HISTÓRIA DO CLIENTE DA AKAMAI

Universidade de Tunghai

O Akamai Secure Internet Access Enterprise melhora a segurança da Universidade de Tunghai e reduz o tempo de gerenciamento de incidentes

Akamai ajuda universidade a poupar recursos da equipe de segurança e a reduzir notificações externas de segurança

As organizações modernas enfrentam ciberameaças complexas, uma vez que invasores usam métodos cada vez mais sofisticados para contornar nossas defesas. Como você equilibra a necessidade de proteção proativa contra esses ataques com a necessidade de flexibilidade e liberdade em uma população universitária grande e global?

Esse foi o desafio que a equipe do Centro de computação da Universidade de Tunghai enfrentou. A universidade adotou o aprendizado digital e desenvolveu um campus inteligente, que oferece aos alunos e funcionários acesso gratuito à Internet sem fio de alta velocidade, dentro e fora do campus. No início de cada ano acadêmico, os alunos conectam seus notebooks à rede da universidade.

No entanto, como a política de TI não exigia a instalação de antivírus nos dispositivos dos alunos, muitos dos notebooks eram infectados por malware. Esses dispositivos comprometidos causaram falhas em redes dentro e fora do campus, consumiram largura de banda excessiva e geraram tráfego de botnets maliciosos. Além disso, o malware se moveu lateralmente para os computadores gerenciados pela universidade, resultando no recebimento de notificações do Centro regional de redes de Taichung informando que a rede da Universidade de Tunghai havia sido atacada e estava fazendo conexões anormais.

“O Centro de computação forneceu treinamento de segurança da informação e solicitou que os alunos e a equipe do corpo docente não clicassem em nenhum link estranho nos e-mails ou nas páginas da web”, diz Chien-Hui Ou, diretor de tecnologia de rede. “Mas os invasores continuaram a criar táticas cada vez mais ardilosas que dificultavam a identificação do que era ou não legítimo, tornando os usuários vítimas dos ataques”.

Universidade de Tunghai
Taichung, Taiwan
eng.thu.edu.tw

Setor
Setor público

Solução
Secure Internet Access Enterprise

Principais impactos

- Melhor postura de segurança e redução do tempo de gerenciamento de segurança e resolução de incidentes
- Bloqueio proativo do tráfego do servidor de comando e controle de dispositivos infectados e redução do movimento lateral
- Redução do volume de notificações de segurança externas
- Orçamento de segurança otimizado movendo o investimento de CapEx para OpEx

"As soluções tradicionais de segurança de informações e softwares antivírus que dependem da análise e identificação de códigos mal-intencionados não são rápidas o suficiente. Se uma nova variante de malware aparecer e os fornecedores de antivírus ainda não tiverem descoberto seu código e assinaturas atualizadas, o malware não será detectado", diz Kuang-Chin Chang do Grupo de redes da Universidade de Tunghai. "E devido à tendência de criptografar o tráfego da Web, os invasores também estão agora usando esses canais criptografados para lançar ataques, tornando cada vez mais difícil de impedir ataques de dia zero".

Akamai interrompe conexões suspeitas com eficiência

Ao perceber que a universidade precisava melhorar sua postura em relação à segurança, a equipe do Centro de computação começou a analisar os produtos que utilizavam o DNS como um ponto de controle de segurança. Para ela, essa abordagem permitiria que a universidade melhorasse sua segurança geral sem afetar a liberdade acadêmica.

Por meio de um processo de avaliação de concorrentes, a universidade escolheu o Akamai Secure Internet Access Enterprise como solução prioritária. O Secure Internet Access Enterprise é um serviço baseado em nuvem que protege proativamente uma rede e seus usuários analisando todas as solicitações de DNS. A partir da inigualável visibilidade de tráfego da Internet que a Akamai possui, todas as solicitações são comparadas a dados de inteligência de ameaças em tempo real antes que o conteúdo Web solicitado seja bloqueado ou entregue.

"O Secure Internet Access Enterprise detecta e bloqueia solicitações de DNS para domínios com possível conteúdo malicioso, como malware de mineração de moedas ou ransomware, ou que possam roubar informações de usuários", diz Chang. "Mesmo que o computador de um aluno seja infectado por malware durante o uso fora do campus, o malware não conseguirá se conectar externamente ao servidor de comando e controle dos invasores quando o computador retornar à rede do campus."

Antes do Secure Internet Access Enterprise, mitigar um incidente de segurança da informação era uma tarefa difícil. Quando um relatório de uma conexão anormal era recebido, a equipe de gerenciamento de rede normalmente tinha que usar endereços IP para rastrear o computador comprometido, encontrar registros de conexão de arquivos de log para convencer a parte afetada de que um incidente havia ocorrido, e então pedir que cooperasse com os procedimentos de limpeza de vírus.

"Era por isso que levávamos cerca de uma semana para resolver um incidente. E isso consumia uma grande quantidade de nossos recursos de segurança", diz Chang. "No entanto, após implantarmos o Secure Internet Access Enterprise, o número de incidentes de segurança relatados despencou, permitindo que nossos recursos se destinassem a outros projetos de segurança."

Chang acrescenta: "O Secure Internet Access Enterprise é especialmente rápido e fácil de implantar e configurar, o que o diferencia de equipamentos físicos tradicionais, que requerem primeiro a desconexão da rede e depois o teste antes que um sistema seja ativado. Com o Secure Internet Access Enterprise, basta direcionar o tráfego de DNS diretamente para a plataforma da Akamai e o processo estará concluído em questão de minutos."

O diretor Ou afirma: "O Secure Internet Access Enterprise fornece relatórios de incidentes detalhados automaticamente para que a equipe de segurança identifique rapidamente com qual malware os computadores dos clientes foram infectados ou quais links da Web foram abertos antes de os computadores serem infectados por malware de mineração de moedas. Os dados se integram ao nosso SIEM, de modo que os relatórios também ajudam a equipe a entender qualquer atividade anormal recente na rede para que possamos responder de forma proativa".

Após implantarmos o Secure Internet Access Enterprise, o número de incidentes de segurança relatados despencou, permitindo que nossos recursos se destinassem a outros projetos de segurança.

Kuang-Chin Chang
Grupo de rede da Universidade de Tunghai

Economia significativa de mão de obra e custos

Chao-Tung Yang, Diretor do centro de computação eletrônica da Universidade de Tunghai, enfatiza os benefícios estratégicos. “A segurança da informação é importante agora e será cada vez mais no futuro à medida que as aplicações digitais crescerem. A Tunghai sempre priorizou a proteção de aplicações de TI e da segurança da informação, e o presidente da universidade apoia o investimento.”

Yang continua, “Quando observamos a direção atual de crescimento da TI, fica evidente que os serviços baseados em nuvem vieram para ficar. Os sistemas de defesa anteriores foram implantados com uma combinação de software e hardware, e sua manutenção, atualização de patches etc., exigia mão de obra e tempo”.

Os serviços baseados em nuvem da Akamai mudam isso, permitindo uma redução total da mão de obra de manutenção. Yang está otimista sobre o futuro dos serviços de segurança da informação baseados em nuvem e afirma: “Além de reduzirem a mão de obra, eles também reduzirão a necessidade de espaço em salas de computadores físicos e economizarão em ar-condicionado e eletricidade. Isso se alinha à proposta do Centro de computação de reduzir a quantidade de energia usada nas salas de equipamentos”.

“Quanto ao custo, o uso de serviços baseados em nuvem, ao contrário da compra imediata de equipamentos físicos, não exige um grande e único investimento de fundos”, diz Yang. “Como é arrendado anualmente, o Secure Internet Access Enterprise é mais fácil de ser adquirido pelas universidades.”

“A segurança da informação está sempre em andamento. Com o Secure Internet Access Enterprise, as atividades de gerenciamento de incidentes diminuem significativamente, proporcionando mais recursos para fortalecer as defesas contra ataques de botnet e análises de atividades mais abrangentes,” conclui Yang.

> O Secure Internet Access Enterprise é especialmente rápido e fácil de implantar e configurar, o que o diferencia de equipamentos físicos tradicionais, que requerem primeiro a desconexão da rede e depois o teste antes que um sistema seja ativado.
>
> **Kuang-Chin Chang**
> Grupo de rede da Universidade de Tunghai

A Universidade de Tunghai foi fundada em 1955, e foi a primeira universidade privada de Taiwan. É a primeira e única instituição de ensino com um programa educacional completo, do jardim de infância ao PhD. Atualmente, Tunghai tem nove faculdades: Faculdade de Artes, Faculdade de Ciências, Faculdade de Engenharia, Faculdade de Administração, Faculdade de Ciências Sociais, Faculdade de Agricultura, Faculdade de Belas Artes e Design Criativo, Faculdade de Direito e Faculdade Internacional. Tunghai tem aproximadamente 17 mil alunos e cerca de 500 professores: http://eng.thu.edu.tw/.