Akamai 솔루션 설명서

금융 기관의 Akamai를 통한 PCI DSS 컴플라이언스 대비 | Akamai

2004년 이후 결제 카드 업계 보안 표준에 가장 큰 변화를 불러온 PCI DSS v4.0에 따라 금융 기관은 신속한 적응을 통해 컴플라이언스를 유지해야 합니다. PCI 보안 표준 협의회(PCI Security Standards Council)가 수립한 이 포괄적인 프레임워크는 카드 소유자 데이터를 보호하기 위한 엄격한 조치를 의무화하고 있습니다. Akamai의 솔루션은 고급 보안 기능, 지속적인 모니터링, 강력한 모의 해킹을 통해 금융 기관이 이러한 진화하는 요구사항을 충족할 수 있도록 지원합니다. Akamai의 툴은 컴플라이언스를 간소화하고, 고객 정보를 보호하고, 금융 기관이 PCI의 2025년 3월 마감 기한까지 준비하도록 지원합니다.

통합 컴플라이언스: 단일 공급업체를 통한 PCI DSS 간소화

금융 기관의 PCI DSS 컴플라이언스에는 직원 교육과 기업 정책뿐 아니라 대부분의 요구사항을 충족하기 위한 정교한 보안 소프트웨어가 필요합니다. 이러한 요구사항의 포괄적인 특성을 고려할 때, 이는 종종 여러 공급업체와 협력하는 것을 의미합니다. 일부 요구사항에는 방화벽이 필요한 경우도 있고, ID 관리가 필요한 경우도 있습니다. 통합 기술을 갖춘 단일 공급업체를 찾을 수 있는 금융 기관은 감사 프로세스가 간소화되고 고객 금융 정보에 대한 보안이 강화되는 장점을 누릴 수 있습니다. 광범위한 보안 전략의 일환으로 이러한 요구사항을 충족하는 강력한 사이버 보안 솔루션을 도입하면 장기적으로 비용을 절감하고 복잡성을 줄일 수 있습니다. Akamai의 솔루션 포트폴리오는 기존 및 향후 PCI DSS 요구사항을 포괄적으로 해결해 금융 기관에 원활한 경험을 제공합니다.

범위 문제 해결

PCI DSS 요구사항을 충족하고자 하는 금융 기관에 있어 중요한 도전 과제는 범위 문제입니다. PCI에서 '범위 내'로 간주하는 애플리케이션과 네트워크 환경은 다양한 종류의 인프라, 기술, 위치에 걸쳐 복잡할 수 있습니다. 금융 기관이 클라우드 인프라와 SaaS 기반 애플리케이션을 도입함에 따라 온프레미스 및 온디맨드 서비스의 하이브리드 환경이 복잡성을 더하고 있습니다. 자동 확장형 이커머스 비즈니스를 운영하는 금융 기관을 포함한 금융 기관의 경우, 특정 워크로드의 위치를 언제든지 파악하는 것이 특히 어려울 수 있습니다.

금융 기관은 범위 문제를 해결하기 위해 내부 방화벽, VLAN, 접속 제어 목록에 의존해 왔습니다. 그러나 이러한 레거시 애플리케이션은 하이브리드 환경을 따라잡는 데 어려움을 겪는 경우가 많아 복잡성, 다운타임, 운영 오버헤드가 증가하는 동시에 보안 공백이 발생하게 됩니다.

장점

- **보안 및 컴플라이언스 워크플로우 간소화**
- **전용 PCI 기능으로 감사 부담 감소**
- **실행 가능한 PCI 컴플라이언스 알림 수신 및 기록**
- **민감한 금융 데이터 보호**
- **운영 효율성 향상 및 컴플라이언스 비용 절감**

Akamai Guardicore Segmentation은 컴플라이언스 프로세스에서 중요한 단계인 CDE(Cardholder Data Environment)와 해당 경계에 대한 가시성을 제공합니다. 이러한 가시성을 통해 금융 기관은 PCI DSS의 여러 요구사항을 충족하고 네트워크에 대한 포괄적인 감독을 수행할 수 있습니다. 예를 들면 다음과 같습니다.

- 요구사항 1.2.3에 따라 기업은 네트워크 다이어그램을 보유해야 합니다. Akamai Guardicore Segmentation의 대시보드는 CDE와 다른 네트워크 간의 모든 링크를 표시해 금융 기관이 이 요구사항을 충족할 수 있도록 지원합니다.
- 요구사항 1.2.4에 따라 기업은 계정 데이터가 시스템과 네트워크 간에 어떻게 이동하는지 보여주는 데이터 흐름의 다이어그램을 유지 관리해야 합니다. Akamai Guardicore Segmentation의 대시보드는 필요한 연결을 표시해 금융 기관이 이 요구사항을 검증할 수 있도록 지원합니다.

제어 해결

- 요구사항 1.2.5에는 허용된 모든 서비스, 프로토콜, 포트에 대해 식별, 승인, 명확한 비즈니스 정당성을 확보해야 할 필요성이 명시되어 있습니다. Akamai Guardicore Segmentation은 금융 기관이 보편적으로 적용되는 정책을 적용하고 허용되는 프로토콜이나 서비스를 결정함으로써 이 요구사항을 충족할 수 있도록 지원합니다.

클라이언트측 보안 해결

결제 카드 데이터를 수락하는 금융 기관은 자체 환경만 책임지는 것이 아닙니다. 최신 웹 개발에서 자바스크립트를 사용하면서 혁신과 일관성을 가져왔지만, 결제 카드 처리업체에는 새로운 과제를 안겨주기도 했습니다. 자바스크립트의 분산된 클라이언트측 실행과 써드파티 의존성으로 인해 금융 기관의 모니터링 및 관리가 매우 어렵습니다. 공격자들은 이러한 맹점을 악용해 클라이언트측 웹사이트에 유해한 코드를 삽입해 민감한 데이터를 탈취해 왔습니다. 웹 스키밍, 폼재킹, Magecart 등 이러한 종류의 공격이 증가하면서 클라이언트측 보안 및 스크립트 모니터링에 대한 새로운 요구사항이 생겨났습니다.

PCI DSS v4.0에 따라 금융 기관은 퍼블릭 웹사이트의 결제 페이지에서 실행되는 모든 자바스크립트를 추적, 인벤토리화, 정당화해야 합니다. 요구사항 6.4.3에 따라 모든 스크립트의 행동 무결성과 권한 부여를 보장하고, 해당 스크립트의 목록을 개별 필요성을 정당화하는 서면과 함께 제공해야 합니다. 또한, 요구사항 11.6.1에 따라 금융 기관은 결제 페이지의 무단 변경을 탐지하고 이에 대응해야 합니다. 소비자의 브라우저에서 HTTP 헤더와 결제 페이지 콘텐츠에 대한 감염, 변경, 추가, 삭제 등 모든 수정 사항이 발견되면 권한 있는 담당자에게 알려야 합니다.

> Akamai Guardicore Segmentation 덕분에 레거시 방화벽 업그레이드와 관련된 비용과 지연 없이 공격 표면을 크게 줄였습니다.
>
> **- 데이브 위글리(Dave Wigley), Daiwa Capital Markets Europe CISO**

요약하면, PCI DSS v4.0에 따라 금융 기관은 다음과 같이 조치해야 합니다.

- 결제 페이지에서 실행되는 모든 스크립트의 인벤토리와 정당성을 유지합니다.
- 모든 스크립트가 승인되고 의도한 작업을 실행하도록 합니다.
- 결제 페이지에서 스크립트 무단 변경, 보호 변조, 데이터 유출을 해결하기 위한 탐지, 알림, 대응 메커니즘을 구축해야 합니다.

Akamai Client-Side Protection & Compliance는 금융 기관이 PCI DSS v4.0의 요구사항 6.4.3 및 11.6.1을 준수할 수 있도록 광범위하게 지원합니다. 결제 페이지의 스크립트를 자동으로 추적하고 인벤토리를 생성해 무결성 및 권한 부여를 강화합니다. 보안팀은 사전 정의된 정당성 및 자동화된 룰을 통해 결제 페이지에서 실행되는 스크립트의 목적을 쉽게 정당화할 수 있습니다. 또한 HTTP 헤더의 변경 사항과 결제 페이지 보안 기능을 모니터링해 페이지 변조를 차단합니다. 포괄적인 대시보드와 전용 PCI 알림을 통해 컴플라이언스 관련 이벤트에 신속하게 대응하고 감사 근거를 쉽게 제공할 수 있습니다.

공격으로부터 보호

카드 소유자 데이터 보호는 PCI DSS의 핵심 원칙이지만 웹 애플리케이션과 API가 확산되면서 공격자의 진입 지점이 될 수도 있습니다. 금융 기관이 PCI DSS를 준수하려면 멀웨어, 제로데이 공격, 기타 데이터 유출로 이어질 수 있는 공격에 대한 강력한 방어가 필요합니다.

멀웨어 방어 모듈이 포함된 Akamai App & API Protector는 멀웨어가 내부로 침투해 멀웨어를 확산하기 전에 네트워크 엣지에서 파일을 스캔해 금융 기관이 결제 카드 정보 데이터 유출을 방지할 수 있도록 지원합니다. API는 결제 카드 데이터를 노리는 공격자가 악용할 수 있는 새로운 취약점을 야기할 수 있습니다. 많은 금융 기관은 API가 안전하다는 것을 증명하기는커녕 모든 API를 설명할 수도 없습니다. 카드 소유자 데이터를 수신하거나 전송하는 모든 API는 PCI DSS의 적용 범위에 속하므로 금융 기관은 API 개발 및 인증을 모니터링하고 이러한 API를 보호해야 합니다.

Akamai API Security는 기업 환경 전반에서 API의 지속적인 검색을 자동화합니다. API를 기존 문서와 비교하고 잘못된 설정과 취약점을 보안, 개발자, API 팀에 알림으로써 API와 엔드포인트에 리스크 점수를 할당합니다. 이러한 지속적인 자동화를 통해 API 자산에 대한 업데이트를 완료할 때 취약점을 평가할 수 있습니다.

결론

PCI DSS 제어 구축의 궁극적인 목표는 카드 소유자 데이터를 보호해 고객과 비즈니스를 보호하는 것이지만, 금융 기관은 여전히 감사자를 만족시켜야 합니다. 바로 이 부분에서 단일 공급업체가 뚜렷한 장점을 제공합니다. 네트워크에 대한 실시간 및 기록 보기를 통해 감사의 여러 측면을 더 빠르고 쉽게 충족할 수 있습니다. 또한, 업계에서 리더십을 입증한 단일 공급업체와 PCI DSS 요구사항을 성공적으로 충족한 고객사들과 협력하면 더 원활한 구축, 빠른 감사, 지속적인 컴플라이언스 지원으로 이어질 수 있습니다. Akamai의 포괄적인 가시성과 통합 솔루션은 금융 기관이 컴플라이언스 노력을 간소화하고 진화하는 위협에 대한 방어 체계를 강화할 수 있도록 지원합니다.

자세한 내용은 akamai.com에서 확인하거나 Akamai 영업 담당자에게 문의하시기 바랍니다.