

AKAMAI-KUNDENREFERENZ

KKLab

Das Venture Studio führt die Zero-Trust-Lösung von Akamai ein, die Flexibilität und Schutz sowohl für interne und als auch für externe Netzwerke kombiniert

100

E-Mails mit schädlichem Inhalt werden automatisch pro Tag blockiert



Proof of Concept in nur 30 Minuten erstellt



Verbessert die Sicherheit und wahrt die Flexibilität

Ungefähr im Jahr 2015 begann die F&E-Abteilung von KKBOX, das 2019 zum innovativen Forschungsunternehmen KKLab wurde, sich mit Informationssicherheit zu befassen. Das F&E-Team führte verschiedene Versuche durch und beauftragte ein externes Team von Fachleuten mit Hacking-Angriffssimulationen und Penetrationstests, um potenzielle Schwachstellen an Systemen aufzudecken und zu beheben. Das Unternehmen entschied sich für die Implementierung einer Multi-Faktor-Authentifizierung und führte außerdem Akamai Secure Internet Access Enterprise ein, um gezielte Angriffe zu verhindern. Darüber hinaus wurde Akamai Enterprise Application Access implementiert, um einen sicheren Zugriff auf Anwendungssysteme zu gewährleisten. Mit der Einführung dieser beiden cloudbasierten Informationssicherheitservices setzte das Unternehmen Zero-Trust-Sicherheit um.

Mit einer Zero-Trust-Architektur gehören Schwachstellen herkömmlicher VPNs der Vergangenheit an

Laut Hung-Yi Chen, Assistant Vice President bei KKLab, war die KKBOX Group schon immer technologieorientiert. Er fing im Jahr 2005, während er noch mitten im Studienabschluss steckte, bei der Gruppe an und konzentriert sich seit 15 Jahren auf technologische Forschung und Entwicklung. Die Gruppe wuchs weiter und er unterstützte die Einführung vieler interessanter und herausfordernder neuer Technologien. Dazu gehörten die Einrichtung eines Engineering-Teams für Website-Zuverlässigkeit im Jahr 2010, die Einführung von CI/CD und die Implementierung einer Hybrid-Cloud-Architektur. Später wechselte er zu KKLab, einem cloudbasierten Technologiedienstleister, der Chens Forschungsergebnisse zur Cloud und zu künstlicher Intelligenz nutzt, um Unternehmen bei der Förderung des technologischen Wandels zu unterstützen.

KKLab bietet Technologiedienstleistungen für verschiedene Unternehmen innerhalb der Gruppe, darunter KKBOX, KKTv, KKStream, KKTIX und theFARM. Darüber hinaus arbeitet das Unternehmen mit externen Unternehmen zusammen, wobei es sich auf Toolketten für künstliche Intelligenz und maschinelles Lernen, Big-Data-Hochgeschwindigkeits-Computing-Plattformen, den Aufbau mehrerer Hybrid Clouds und Beratungsservices konzentriert. Das Unternehmen erweiterte seinen digitalen Support um Services für Unternehmen in Bereichen wie High-Tech-Fertigung, Einzelhandelslogistik, Medien und Unterhaltung, Finanzen und Versicherungen.

KKLab

KKLab
Taipeh, Taiwan
www.kklab.com

Branche
Medien

Herausforderung
Übergang zu Zero-Trust-Sicherheit mit Multi-Faktor-Authentifizierung, Zugriffssicherheit für Anwendungssysteme und Verhinderung gezielter Angriffe

Lösungen

- [Secure Internet Access Enterprise](#)
- [Enterprise Application Access](#)



KKLab bietet aber nicht nur technische Services, sondern auch Informationssicherheit als zentrales Ziel an. Das Unternehmen führte speziell Funktionen zum Testen der Informationssicherheit von Drittanbietern ein und nutzte Hacking-Angriffssimulationen, um potenzielle Sicherheitsschwachstellen in seinen Systemen aufzudecken. Viele Mitarbeiter waren sich sicher, dass die Informationssicherheit im Unternehmen bereits hoch war und den Tests problemlos standhalten würde. Aber ein simulierter Angriff auf eine Datenbank zeigte, dass viele Konten und Passwörter von Hackern kompromittiert werden konnten. Das KCLab-Team erkannte, dass das herkömmliche Framework für Informationssicherheit und der Zugriff auf Intranet-Ressourcen über ein VPN tatsächlich ziemlich unsicher waren. Sobald ein Hacker an ein Passwort für ein internes Konto gelangt, kann er dem VPN folgen, um ins Intranet zu gelangen und Informationen nach Belieben zu stehlen, wodurch die Gruppe großen Geschäftsrisiken ausgesetzt wird.

Um diesen Risiken entgegenzuwirken, hat KCLab zweistufige Maßnahmen zur Verbesserung der Sicherheit ergriffen. Zunächst einmal wird die Multi-Faktor-Authentifizierung erzwungen. Jeder muss das Kontopasswort und den Code für das Einmalpasswort gleichzeitig eingeben, bevor eine Verbindung zum VPN hergestellt werden kann. Darüber hinaus plant KCLab aktiv eine Zero-Trust-Architektur, die kontinuierlich überprüft und sicherstellt, dass jeder Besucher wirklich ein legitimer Nutzer ist. Das Endziel von KCLab ist es, eine flexiblere und sicherere Arbeitsumgebung zu schaffen, die auf Zero Trust basiert.

Ein Sicherheitsnetz mit Secure Internet Access Enterprise und Enterprise Application Access blockiert jede verdächtige Verbindung

Chen betont, dass sich die KKBOX Group, die sich auf Services im Bereich Unterhaltungsmedien und Streaming-Technologie konzentriert, Flexibilität wünscht, um schädliches Verhalten sofort zu blockieren. Das Unternehmen will keine übermäßigen Kontrollmaßnahmen ergreifen, die die Kreativität der Mitarbeiter einschränken. Deshalb empfiehlt KCLab die Einführung des Zero-Trust-Modells. Die Lösung muss einfach bereitzustellen und zu warten sein und gleichzeitig den Workflow des Nutzers so wenig wie möglich beeinträchtigen. Aufgrund dieser Anforderungen entschied sich das Unternehmen für die Lösungen von Akamai.

Chen dazu: „Akamai Secure Internet Access Enterprise ist in erster Linie für das Filtern und Analysieren von Verbindungen aus dem Intranet zuständig und muss bestimmen, ob das Ziel über eine schädliche IP-Adresse oder Domain verfügt. Der Schlüssel liegt in der Big-Data-Datenbank.“ Er fügt hinzu, dass Akamai einen hohen Marktanteil habe. Zum einen hat sich KCLab wegen der Basis auf CDN- und Anti-DDoS-Services für Akamai entschieden. Diese erfassen eine große Menge an Daten zu schädlichem Verhalten. Die leistungsstarken Ressourcen sind eine wichtige Grundlage für den effektiven Betrieb von Secure Internet Access Enterprise.

Und zum anderen unterscheiden sich die Bereitstellungsanforderungen von anderen Lösungen auf dem Markt, die Secure Internet Access Enterprise ähneln. Einige erfordern die Installation eines Agents auf jedem Endgerät und andere die Installation eines Connectors im Backbone-Netzwerk des Unternehmens. Akamai unterstützt hingegen gleichzeitige Verbindungen. Der Akamai Connector ist ein schlankes Image einer virtuellen Maschine, und nur wenige Netzwerkeinstellungen müssen angepasst werden. Im Jahr 2018 hat KCLab den Proof of Concept in nur 30 Minuten abgeschlossen. Dieser bestätigte, dass Secure Internet Access Enterprise mit dem Akamai Connector und der umfangreichen Datenbank den Anforderungen gerecht werden konnte. Daher entschied sich das Unternehmen für die Zusammenarbeit mit Akamai.



Akamai Secure Internet Access Enterprise ist in erster Linie für das Filtern und Analysieren von Verbindungen aus dem Intranet zuständig und muss bestimmen, ob das Ziel über eine schädliche IP-Adresse oder Domain verfügt. Der Schlüssel liegt in der Big-Data-Datenbank.

Hung-Yi Chen

Assistant Vice President, KCLab

Zusätzlich zur Filterung interner und externer Verbindungen führte KCLab im Jahr 2020 Enterprise Application Access ein, um das Verhalten von Mitarbeitern zu steuern, die von jedem beliebigen Standort aus auf Intranet-Ressourcen zugreifen. Der Akamai Connector wurde mithilfe des Docker-Images bereitgestellt. Bisher hat KCLab über Enterprise Application Access mehr als 100 interne Anwendungssysteme verbunden. Auch wenn viele Partner komplizierte VPN-Kanäle für die Verbindung mit dem Intranet verwendeten, können sie jetzt das Modell von Enterprise Application Access nutzen, wodurch sie weniger Risiken bei der IT-Wartung eingehen müssen und Mitarbeitern den zusätzlichen Wartungsaufwand ersparen.

Seit der Implementierung der Lösung von Akamai hat sich KCLab zu mehr als nur einem Kunden entwickelt. KCLab verfügt über langjährige Erfahrung im Kundenservice für Unternehmen und hat viele Vorschläge und Anwendungsfälle bereitgestellt, die für Kunden hilfreich sind, wie z. B. das Hinzufügen zusätzlicher Informationen im Reporting. So wollte KCLab nicht nur die Statistiken von Ereignissen in Zusammenhang mit Trojanern oder Phishing aus einem bestimmten Zeitraum erfahren, sondern auch wissen, wer und welches Gerät diese Ereignisse ausgelöst hat. Außerdem schlugen sie vor, dem Text und den Zahlen in Berichten Datenvisualisierungen wie Kreisdiagramme, Balkendiagramme und Liniendiagramme hinzuzufügen. Akamai reagierte schnell auf diese Vorschläge und passte seine Berichte an, was allen Nutzern einen Vorteil bietet.

Heute blockiert die KKBBOX Group mit dem Schutz der Zero-Trust-Lösung von Akamai automatisch durchschnittlich etwa 100 E-Mails pro Tag, die versuchen, Nutzer mit Websites mit schädlicher Werbung, Schadprogrammen oder Phishing-Versuchen zu verbinden. KCLab kann nun ganz leicht verdächtiges Verbindungsverhalten erkennen und so Sicherheitsvorfälle vermeiden. Das Unternehmen kann dann Probleme in der Architektur oder im Nutzerverhalten überprüfen und Verbesserungen vornehmen und so die Informationssicherheit bei der KKBBOX Group kontinuierlich stärken. Mit Blick auf die Zukunft plant KCLab, ein Modell für die Zero-Trust-Journey zu etablieren und dieses als Service für Unternehmen außerhalb der Gruppe bereitzustellen, damit eine Vielzahl von Unternehmen davon profitieren können.

[Ursprünglicher Artikel von iThome](#), 7. Dezember 2020.



KCLab Keke Experimental Co., Ltd. wurde 2019 gegründet. Das Unternehmen entwickelt wegweisende Technologien, beschleunigt die industrielle Entwicklung und unterstützt die digitale Transformation von Unternehmen. Gleichzeitig kann es „künstliche Intelligenz und maschinelles Lernen, Aufbau und Betrieb von Cloud-Plattformen sowie Website-Betriebssicherheit (SRE)“ sowie andere Services aus einer Hand bereitstellen. KCLab verfügt außerdem über ein innovatives Team zur Beschleunigung der Service-/IP-Bereitstellung, das die Entwicklung neuer Geschäftsmöglichkeiten unterstützt. Derzeit umfasst das Leistungsspektrum viele Branchen wie Medien, Unterhaltung, Telekommunikation, medizinische Versorgung und Plastifizierung. Wir verbessern die Technologie, fördern die Branchen und streben danach, mehr Wert für Kunden und die Branche zu schaffen:

www.kclab.com