HISTÓRIA DO CLIENTE DA AKAMAI

Grande empresa de serviços financeiros protege o acesso remoto com a Akamai após ataque de ransomware

Visibilidade abrangente da rede

Rapidez na implantação da política

Força de trabalho remota protegida

O cliente

Uma grande empresa de serviços financeiros sediada no Brasil.

O desafio

Maior acesso remoto

Semelhante a muitas organizações, a pandemia do COVID-19 levou ao aumento das necessidades de acesso remoto neste provedor de serviços financeiros, e grande parte da equipe de TI do banco passou a trabalhar em casa em dispositivos gerenciados pela empresa. À medida que os usuários começaram a acessar os dados e aplicações necessários para suas funções principalmente fora da rede corporativa segura, a superfície de ataque da organização cresceu rapidamente.

Incidente de ransomware bem-sucedido

Logo após a transição para um modelo de trabalho em casa, um ataque de ransomware bem-sucedido atingiu um banco de dados Oracle Cloud essencial no banco, que eles descobririam mais tarde como originário de um ambiente VDI. A segurança e a TI sabiam que precisavam tomar medidas rápidas para limitar a perda de dados financeiros confidenciais. Além disso, eles entenderam que, se não pudessem determinar e proteger o vetor de ataque original, haveria um risco real de o ransomware se espalhar lateralmente para os servidores de backup e o ambiente de produção da organização. Se isso acontecesse, o banco certamente seria afetado por perdas financeiras e de dados significativas.

A escolha da solução

A Akamai Guardicore Segmentation já estava sendo usada amplamente em outras áreas do banco. Antes do ataque de ransomware, a plataforma era responsável por gerenciar e aplicar as políticas de segmentação de mais de 23.000 servidores com cargas de trabalho abrangendo infraestrutura local, virtual, bare-metal e VDI, bem como ambientes de contêiner Azure e OpenShift.

Large Financial Services Company

Setor
Serviços financeiros

Solução
Akamai Guardicore Segmentation

Principais impactos

- Mitiga a disseminação de ransomware por meio de movimento lateral
- Fornece visibilidade granular dos fluxos de rede
- Protege o acesso remoto por meio da segmentação de ambientes de VDI
- Permite resposta rápida a incidentes

Akamai

Como uma solução de segmentação baseada em software, ela havia sido usada pelo banco anteriormente para realizar várias iniciativas de segurança e conformidade, incluindo o gerenciamento de acesso à jump box do administrador e a segmentação de aplicações Swift. Conhecendo o histórico da plataforma de fornecer excelente visibilidade e rápido tempo de implementação da política, a equipe de resposta se movimentou rapidamente para aproveitar os recursos da Akamai Guardicore Segmentation e enfrentar a violação.

Benefícios da Akamai Guardicore Segmentation

Visibilidade no nível do processo

Usando a plataforma, a equipe de resposta do banco investigou fluxos históricos de comunicação. Eles rastrearam a introdução inicial do ransomware à conexão VDI remota de um administrador de banco de dados que se comunica com um banco de dados Oracle Cloud.

Rapidez na implantação da política

Depois de identificar o vetor de ataque, a equipe acelerou a segmentação de VDI, tornando-a uma prioridade. O processo de planejamento de políticas começou em um sábado, usando os recursos de visibilidade da Akamai Guardicore Segmentation para definir possíveis necessidades de políticas. Na terça-feira seguinte, o banco tinha políticas aplicáveispara as mais de 3.000 conexões VDI com o Oracle Cloud.

Recuperação após ataque de ransomware

A equipe implantou agentes da Akamai na aplicação de backup e configurou o isolamento ("ringfencing") da aplicação, definindo (até o nível do processo) o que poderia se comunicar com o ativo. Depois, eles foram implantados na área violada, impedindo que o ransomware se propagasse ainda mais, usando regras globais de negação.

Para reduzir o risco adicional de acesso de funcionários remotos, também foram definidas políticas para as duas soluções de VDI usadas pelos funcionários do call center, evitando ainda mais o movimento lateral não autorizado entre endpoints do banco.

Ao aplicar a política de segmentação em apenas três dias, a organização de serviços financeiros reduziu consideravelmente o impacto do incidente de ransomware e melhorou significativamente a segurança do acesso remoto.

> A visibilidade fornecida pela [Akamai Guardicore Segmentation] foi como um feixe de luz brilhante que afastou a escuridão!
>
> Chefe de segurança da infraestrutura na grande empresa de serviços financeiros

Acesse akamai.com/guardicore para obter mais informações.