HISTÓRIA DO CLIENTE DA AKAMAI

KKLab

O venture studio implementa a solução Zero Trust da Akamai, combinando flexibilidade e proteção para redes internas e externas

100

E-mails com conteúdo mal-intencionado bloqueados automaticamente por dia

Prova de conceito definida em apenas 30 minutos

Fortalece a segurança e mantém a flexibilidade

Por volta de 2015, a unidade de pesquisa e desenvolvimento da KKBOX, que se tornou a inovadora empresa de pesquisa KKLab em 2019, passou a dar mais atenção à segurança da informação. A equipe de pesquisa e desenvolvimento realizou diferentes experimentos e contratou uma equipe externa de profissionais para realizar exercícios de intrusão de hackers e testes de penetração para descobrir possíveis violações em sistemas que pudessem ser refinados e aprimorados. A unidade decidiu implementar a autenticação multifator e implementou o Akamai Secure Internet Access Enterprise para evitar ataques direcionados e o Akamai Enterprise Application Access para garantir a segurança do acesso aos sistemas das aplicações. Com a introdução desses dois serviços de segurança de informações baseados em nuvem, a empresa criou a segurança Zero Trust.

A mudança para uma arquitetura Zero Trust reforça as vulnerabilidades das VPNs tradicionais

Hung-Yi Chen, vice-presidente assistente da KKLab, disse que o KKBOX Group sempre foi voltado à tecnologia. Ele ingressou no grupo enquanto concluía seus estudos em 2005, e concentrou-se em pesquisa e desenvolvimento de tecnologia por 15 anos. À medida que o grupo cresceu, ele ajudou a introduzir muitas novas tecnologias interessantes e desafiadoras. Isso incluiu o estabelecimento de uma equipe de engenharia de confiabilidade de websites em 2010, a introdução de CI/CD e a implantação de uma arquitetura de nuvem híbrida. Mais tarde, Chen ingressou na KKLab, um provedor de serviços de tecnologia baseado em nuvem que usa sua base de pesquisa sobre nuvem e inteligência artificial para ajudar as empresas a promover a transformação tecnológica.

A KKLab oferece suporte a serviços de tecnologia para várias empresas do grupo, como KKBOX, KKTV, KKStream, KKTIX e theFARM. Ela também trabalha com empresas externas através de seu enfoque em cadeias de ferramentas de inteligência artificial e machine learning, plataformas de computação de alta velocidade de big data, construção de várias nuvens híbridas e serviços de consultoria. A empresa expandiu seu suporte digital para fornecer serviços a empresas em áreas como fabricação de alta tecnologia, logística de varejo, mídia, entretenimento, finanças e seguros.

KKLab
Taipé, Taiwan
www.kklab.com

Setor
Mídia

Desafio
Mudar para a segurança Zero Trust com autenticação multifator, segurança de acesso ao sistema de aplicações e prevenção adicional contra ataques direcionados

Soluções
- Secure Internet Access Enterprise
- Enterprise Application Access

Ao mesmo tempo em que fornece serviços técnicos, a KKLab também inclui a segurança das informações como meta essencial. A empresa introduziu especialmente recursos de teste de segurança de informações de terceiros e usou exercícios de invasão por hackers para revelar possíveis pontos fracos de segurança em seus sistemas. Muitas pessoas na empresa estavam confiantes de que ela tinha um alto nível de segurança da informação e que resistiria facilmente ao teste. Mas um teste de ataque ao banco de dados revelou que muitas contas e senhas poderiam ser comprometidas por hackers. Isso fez com que a equipe da KKLab percebesse que a estrutura tradicional de segurança das informações e o conceito de acesso aos recursos da intranet por meio de uma VPN são, na verdade, bastante perigosos. Quando um hacker obtém uma senha de conta interna, ele pode seguir a VPN para entrar na intranet e roubar informações à vontade, expondo o grupo a grandes riscos operacionais.

Para neutralizar os riscos, a KKLab adotou medidas de reforço de segurança em dois estágios. Primeiro, a autenticação multifator é aplicada. Todos devem digitar a senha da conta e o código de uso único em conjunto para se conectar à VPN. Além disso, a KKLab está planejando ativamente uma arquitetura Zero Trust, que verificará continuamente se cada visitante é realmente um usuário legítimo. O objetivo final da KKLab é criar um ambiente de trabalho mais flexível e seguro com base em Zero Trust.

Construção de uma rede de proteção com o Secure Internet Access Enterprise e o Enterprise Application Access para bloquear todas as conexões suspeitas

Chen observou que o KKBOX Group, voltado a serviços de tecnologia de streaming e mídia de entretenimento, espera aproveitar essa flexibilidade e bloquear imediatamente o comportamento malicioso. A empresa não quer tomar medidas de controle excessivas que inibam a criatividade dos colegas, e é por isso que a KKLab recomenda a adoção do modelo Zero Trust. A solução deve ser fácil de implantar e manter, afetando o fluxo de trabalho do usuário o mínimo possível. Com base nesses requisitos, a empresa decidiu trabalhar com as soluções da Akamai.

Chen afirma: “O Akamai Secure Internet Access Enterprise é responsável, principalmente, por filtrar e analisar conexões da intranet e determinar com precisão se o endereço IP ou o domínio do destino é mal-intencionado. A chave está no banco de dados de big data." Ele também comentou que a Akamai tem uma alta participação no mercado. A primeira razão pela qual a KKLab escolheu a Akamai é a base construída a partir de serviços de CDN (Rede de Entrega de Conteúdo) e anti-DDoS, da qual uma grande quantidade de dados de comportamento malicioso é coletada. Esses recursos avançados servem como o núcleo da operação eficaz do Secure Internet Access Enterprise.

O segundo motivo: os requisitos de implantação são diferentes ao analisar soluções semelhantes ao Secure Internet Access Enterprise disponíveis no mercado. Alguns requerem a instalação de um agente em cada dispositivo de endpoint e outros requerem a instalação de um conector na rede de backbone corporativa. A Akamai suporta conexões simultâneas. O Akamai Connector é uma imagem de máquina virtual leve, e apenas algumas configurações de rede precisam ser definidas. Em 2018, a KKLab concluiu a prova de conceito em apenas 30 minutos. Através de seu amplo banco de dados de inteligência, confirmou-se que o Secure Internet Access Enterprise, em conjunto com o Akamai Connector, atenderia às necessidades da empresa, que decidiu trabalhar com a Akamai.

> “O Akamai Secure Internet Access Enterprise é responsável, principalmente, por filtrar e analisar conexões da intranet e determinar com precisão se o endereço IP ou o domínio do destino é mal-intencionado. A chave está no banco de dados de big data.
>
> **Hung-Yi Chen**
> Vice-presidente assistente da KKLab

Além de filtrar conexões internas e externas, a KKLab implementou o Enterprise Application Access em 2020 para controlar o comportamento dos funcionários que acessam recursos da intranet de locais diferentes. A empresa implantou o Akamai Connector usando a imagem do Docker. Até agora, a KKLab conectou mais de 100 sistemas internos de aplicações por meio do Enterprise Application Access. Embora muitos parceiros tenham usado canais de VPN mais complicados para se conectar ao sistema de intranet, agora eles podem usar o modelo do Enterprise Application Access, que previne mais riscos de manutenção de TI e poupa os colegas da carga extra de manutenção.

Desde a implantação dos serviços da Akamai, a KKLab cresceu para se tornar algo mais do que apenas um cliente. A KKLab tem profunda experiência no atendimento ao cliente corporativo e forneceu muitas sugestões e casos de uso que são úteis aos clientes, como adicionar informações mais detalhadas ao relatório. Por exemplo, além de conhecer as estatísticas de eventos como cavalos de Troia ou phishing durante um determinado período, a KKLab queria saber quem e qual dispositivo acionou esses eventos. A empresa também sugeriu a adição de visualizações de dados, como gráficos de pizza, gráficos de barras e gráficos de linhas, juntamente com texto e números em relatórios. A Akamai respondeu rapidamente a essas sugestões, ajustando seus relatórios e oferecendo maiores benefícios aos usuários globais.

Atualmente, sob a proteção da solução Zero Trust da Akamai, o KKBOX Group bloqueia automaticamente uma média diária de cerca de 100 e-mails que tentam levar os usuários a websites com anúncios mal-intencionados, programas maliciosos ou comportamentos de phishing. A KKLab consegue notar facilmente qualquer comportamento de conexão suspeito e evitar problemas antes que eles causem danos. Dessa forma, a empresa pode analisar problemas na arquitetura ou no comportamento do usuário e fazer melhorias, promovendo o aprimoramento contínuo da segurança das informações no KKBOX Group. No futuro, a KKLab planeja estabelecer um modelo para a experiência da jornada Zero Trust e fornecê-lo como um serviço a empresas fora do grupo, para que uma variedade de empresas possam se beneficiar dele.

Artigo original publicado por iThome, 7 de dezembro de 2020.

A KKLab Keke Experimental Co., Ltd. foi fundada em 2019. Ela desenvolve tecnologia pioneira, acelera o desenvolvimento industrial, auxilia na transformação digital das empresas e pode, simultaneamente, fornecer "inteligência artificial e machine learning, construção e operação de plataformas de nuvem e SRE (engenharia de confiabilidade de websites)", além de outros serviços centralizados. A KKLab também tem uma equipe inovadora de aceleração de desenvolvimento de serviço/IP para ajudar no desenvolvimento de novas oportunidades de negócios. Atualmente, o escopo dos serviços abrange muitos setores, como mídia, entretenimento, telecomunicações, assistência médica e plastificação. Continuamos aprimorando a tecnologia e expandindo o setor, fazendo o possível para criar mais valor para os clientes e para o segmento. www.kklab.com