HISTÓRIA DO CLIENTE DA AKAMAI

Provedor de infraestrutura de comunicações

detém ataques de ransomware imediatamente com a Akamai

Prevenção contra a possível perda de US$ 1 milhão

Prevenção contra possível TI sombra

Visibilidade do tráfego leste-oeste

O cliente

Esse provedor de infraestrutura de comunicações dos EUA garante que as empresas e os cidadãos permaneçam conectados no mundo acelerado de hoje. A empresa é responsável por diversas redes de fibra e torres de telefonia usadas por clientes diariamente.

Os desafios

Visibilidade e controle limitado do ponto de extremidade

Com mais de 6.000 notebooks utilizados em toda a organização, a equipe de segurança de TI tinha preocupações crescentes sobre o risco da frota ao ambiente de TI mais amplo. Além disso, problemas contínuos com a atividade TI sombra de alguns dos usuários avançados da empresa precisavam ser resolvidos.

Embora algumas medidas de segurança tivessem sido aplicadas pela equipe de computação de usuários finais, elas eram limitadas. Nenhuma delas conseguia controlar de forma granular o acesso de usuários ao sistema ou limitar a comunicação ponto a ponto para interromper a propagação de malware de forma eficaz, sendo esta uma grande preocupação para a organização.

Para lidar com essas lacunas, as partes interessadas queriam melhorar a postura de segurança da empresa, introduzindo uma solução que permitisse estender a visibilidade e os controles de segmentação granulares para os dispositivos dos funcionários. Isso também garantiria a capacidade de observar e evitar movimentações laterais não autorizadas.

A escolha da solução

As partes interessadas nos processos de segurança já estavam considerando implementar a Akamai Guardicore Segmentation há algum tempo, e estavam interessadas em usá-la para vários casos de uso de cibersegurança. A organização escolheu uma abordagem em fases para ver o grande potencial da visibilidade granular e facilitar o processo de criação de políticas.

Provedor de infraestrutura de comunicações

Localização
Estados Unidos

Setor
Infraestrutura de comunicações

Solução
Akamai Guardicore Segmentation

Principais impactos
- Prevenção contra ransomware
- Interrupção da TI sombra
- Visibilidade do tráfego leste-oeste

Como as políticas de segmentação definidas por software da Akamai não estão vinculadas à infraestrutura subjacente, o provedor podia optar por abordar todas as iniciativas de segurança. No entanto, a frota de notebooks dos funcionários foi identificada como de alto risco. Por isso, a equipe priorizou a implantação de agentes da Akamai nos pontos de extremidade.

Akamai Guardicore Segmentation

Assim que o projeto começou, foi rápida a implementação do agente Windows simplificado da Akamai nos computadores da organização. Isso estendeu a visibilidade do processo para o acesso de usuários e a atividade de notebooks.

A equipe de segurança de TI conseguiu criar e gerenciar controles de segurança para esses pontos de extremidade centralmente, tudo com base nos dados precisos do ambiente. Em seguida, ela configurou rapidamente várias políticas, inclusive um alerta sobre atividades específicas do Remote Desktop Protocol (RDP) da Microsoft, incluindo tentativas de login malsucedidas.

Visibilidade granular em ação

Em um curto período de tempo após a implantação, a política configurada para relatar atividades incomuns relacionadas ao RDP forneceu uma série de alertas. Ficou óbvio que um invasor estava tentando um ataque de força bruta, quando foram observados casos subsequentes de tentativas malsucedidas de login.

A equipe de segurança de TI acompanhou atentamente a situação e, à medida que os invasores continuaram o ataque, tomou a decisão de bloquear o RDP em cada ponto de extremidade com um agente da Akamai. Com apenas alguns cliques, a equipe criou e aplicou uma nova política de segmentação que desativava o RDP, interrompendo o invasor antes que um único ponto de extremidade fosse comprometido.

Ransomware interrompido imediatamente

Durante o processo postmortem, a equipe de segurança rapidamente percebeu que todos os indicadores apontavam para um importante e conhecido agente de ameaça de ransomware.

Se a campanha tivesse sido bem-sucedida, os invasores provavelmente tentariam prosseguir com suas táticas habituais, criptografando tudo ao seu alcance antes de emitir um pedido de resgate. Devido ao porte da organização do fornecedor e às tendências atuais, as exigências dos invasores teriam certamente ultrapassado US$ 1 milhão. Se os ativos essenciais aos negócios, como o sistema ERP, tivessem sido comprometidos, isso geraria interrupção e tempo de inatividade significativos.

No entanto, graças à ação rápida da equipe de segurança e à Akamai, a tentativa de ataque não causou impactos na organização.

Interrupção da TI sombra

Além de impedir ameaças externas, a equipe também conseguiu lidar com desafios internos usando a plataforma. Antes da Akamai, a visibilidade dos pontos de extremidade era limitada. Por isso, alguns usuários tinham mais facilidade para burlar processos oficiais, executando atividades por conta própria que não estavam em conformidade com as políticas da organização. A nova percepção e a capacidade de impor controles de segurança em pontos de extremidade permitiram que a segurança de TI restringisse a TI sombra. Isso incluiu impedir que os membros da organização DevOps ativassem novos recursos por conta própria sem passar por canais oficiais para autorização.

Aumento da proteção com a Akamai

Para o provedor de infraestrutura de comunicações, a proteção dos pontos de extremidade é apenas o começo. Ele planeja explorar novos recursos, implementar a Akamai em seu data center, proteger seu ambiente Citrix e aplicar controles de acesso de terceiros a fornecedores externos.

Com a natureza flexível da plataforma, a equipe tem a garantia de que pode estender a proteção contra ameaças avançadas em qualquer lugar do ambiente, independentemente de como suas estratégias de fusão e aquisição ou iniciativas de transformação digital acontecerão no futuro.

Acesse akamai.com/guardicore para obter mais informações.

 | Suporte | | Publicado em 05/23