HISTÓRIA DO CLIENTE DA AKAMAI

Universidade estadual seleciona a Akamai para proteger a tecnologia operacional de edifícios críticos em 24 campi

Visibilidade abrangente da rede

Políticas de segmentação

Detecção e resposta a ameaças

O cliente

Grande universidade estadual

Esta grande universidade estadual atende às necessidades de ensino superior de mais de 100.000 alunos, com mais de 17.000 professores e funcionários em seus 24 *campi*.

O desafio

Centralizando a infraestrutura de rede de mais de 600 edifícios

Uma importante universidade estadual queria incorporar sistemas de automação predial com segurança em uma iniciativa de campus inteligente em todo o estado. A equipe responsável pela planta física da universidade e pelos sistemas de OT estava preocupada com a falta de segmentação que protegesse esses dispositivos e aplicações. Eles também estavam preocupados com a rede de TI da universidade se ela fosse removida de seu estado de rede desconectada. Como resultado, a equipe responsável empreendeu um esforço ambicioso para centralizar seus sistemas de automação predial e melhorar a segurança.

O líder do projeto da universidade explicou: "Até cerca de dois anos atrás, todos os *campi* eram praticamente independentes. Estávamos hospedando o servidor de aplicações principal, mas os controladores individuais do campus estavam em redes de TI e nem sempre segmentados em VLANs separadas do restante do tráfego do campus."

Isso significava que um ataque aos sistemas de controle de um único edifício poderia se espalhar facilmente para a rede de TI de um campus ou vice-versa.

Havia uma razão econômica adicional para o projeto também. "A universidade queria fazer o gerenciamento de energia e ver onde poderíamos cortar custo", explicou o líder do projeto, "mas não estávamos obtendo nenhum dado dos *campi* porque eram todos sistemas autônomos.

"Então precisávamos conectá-los, mas precisávamos fazer isso com segurança. Com as conexões provenientes desses *campi* remotos em nosso data center, eles podem criar um backdoor em nossa rede para um possível ataque."

Large State University

Setor
Educação

Solução
Akamai Guardicore Segmentation

Principais impactos
- Prevenção da movimentação lateral
- Ringfencing de aplicação

Akamai

O ambicioso projeto de trazer tudo para uma infraestrutura de rede compartilhada cobriu mais de 600 edifícios em 24 campi em seu escopo. A equipe de Facilities Automation do departamento foi selecionada para executar o projeto.

No entanto, a grande complexidade dos sistemas de automação da universidade e o número de fornecedores envolvidos apresentavam outro enorme desafio.

"Estamos gerenciando sistemas de elevadores, HVAC, análise de vibração, iluminação, distribuição elétrica e medição elétrica. Depois, temos todas as nossas principais utilidades, incluindo geração de vapor, distribuição elétrica e tratamento de águas residuais. Lidamos com mais de 260 empreiteiros que trabalham nesses sistemas em todas as várias empresas." Todos esses fornecedores precisavam de acesso à rede, sem introduzir riscos ou interferir nos sistemas de controle uns dos outros.

> Um sistema de gerenciamento de firewall não pode competir com a Akamai.
>
> Líder de projeto da universidade

A escolha da solução

Procuram-se: Visibilidade de tráfego leste-oeste e políticas centralizadas

A Tempered Networks, um provedor de segurança focado em sistemas de controle inteligentes e redes da Internet das Coisas, foi usada para abordar as conexões norte-sul entre os campi remotos e o data center principal da universidade. Com esse desafio sob controle, a universidade ainda enfrentava o problema de proteger contra violações mais de 300 servidores em execução no data center.

"Estávamos procurando soluções que supostamente lidassem com o tráfego leste-oeste, mas nenhuma era tão limpa e simples quanto queríamos", lembrou o líder do projeto da universidade.

A equipe descobriu a Akamai quando se deparou com sua ferramenta gratuita de simulação de ataque e violação, o Infection Monkey. O Infection Monkey ajuda os operadores de data center a avaliar a resiliência de seus ambientes a ataques pós-violação e movimentação lateral.

Depois que a equipe baixou a ferramenta e começou a usá-la, percebeu que o Akamai Guardicore Segmentation poderia resolver os problemas descobertos pelo Infection Monkey.

O Akamai Guardicore Segmentation é uma das poucas soluções no mercado hoje focada principalmente na microssegmentação. Ele torna mais fácil para os operadores definir, criar e implantar políticas de segurança para controlar as comunicações entre aplicações individuais ou agrupadas logicamente.

Logo na primeira apresentação com a universidade, a equipe da Akamai demonstrou os recursos exclusivos de visualização da plataforma. Usando o Akamai Guardicore Segmentation, os operadores de data center podem ver todas as aplicações em execução em seu ambiente e mapear graficamente as dependências entre elas.

"Resolveu instantaneamente para nós. Sabíamos que era exatamente disso que precisávamos."

Akamai Guardicore Segmentation

Akamai versus firewalls internos

"Com o gerenciamento de firewall central, você ainda precisa configurar as regras para cada firewall individualmente. Com a Akamai, podemos criar um grupo de aplicações e dizer: 'Queremos que esses sistemas conversem apenas entre si.'"

Os firewalls também apresentam problemas de custo, recursos e capacidade de gerenciamento. "O gerenciamento de todos esses firewalls seria apenas um pesadelo. Provavelmente precisaríamos de meia dúzia de pessoas apenas para implantar o sistema e garantir que não houvesse problemas, e pelo menos duas pessoas dedicadas apenas para gerenciá-lo."

Além disso, os firewalls não têm flexibilidade para definir e modificar políticas no nível da aplicação. "Com a Akamai, podemos ouvir por um tempo e entender o que está acontecendo entre os sistemas e por que eles precisam se comunicar. Com firewalls, é tudo ou nada. Um firewall só vai bloquear porta a porta, e é isso."

Microssegmentação com gerenciamento centralizado e fácil

A velocidade e a facilidade com que os membros da equipe podem criar e implantar regras foram citadas como outro benefício significativo.

"No primeiro dia em que o ligamos, instalamos em algumas caixas e, em seguida, tentamos criar uma política para impedir que um fornecedor pudesse ver outro. E assim, bloqueou o primeiro fornecedor. Isso provou para mim que este produto era o que procurávamos", observou o líder do projeto.

As ferramentas e a metodologia de microssegmentação da Akamai não exigem um especialista. "Ter algo simples o suficiente para que qualquer pessoa em nossa equipe possa usar foi uma grande vantagem para mim."

Além da microssegmentação: detecção e resposta

A visibilidade obtida com a Akamai teve o benefício adicional de revelar anomalias operacionais no data center. "Encontramos um serviço de spool de impressão conectando-se a uma rede que não era nossa", contou o líder do projeto. "Quando finalmente o localizamos, era a sessão de área de trabalho remota de alguém que desconectou, mas nunca encerrou, e estava continuamente tentando se comunicar com o servidor de impressão em seu PC. Se esse PC for comprometido, pode ser um caminho de volta para o servidor de aplicações."

Agora que a equipe está usando ativamente a Akamai, a universidade já está vislumbrando mais aprimoramentos de segurança e eficiência que a solução possibilita.

"Um projeto futuro está automatizando muitas das funcionalidades da rede caso ocorra um incidente. Por exemplo, se detectarmos um endereço MAC não autorizado ou ponto de acesso de um edifício, poderíamos usar o Akamai Guardicore Segmentation para enviar um comando para a solução Tempered Networks para bloquear esse edifício e, em seguida, enviar um alerta a um operador para corrigi-lo e descobrir o que aconteceu. Até agora, não tínhamos essa capacidade de detecção."

A plataforma da Akamai permitiu que a equipe de automação de instalações da universidade atingisse o estado de segurança desejado com mais rapidez e facilidade do que o previsto. "Nunca tivemos uma ferramenta proativa como essa que monitora tudo constantemente", explicou o líder do projeto.

Como a Akamai está monitorando o tráfego leste-oeste do data center, a equipe não precisa fazer isso. "Quero que nossa equipe possa se concentrar em nosso trabalho, que é ajudar a universidade a economizar energia e economizar dinheiro. Não podemos nos concentrar nisso se tivermos que nos preocupar com o que está acontecendo no data center."

A equipe da universidade decidiu encontrar uma solução simples de microssegmentação. Com a Akamai, eles descobriram isso e muito mais.

"Ele faz o que diz que faz."

Acesse akamai.com/guardicore para mais informações.

> “Assim que o instalamos, a equipe conseguiu entrar, implantá-lo e colocar algumas regras de proteção em vigor, e eles acreditaram nisso.
>
> Líder de projeto da universidade

 | Suporte | Publicado em 06/23