TÉMOIGNAGE CLIENT AKAMAI

KKLab

Le venture studio adopte la solution Zero Trust d'Akamai, alliant flexibilité et protection des réseaux internes et externes

100

E-mails contenant des comportements malveillants automatiquement bloqués chaque jour

Met en place une version de démonstration en seulement 30 minutes

Renforce la sécurité tout en conservant la flexibilité

En 2015, la branche R&D de KKBOX, qui deviendra l'entreprise de recherche innovante KKLab en 2019, a commencé à s'intéresser de plus près à la sécurité de l'information. L'équipe de R&D a mené différentes expériences et embauché une équipe externe de professionnels, en vue d'effectuer des exercices d'intrusion de pirates informatiques et des tests de pénétration. Le but était d'identifier les failles potentielles de systèmes pouvant être affinés et améliorés. La branche a décidé de mettre en place l'authentification multifactorielle et a également adopté Secure Internet Access Enterprise d'Akamai pour bloquer les attaques ciblées et Enterprise Application Access d'Akamai pour garantir la sécurité de l'accès au système d'applications. Avec l'introduction de ces deux services de sécurité de l'information basés sur le cloud, l'entreprise a mis en place une sécurité Zero Trust.

Le passage à une architecture Zero Trust renforce les vulnérabilités des VPN traditionnels

Hung-Yi Chen, Assistant Vice President de KKLab, a déclaré que KKBOX Group a toujours été axé sur la technologie. Il a rejoint le groupe alors qu'il était encore étudiant en 2005 et se consacre à la R&D dans le domaine technologique depuis 15 ans. Au fur et à mesure du développement du groupe, il a contribué à l'introduction de nombreuses nouvelles technologies intéressantes et audacieuses. Il a notamment créé une équipe d'ingénierie de la fiabilité du site en 2010, introduit les processus CI/CD et déployé une architecture de cloud hybride. Il a ensuite rejoint KKLab, un fournisseur de services technologiques cloud qui utilise ses bases de recherche sur le cloud et l'intelligence artificielle pour aider les entreprises à promouvoir la transformation technologique.

KKLab fournit des services technologiques à diverses entreprises du groupe, telles que KKBOX, KKTV, KKStream, KKTIX et The Farm. Il collabore également avec des entreprises externes en mettant l'accent sur les chaînes d'outils d'intelligence artificielle et d'apprentissage automatique, les plateformes de calcul à grande vitesse de données massives, la construction de plusieurs clouds hybrides et les services de conseil. KKLab a élargi son support digital pour fournir aux entreprises des services dans des domaines tels que la fabrication de haute technologie, la logistique du commerce de détail, les médias et le divertissement, ainsi que la finance et l'assurance.

KKLab
Taipei, Taïwan
www.kklab.com

Secteur
Médias

Le défi
Passer à la sécurité Zero Trust avec une authentification multifactorielle, une sécurité d'accès aux systèmes d'application et une meilleure prévention des attaques ciblées

Solutions
- Secure Internet Access Enterprise
- Enterprise Application Access

KKLab considère la sécurité de l'information comme un objectif principal dans la fourniture de services techniques. L'entreprise a notamment introduit des fonctionnalités de test de sécurité de l'information par des tiers et a utilisé des exercices d'intrusion pour révéler les faiblesses de sécurité potentielles de ses systèmes. De nombreuses personnes au sein de l'entreprise étaient certaines qu'elle disposait d'un niveau élevé de sécurité de l'information et qu'elle passerait facilement le test. Cependant, un test d'attaque de base de données a révélé que de nombreux comptes et mots de passe pouvaient être compromis par des pirates. L'équipe de KKLab s'est alors rendu compte que le cadre traditionnel de sécurité de l'information et le concept d'accès aux ressources intranet via un VPN sont en fait très dangereux. Une fois qu'un pirate obtient le mot de passe d'un compte interne, il peut suivre le VPN pour accéder à l'intranet et dérober des informations à son gré, ce qui expose le groupe à des risques opérationnels majeurs.

Pour contrer ces risques, KKLab a adopté des mesures de renforcement de sécurité en deux étapes. KKLab a tout d'abord implémenté l'authentification multifactorielle. Chaque personne doit saisir à la fois son mot de passe de compte et un mot de passe à usage unique avant d'être autorisée à se connecter au VPN. En outre, KKLab planifie activement une architecture Zero Trust, pour contrôler et vérifier en permanence si chaque visiteur est vraiment un utilisateur légitime. L'objectif ultime de KKLab est de créer un environnement de travail plus flexible et plus sûr, construit autour de Zero Trust.

Construction d'un filet de protection avec Secure Internet Access Enterprise et Enterprise Application Access pour bloquer toutes les connexions suspectes

Hung-Yi Chen a fait remarquer que le groupe KKBOX, spécialisé dans les médias de divertissement et les services de technologie de streaming, espère pouvoir profiter de cette flexibilité et bloquer immédiatement les comportements malveillants. L'entreprise ne souhaite pas prendre de mesures de contrôle excessives qui freineraient la créativité de ses collaborateurs. C'est pourquoi KKLab recommande d'adopter le modèle Zero Trust. La solution doit être facile à déployer et à entretenir, tout en affectant le moins possible le flux de travail de l'utilisateur. Sur la base de ces exigences, l'entreprise a décidé de travailler avec les solutions d'Akamai.

« La mission première de Secure Internet Access Enterprise d'Akamai est de filtrer et d'analyser les connexions provenant de l'intranet et de déterminer avec précision si la destination comporte une adresse IP ou un domaine malveillant. La clé réside dans la base de données massives. », explique-t-il. Il a ajouté qu'Akamai détenait une part de marché élevée. La raison principale pour laquelle KKLab a choisi Akamai est que la solution se fonde sur les réseaux de diffusion de contenu (CDN) et les services anti-DDoS, à partir desquels une grande quantité de données sur les comportements malveillants est collectée. Ces ressources puissantes constituent la pierre angulaire essentielle au bon fonctionnement de Secure Internet Access Enterprise.

De plus, les exigences de déploiement de Secure Internet Access Enterprise sont minimales en comparaison avec les solutions similaires sur le marché. Certaines requièrent l'installation d'un agent sur chaque terminal, et d'autres l'installation d'un connecteur sur le réseau d'infrastructure de l'entreprise. Akamai promeut des connexions simultanées. Akamai Connector est une image de machine virtuelle légère, et seuls quelques paramètres réseau doivent être ajustés. En 2018, KKLab a mis en place la version de démonstration en seulement 30 minutes. L'entreprise a pu vérifier qu'avec la vaste base de données intelligente, Secure Internet Access Enterprise et Akamai Connector pouvaient répondre à ses besoins, et elle a donc décidé de travailler avec Akamai.

La mission première de Secure Internet Access Enterprise d'Akamai est de filtrer et d'analyser les connexions provenant de l'intranet et de déterminer avec précision si la destination comporte une adresse IP ou un domaine malveillant. La clé réside dans la base de données massives.

Hung-Yi Chen
Assistant Vice President, KKLab

Outre le filtrage des connexions internes et externes, KKLab a introduit Enterprise Application Access en 2020 pour contrôler le comportement des employés qui accèdent aux ressources intranet depuis n'importe quel endroit. L'entreprise a déployé Akamai Connector à l'aide de l'image Docker. À ce jour, KKLab a connecté plus de 100 systèmes d'applications internes via Enterprise Application Access. Alors que de nombreux partenaires utilisaient des canaux VPN plus compliqués pour se connecter au système intranet, ils peuvent désormais utiliser le modèle Enterprise Application Access, ce qui leur évite de s'exposer aux risques en matière de maintenance informatique et libère leurs collègues de charges de maintenance superflue.

Depuis le déploiement d'Akamai, KKLab est devenu plus qu'un simple client. KKLab a une grande expérience du service client d'entreprise et a fourni de nombreuses suggestions et de nombreux exemples d'utilisation utiles aux clients, comme l'ajout d'informations plus détaillées dans les rapports. Par exemple, en plus de connaître les statistiques d'événements tels que les chevaux de Troie ou l'hameçonnage pendant une certaine période, KKLab souhaitait savoir quelle personne et quel terminal avaient déclenché ces événements. KKLab a également suggéré d'ajouter des visualisations de données, telles que des diagrammes circulaires, des diagrammes à barres et des graphiques linéaires, en plus du texte et des chiffres des rapports. Akamai a rapidement répondu à ces suggestions, en ajustant ses rapports et en offrant de plus grands avantages aux utilisateurs partout dans le monde.

Aujourd'hui, avec la protection de la solution Zero Trust d'Akamai, KKBOX Group bloque automatiquement environ 100 e-mails par jour qui tentent de connecter des utilisateurs à des sites contenant des publicités malveillantes, des programmes malveillants ou de l'hameçonnage. KKLab peut facilement identifier tout comportement de connexion suspect et prévenir les problèmes avant qu'ils ne causent des dommages. L'entreprise peut alors examiner les problèmes d'architecture ou de comportement des utilisateurs et apporter des améliorations, favorisant ainsi l'optimisation continue de la sécurité de l'information au sein de KKBOX Group. À l'avenir, KKLab prévoit d'établir un modèle pour l'expérience de parcours Zero Trust et de le fournir à des entreprises extérieures au groupe, afin qu'un grand nombre d'entreprises puissent en bénéficier.

Article original publié par iThome, 7 décembre 2020.

Le groupe KKLab Keke Experimental Co., Ltd. a été créé en 2019. Il développe une technologie pionnière, accélère le développement du secteur, participe à la transformation digitale des entreprises et peut fournir simultanément « l'intelligence artificielle (IA) et le machine learning, la construction et l'exploitation de plateformes cloud, ainsi que l'ingénierie de fiabilité des sites Web (SRE) » et d'autres services à guichet unique. KKLab dispose également d'une équipe d'accélération du développement de services innovants/IP pour aider à développer de nouvelles opportunités commerciales. À l'heure actuelle, la portée des services s'étend à de nombreux secteurs tels que les médias, le divertissement, les télécommunications, les soins médicaux et la plastification. Nous continuons à améliorer la technologie et à approfondir notre connaissance du secteur, et nous nous efforçons de créer plus de valeur pour les clients et le secteur. www.kklab.com.