HISTÓRIA DO CLIENTE DA AKAMAI

# Empresa de remediação de violações aproveita a Akamai na resposta e recuperação de ransomware

Visibilidade abrangente da rede

Segmentação entre infraestruturas de TI

Resposta a ameaças de ransomware

## O cliente

Uma empresa de serviços de remediação de violações com sede nos EUA foi contratada por um fabricante global de equipamentos após um grande incidente de segurança.

## O desafio

### Ransomware que se espalha rapidamente

Após um ataque bem-sucedido de propagação de malware que afetou as operações comerciais, o fabricante global começou a trabalhar com a empresa de serviços de remediação de violações para restaurar e melhorar a segurança em seu ambiente. O ataque, iniciado a partir do laptop de um funcionário, se espalhou rapidamente e impactou a maioria dos locais operacionais, além de penetrar nos servidores de backup da organização.

## A escolha da solução

Os métodos de contenção iniciais, como a aplicação de regras de restrição de acesso à Internet em firewalls, demoraram a conter o rápido agravamento da violação. A complexidade do ambiente e a realidade da rede em uma empresa distribuída tornaram a implementação e a aplicação de regras de restrição com firewalls um processo lento e ineficaz.

Além disso, a visibilidade das máquinas legadas era um problema significativo para os responsáveis pela resposta a incidentes pela investigação e contenção da violação. Observando a urgência e a necessidade de acelerar a segmentação antes que a disseminação lateral impactasse ainda mais ativos, o provedor de serviços de remediação de violação recomendou Akamai Guardicore Segmentation.

Breach Remediation Company

**Setor**
Tecnologia da Informação

**Solução**
Akamai Guardicore Segmentation

**Principais impactos**

- Mitiga a disseminação de ransomware por meio de movimento lateral
- Fornece visibilidade granular dos fluxos de rede
- Protege máquinas modernas e antigas
- Permite resposta rápida a incidentes

Akamai

## Benefícios da Akamai Guardicore Segmentation

### Visibilidade instantânea

Dentro de três horas, a organização de serviços de remediação de violações provisionou rapidamente agentes da Akamai em mais de 3.000 servidores da empresa. E apenas alguns minutos após a implantação, a visibilidade granular dos fluxos de rede e comunicações começou a surgir, dando à equipe de resposta a incidentes o contexto e os dados precisos necessários para investigar a violação e validar a contenção.

### Rapidez na implantação da política

Logo depois de obter a visibilidade necessária, as equipes tomaram medidas para segmentar ativos críticos a partir de um ambiente mais amplo. Duas aplicações de produção cruciais, responsáveis pela única linha de fabricação em funcionamento, foram rapidamente identificadas e protegidas. Usando Akamai Guardicore Segmentation, uma política foi imediatamente introduzida para restringir as conexões entre as sub-redes infectadas e partes do data center e as aplicações, uma tarefa que levaria semanas com firewalls legados.

Uma consulta simples também revelou que as máquinas legadas conectadas à Internet, ignorando firewalls legados, tentaram restrições de contenção. Depois de descobrir comunicações não conformes, a equipe criou políticas que restringiram efetivamente o acesso à Internet para todos os servidores, incluindo máquinas legadas, em poucos minutos.

### Prevenir movimentos laterais durante a recuperação

Durante a parte seguinte do processo de recuperação, a equipe recriou os clusters de aplicações do fabricante, incorporando os agentes da Akamai. Eles configuraram uma política inicial que bloqueou todas as conexões de entrada e usaram Akamai Guardicore Segmentation para identificar dependências. Em seguida, as comunicações foram permitidas com base na necessidade, somente após validar os requisitos e entender o contexto. Essa abordagem permitiu que a equipe recuperasse e trouxesse os aplicativos afetados pelo ataque de ransomware online sem o risco de reinfecção.

### Proteção futura

A Akamai Guardicore Segmentation permitiu que a empresa de serviços de correção de violações demonstrasse um valor agregado significativo para seu cliente, o fabricante, ajudando-o a se recuperar do ataque de ransomware. Isso abriu a oportunidade para a empresa de serviços aumentar a receita, expandir sua presença e ajudar melhor os clientes a atingir as metas de TI e segurança.

A segmentação interna do data center introduzida durante a recuperação em fases reduziu significativamente a superfície de ataque. Hoje, a postura de segurança da organização melhorou, e o impacto de qualquer violação futura foi bastante reduzido.

Acesse akamai.com/guardicore para obter mais informações.

> A [Akamai], em até quatro horas, impediu que o ataque se espalhasse e restaurou linhas de produção interrompidas em um segmento de rede "estéril" sem modificar qualquer rede subjacente. Tudo isso durante a investigação e contenção contínuas de IR.
>
> CISO na empresa de remediação de violações