RESUMO DA SOLUÇÃO DA AKAMAI

Preparação de instituições financeiras para conformidade com o PCI DSS com a Akamai

Com o PCI DSS v4.0 trazendo as mudanças mais significativas nos padrões de segurança do setor de cartões de pagamento desde que 2004, as instituições financeiras devem se adaptar rapidamente para permanecer em conformidade. Essa estrutura abrangente, estabelecida pelo PCI Security Standards Council, define medidas rigorosas para proteger os dados de titulares de cartões. As soluções da Akamai capacitam as instituições financeiras a atender a esses requisitos dinâmicos por meio de recursos avançados de segurança, monitoramento contínuo e testes de penetração robustos. Nossas ferramentas são projetadas para simplificar a conformidade, proteger as informações dos clientes e ajudar sua instituição a se preparar até o prazo final do PCI, em março de 2025.

Conformidade unificada: simplificação do PCI DSS com um provedor

Para as instituições financeiras, a conformidade com o PCI DSS envolve não apenas treinamento de funcionários e políticas corporativas, mas também um software de segurança sofisticado para atender à maioria dos requisitos. Dada a natureza abrangente desses requisitos, isso geralmente significa trabalhar com vários provedores. Alguns requisitos podem exigir um firewall, enquanto outros incluem o gerenciamento de identidades. As instituições financeiras que trabalhem com um único fornecedor com tecnologia integrada se beneficiarão de um processo de auditoria simplificado e mais segurança para as informações financeiras de seus clientes. A adoção de soluções robustas de cibersegurança que atendam a esses requisitos como parte de uma estratégia de segurança mais ampla pode resultar na economia dos custos e na redução da complexidade no longo prazo. O portfólio de soluções da Akamai aborda de forma abrangente os requisitos existentes e futuros do PCI DSS, proporcionando uma experiência perfeita para instituições financeiras.

Benefícios

- **Simplifique os fluxos de trabalho de segurança e conformidade**
- **Reduza os encargos de auditoria com recursos dedicados do PCI**
- **Receba e registre alertas de conformidade práticos do PCI**
- **Proteja dados financeiros confidenciais**
- **Aumente a eficiência operacional e reduza os custos com a conformidade**

Sobre o escopo

A questão do escopo é um desafio significativo para qualquer instituição financeira que queira atender aos requisitos do PCI DSS. Os aplicativos e ambientes de rede considerados "dentro do escopo" pelo PCI podem ser complexos, abrangendo diferentes tipos de infraestrutura, tecnologia e local. À medida que as instituições financeiras adotam uma infraestrutura de nuvem e aplicativos baseados em SaaS, esse ambiente híbrido de serviços no local e sob demanda traz uma camada adicional de complexidade. Para as instituições financeiras, incluindo aquelas com empreendimentos de comércio eletrônico com escalonamento automático, conhecer a localização de uma determinada carga de trabalho a qualquer momento pode ser um grande desafio.

As instituições financeiras têm recorrido a firewalls internos, VLANs e listas de controle de acesso para lidar com o desafio do escopo. No entanto, esses aplicativos legados geralmente não conseguem acompanhar o ritmo dos ambientes híbridos e trazem outras complexidades, tempo de inatividade e sobrecarga operacional, além de falhas de segurança.

A Akamai Guardicore Segmentation oferece visibilidade do CDE (Cardholder Data Environment, ambiente de dados de titulares de cartões) e seus limites, uma etapa crucial no processo de conformidade. Essa visibilidade ajuda as instituições financeiras a cumprir vários requisitos do PCI DSS e proporciona uma visão geral abrangente da rede. Por exemplo:

- O requisito 1.2.3 exige que as organizações tenham um diagrama de sua rede. O painel da Akamai Guardicore Segmentation exibe todos os vínculos entre o CDE e outras redes, ajudando as instituições financeiras a atender a esse requisito.
- O requisito 1.2.4 exige que as organizações mantenham um fluxograma de dados que mostre como os dados das contas são transmitidos entre sistemas e redes. O painel de controle da Akamai Guardicore Segmentation ajuda as instituições financeiras a validar esse requisito ao exibir as conexões necessárias.

Sobre os controles

- O requisito 1.2.5 especifica a necessidade de identificar, aprovar e ter uma justificativa de negócios clara para todos os serviços, protocolos e portas permitidos. A Akamai Guardicore Segmentation ajuda as instituições financeiras a atender a esse requisito implementando políticas universalmente impostas, determinando quais protocolos ou serviços são permitidos e quais não são.

Sobre a proteção do lado do cliente

As instituições financeiras que aceitam dados de cartões de pagamento não são apenas responsáveis por seus próprios ambientes. O uso do JavaScript no desenvolvimento moderno da Web trouxe inovação e consistência, mas também criou problemas para processadores de cartões de pagamento. A execução descentralizada do JavaScript no lado do cliente e as dependências de terceiros fazem com que seja extremamente difícil para as instituições financeiras monitorarem e gerenciarem esse aspecto. Os invasores exploram esse ponto cego injetando código prejudicial em websites do lado do cliente para roubar dados confidenciais. Esses tipos de ataque, incluindo skimming na Web, formjacking e Magecart, cresceram em popularidade, o que levou a novos requisitos em torno das proteções do lado do cliente e do monitoramento de scripts.

O PCI DSS v4.0 exigirá que as instituições financeiras rastreiem, inventariem e justifiquem todo o JavaScript em execução nas páginas de pagamento de seu website voltado para o público. De acordo com o requisito 6.4.3, as empresas precisarão garantir a integridade comportamental e a autorização de todos os scripts, bem como fornecer um inventário desses scripts com justificativa por escrito de sua necessidade individual. Além disso, de acordo com o requisito 11.6.1, as instituições financeiras precisarão detectar e responder a quaisquer alterações não autorizadas feitas em suas páginas de pagamento. A equipe autorizada deve ser alertada sobre qualquer modificação, incluindo indicadores de comprometimento, alterações, adições ou exclusões em

Com a Akamai Guardicore Segmentation, reduzimos significativamente nossa superfície de ataque sem nenhum dos custos e atrasos associados à atualização de firewalls legados.

– Dave Wigley,
CISO, Daiwa Capital Markets Europe

cabeçalhos HTTP e conteúdo de página de pagamento pelo navegador do consumidor.

Em resumo, o PCI DSS v4.0 exige que as instituições financeiras:

- Mantenham um inventário e uma justificativa de cada script executado nas páginas de pagamento
- Certifiquem-se de que todos os scripts estejam autorizados e executem as ações a que se destinam
- Estabeleçam mecanismos de detecção, alerta e resposta para lidar com alterações não autorizadas em scripts, violação de proteção e exfiltração de dados em páginas de pagamento

O Akamai Client-Side Protection & Compliance oferece amplo suporte para ajudar as instituições financeiras a cumprir os requisitos 6.4.3 e 11.6.1 do PCI DSS v4.0. Ele rastreia e inventaria os scripts em páginas de pagamento automaticamente, impulsionando sua integridade e autorização. As equipes de segurança podem facilmente justificar a finalidade dos scripts executados em páginas de pagamento, com justificativas predefinidas e regras automatizadas. A solução também monitora as alterações nos cabeçalhos HTTP e nas proteções da página de pagamento para se defender contra adulteração da página. Um painel abrangente e alertas de PCI dedicados facilitam a resposta rápida a eventos relacionados à conformidade e fornecem evidências para auditoria.

Proteção contra ataques

Proteger os dados de titulares de cartão é um princípio fundamental do PCI DSS, mas à medida que os aplicativos da Web e as APIs proliferam, eles também podem se tornar pontos de entrada para os invasores. Para estarem em conformidade com o PCI DSS, as instituições financeiras precisam de proteções sólidas contra malware, ataques de dia zero e outras ações que possam levar ao vazamento de dados.

O Akamai App & API Protector, com o módulo Malware Protection, pode ajudar as instituições financeiras a se proteger contra o vazamento de dados de cartões de pagamento analisando os arquivos na edge da rede antes que eles possam entrar e começar a espalhar malware. As APIs podem introduzir novas vulnerabilidades que serão exploradas pelos invasores que buscam dados de cartões de pagamento. Muitas instituições financeiras não podem sequer contabilizar todas as suas APIs, muito menos atestar que elas estão seguras. Qualquer API que receba ou transmita dados de titulares de cartões está no escopo do PCI DSS, o que significa que as instituições financeiras precisam monitorar o desenvolvimento e a autenticação das API e protegê-las.

O Akamai API Security automatiza a descoberta contínua de APIs em todo o seu ambiente. Ele atribui uma pontuação de risco à API e ao ponto de extremidade comparando as APIs à documentação existente e notificando as equipes de segurança, desenvolvimento e API sobre configurações incorretas e vulnerabilidades. Essa automação contínua significa que as vulnerabilidades são avaliadas quando você finaliza as atualizações de seu patrimônio de APIs.

Conclusão

Embora o objetivo final da implementação de controles do PCI DSS seja proteger os dados de titulares de cartões, protegendo, também, seus clientes e sua empresa, as instituições financeiras ainda precisam atender às exigências dos auditores. É aí que um provedor exclusivo oferece vantagens distintas. Com a visualização histórica e em tempo real de sua rede, você pode atender a muitos aspectos da sua auditoria com mais rapidez e facilidade. Além disso, trabalhar com um único provedor com liderança demonstrada no setor — e um conjunto de clientes que cumpriram os requisitos do PCI DSS com sucesso — pode levar a implementações mais tranquilas, auditorias mais rápidas e suporte contínuo de conformidade. A visibilidade abrangente e as soluções integradas da Akamai ajudam as instituições financeiras a simplificar os esforços de conformidade e fortalecer suas defesas contra ameaças em evolução.

Para saber mais, acesse akamai.com ou entre em contato com a equipe de vendas da Akamai.