ont pas encore déterminé son code ni mis à jour ses signatures, le logiciel malveillant ne sera pas détecté », explique Kuang-Chin Chang du Groupe du réseau de l'université Tunghai. « De plus, en raison de la tendance à chiffrer le trafic Web, les hackers utilisent désormais ces canaux chiffrés pour lancer des attaques, ce qui rend les attaques zero day de plus en plus difficiles à arrêter. »

Akamai stoppe efficacement les connexions suspectes

Sachant que l'université avait besoin d'améliorer sa stratégie de sécurité existante, l'équipe informatique a commencé à étudier les produits utilisant le DNS comme point de contrôle de sécurité. Elle pensait que cette approche permettrait à l'université de renforcer sa sécurité globale sans que cela n'ait d'impact sur la liberté académique.

Après un processus d'évaluation concurrentielle, l'université a arrêté son choix sur la solution Secure Internet Access Enterprise d'Akamai. Secure Internet Access Enterprise est un service basé dans le cloud qui protège de manière proactive un réseau et ses utilisateurs en analysant chaque requête DNS. Chaque requête est comparée aux informations en temps réel sur les menaces obtenues grâce à la visibilité inégalée du trafic Internet d'Akamai, avant de bloquer ou de diffuser le contenu Web demandé.

« Secure Internet Access Enterprise détecte et bloque les requêtes DNS vers des domaines susceptibles de fournir des contenus malveillants tels qu'un ransomware ou un logiciel malveillant de minage de monnaies, ou de dérober des informations utilisateur », explique M. Chang. « Même si l'ordinateur d'un étudiant est infecté par un logiciel malveillant lors d'une utilisation hors du campus, le logiciel malveillant ne pourra pas se connecter en externe au serveur de commande et contrôle des hackers lorsque l'ordinateur se reconnectera au réseau du campus. »

Avant Secure Internet Access Enterprise, il était difficile d'atténuer un incident lié à la sécurité de l'information. Lorsqu'une connexion anormale était signalée, le personnel de gestion du réseau devait souvent utiliser des adresses IP pour suivre l'ordinateur compromis, trouver des enregistrements de connexion à partir des fichiers journaux pour convaincre la partie concernée qu'un incident s'était produit, puis demander à la partie de coopérer avec les procédures de nettoyage antivirus.

« C'est la raison pour laquelle il fallait environ une semaine pour résoudre un incident. Et cela consommait de nombreuses ressources de sécurité », indique M. Chang. « Cependant, après avoir déployé Secure Internet Access Enterprise, le nombre d'incidents de sécurité signalés a chuté, ce qui nous a permis de consacrer nos ressources à d'autres projets de sécurité. »

Il poursuit : « Secure Internet Access Enterprise est particulièrement rapide et facile à déployer et à configurer, ce qui le distingue des équipements physiques traditionnels, qui nécessitent d'abord une déconnexion du réseau, puis un test, avant qu'un système puisse être mis en service. Avec Secure Internet Access Enterprise, il vous suffit de diriger votre trafic DNS directement vers la plateforme Akamai et le processus prend quelques minutes seulement. »

Le directeur Chien-Hui Ou indique : « Secure Internet Access Enterprise fournit automatiquement des rapports détaillés sur les incidents afin que l'équipe de sécurité puisse rapidement savoir quels logiciels malveillants ont infecté les ordinateurs des clients ou sur quels liens Web ils ont cliqué avant que les ordinateurs ne soient infectés par des logiciels malveillants de minage de monnaies. Les données s'intègrent à notre système de gestion des informations et des événements de sécurité. Ainsi, les rapports aident également l'équipe à comprendre toute activité anormale récente du réseau afin que nous puissions réagir de manière proactive. »



Après avoir déployé Secure Internet Access Enterprise, le nombre d'incidents de sécurité signalés a chuté, ce qui a permis à nos ressources de se consacrer à d'autres projets de sécurité.

Kuang-Chin Chang

Groupe réseau de l'université Tunghai

Réductions majeures des coûts et de la main-d'œuvre

Chao-Tung Yang, directeur du centre informatique électronique de l'université Tunghai, met l'accent sur les avantages stratégiques. « La sécurité informatique est aujourd'hui importante et le sera de plus en plus à l'avenir, à mesure que les applications digitales se développeront. Tunghai a toujours privilégié la protection des applications informatiques et la sécurité de l'information, et le président de l'université soutient l'investissement dans la sécurité de l'information. »

M. Yang poursuit : « Lorsque l'on prend du recul et que l'on observe l'orientation actuelle de la croissance informatique, il est clair que les services basés sur le cloud sont là pour durer. Les systèmes de défense précédents étaient déployés avec une combinaison de logiciels et de matériel, et leur entretien, entre autre la mise à jour des correctifs, exigeait beaucoup de temps et de travail. »

Les services basés sur le cloud d'Akamai sont différents, ils permettent une réduction totale du travail de maintenance. M. Yang est optimiste quant à l'avenir des services de sécurité informatique basés sur le cloud : « Non seulement ils diminueront le travail à effectuer, mais ils réduiront également le besoin d'espace physique dans les salles d'informatiques et nous feront faire des économies sur l'air conditionné et l'électricité. Cela s'inscrit dans la politique de réduction de la quantité d'énergie utilisée dans les salles d'équipement du centre informatique. »

« En ce qui concerne le coût, l'utilisation de services basés sur le cloud, ne nécessite pas de dépense ponctuelle majeure contrairement à l'achat d'équipements physiques», explique M. Yang. « Comme il s'agit d'une location annuelle, Secure Internet Access Enterprise est plus facilement accessible pour les universités. »

« Le travail lié à la sécurité informatique n'est jamais terminé. Mais avec Secure Internet Access Enterprise, la masse de travail que représente la gestion des incidents est considérablement réduite, ce qui libère des ressources pour le renforcement des défenses contre les attaques de botnet et des analyses d'activité plus complètes », conclut M. Yang.



Secure Internet Access Enterprise est particulièrement rapide et facile à déployer et à configurer, ce qui le distingue des équipements physiques traditionnels, qui nécessitent d'abord une déconnexion du réseau, puis un test, avant qu'un système puisse être mis en service.

Kuang-Chin Chang

Groupe réseau de l'université Tunghai



Première université privée de Taïwan, l'université Tunghai a été fondée en 1955. L'université est le premier et le seul établissement d'enseignement à offrir un programme d'éducation complet, de la maternelle au doctorat. Tunghai compte actuellement neuf universités : Université des arts, Université scientifique, Université d'ingénierie, Université de gestion, Université des sciences sociales, Université d'agriculture, Université des beaux-arts et de la conception créative, Université de droit et Université internationale. Tunghai compte environ 17 000 étudiants et près de 500 enseignants : <http://eng.thu.edu.tw/>.