Akamai | TechnologyAdvice

제로 트러스트 아키텍처가 금융 기관을 보호하는 3가지 방법

금융 기관을 대상으로 한 웹 애플리케이션 및 API 공격이 2023년 2분기에 전년 대비 65% 증가하면서 금융 기관은 계속해서 공격자의 주요 표적이 되고 있습니다. 진화하는 사이버 위협의 끊임없는 공격은 리소스를 소진할 뿐만 아니라 필수적인 핵심 비즈니스 기능에 대한 집중력을 분산시킵니다.

기존의 방화벽 및 엔드포인트 솔루션은 비밀번호와 사용자 이름을 입력하는 초기 스크리닝을 통과한 엔드포인트, 디바이스, 사용자를 암묵적으로 신뢰하며, 이러한 방식은 MFA(Multi-Factor Authentication)로 강화되기도 합니다. 네트워크 내의 애플리케이션, API, 시스템 서비스는 기본적인 엔드포인트 멀웨어 모니터링 이상의 보안 검사 없이 운영되는 경우가 많습니다. 이제 금융 기관은 랜섬웨어 위협의 확대, 엄격한 컴플라이언스 규정, 클라우드 전환이라는 도전과제에 대응하기 위해 제로 트러스트를 도입하고 있습니다.

제로 트러스트는 암묵적 신뢰를 제거하고 요청 및 권한의 맥락을 기반으로 모든 애플리케이션, 사용자, 디바이스에 대한 접속 권한을 지속적으로 확인합니다. 공격자가 디바이스나 인증정보를 감염시켜 네트워크에 접속하더라도 접속을 엄격하게 제한해 피해를 크게 줄일 수 있습니다.

그렇다면 제로 트러스트 프레임워크는 정확히 어떤 방법으로 금융 기관을 보호할까요?

끊임없이 변화하는 컴플라이언스

금융 기관은 잘 정립된 PCI DSS(Payment Card Industry Data Security Standard) 또는 2025년 1월에 전면 적용될 것으로 예상되는 DORA(Digital Operational Resilience Act) 같은 다양한 규정을 준수하기 위해 상당한 리소스를 투입해야 합니다. 불분명하고 상충되며 변화하는 요구 조건으로 인해 감사의 복잡성, 비용, 시간이 주기적으로 증가하고 있지만 감사에 실패하면 매출 손실, 규제 제재, 벌금 또는 과태료뿐만 아니라 평판 하락과 잠재적인 법적 책임으로 이어질 수 있기 때문에 금융 기관은 이에 투자할 수밖에 없습니다.

컴플라이언스 보고를 위해서는 규제의 대상이 되는 데이터를 다루는 시스템에 대한 명확하고 정확한 설명이 필요하며, 해당 시스템이 적절하게 보호되고 있다는 증거가 필요합니다. 하지만 대형 금융 기관의 경우, IT 환경이 너무 크고 상세하며 복잡해 자산과 접속을 쉽게 추적할 수 없습니다.

레거시 방화벽과 엔드포인트 보안은 주로 기존 사용자와 자산을 추적하고 보호합니다. 네트워크 세그멘테이션에 대한 기존의 접근 방식에 의존하면 운영 확장에 어려움이 있고, 정책 수립 및 적용에 방해가 되며, 민첩성이 제한됩니다.

미래 전략에 부합하는 기술로 레거시 환경의 문제를 극복하려면 금융 기관에 동서 트래픽에 대한 정밀한 가시성과 멀티클라우드 및 컨테이너 환경에서 세그멘테이션 정책을 적용할 수 있는 기능이 필요합니다. 컨테이너 기술을 포함해 여러 지역과 IT 인프라 종류를 관리해야 할 필요성이 커짐에 따라 금융 기관은 정책 유연성, DevOps 통합, 자동화를 갖춘 마이크로세그멘테이션을 위한 가장 빠르고 간단한 경로를 확보해야 합니다.

모든 리소스를 정기적으로 식별, 추적, 보호하지 않으면 금융 기관이 규제의 대상이 되는 데이터에 대한 접속을 완벽하게 제어하고 보호할 수 없습니다. 데이터, 사용자, 애플리케이션, 디바이스를 간과하거나 부적절하게 모니터링하면 사이버 공격의 리스크와 컴플라이언스 감사 실패 가능성이 크게 증가합니다.

제로 트러스트 아키텍처는 기본적으로 접속을 거부하며 모든 연결은 요청된 데이터에 대한 접속 권한이 있는 사용자, 권한 있는 디바이스, 맥락과 함께 명시적으로 부여되어야 합니다. 제로 트러스트는 기본적으로 최소 권한 접속 방식을 사용하며 잊혀졌거나 알 수 없는 레거시 연결은 중단합니다. Akamai의 솔루션은 오래된 지사 또는 인수한 기업의 레거시 기술 환경을 감염시키는 악성 디바이스, 레거시 사용자(사람, API, 애플리케이션), 잊혀진 데이터 소스를 신속하게 식별합니다.

Akamai의 제로 트러스트 아키텍처는 사용자의 위치에 관계없이 적용되지만, 접속 결정 과정에 위치 맥락이 포함될 수 있습니다. 보안팀은 로컬 네트워크, 데이터센터, 클라우드의 리소스에 대한 접속을 신속하게 분석하고 완벽하게 관리하는 데 필요한 통합 제어 및 보고 기능을 확보할 수 있습니다.

중요한 애플리케이션을 보호하고 동서 트래픽을 안전하게 보호해야 한다는 규제가 강화되면서 금융 기관은 환경에 대한 가시성과 이해도를 높이는 데 주력하고 있습니다. 이제 금융기관은 제로 트러스트 원칙을 통해 규정을 준수하지 않는 자산을 원활하게 식별하고 세그멘테이션함으로써 애플리케이션 팀이 세그멘테이션 정책을 자율적으로 관리하도록 지원할 수 있습니다. 이를 통해 효율적인 워크플로우를 보장하고 보고 프로세스를 간소화할 수 있습니다.

동서 트래픽의 맥락에 대한 풍부한 가시성이 확보되기 때문에 인프라나 애플리케이션의 변경 없이도 비즈니스 크리티컬 앱의 매핑과 링펜싱이 더욱 간편해집니다. 이 기능을 통해 써드파티 접속을 제한하고 전반적인 보안을 강화할 수 있습니다.

가시성을 확보하면 클라우드로 안전하고 간편하게 전환할 수 있고 세그멘테이션을 DevOps 주기에 통합하면 인프라를 크게 변경하지 않고도 정책을 즉시 업데이트할 수 있어 기존의 VLAN 관행에서 벗어날 수 있습니다. Akamai는 또한 여러 인프라에서 컴플라이언스 정책을 일관되게 생성, 적용, 보고할 수 있도록 지원하고 해당 과정을 간소화합니다. 이는 가시성 강화, 애플리케이션 의존성 매핑, 자동화된 세그멘테이션 정책, DevOps 정책 자동화, 원활한 변경 관리 통합 덕분에 가능한 일입니다.

랜섬웨어 확산 방지

랜섬웨어 공격은 전 세계적으로 헤드라인을 장식하고 있고 지사와 글로벌 금융 기관은 큰 어려움을 겪고 있습니다. CyberSecurity Ventures는 2022 랜섬웨어 시장 보고서에서 "랜섬웨어는 2031년에 2초마다 기업, 소비자, 디바이스를 공격할 것으로 예상됩니다."라고 밝혔습니다.

금융 서비스 기관은 인수 합병을 통해 성장하는 경우가 많기 때문에 전체 기술 생태계에 대한 가시성이 부족해 공격자에게 백도어를 열어두는 경우가 많습니다. 랜섬웨어 공격자는 백도어를 악용하거나, 피싱 공격을 통해 인증정보를 탈취하거나, 엔드포인트 보안을 회피하는 알려지지 않은 멀웨어를 엔드포인트에 배포합니다.

허용 수준이 과도한 사용자 접속 정책과 비밀번호 중심 인증은 공격자가 방화벽을 우회하고, 엔드포인트 탐지를 회피하고, 트래픽, 사용자, 연결된 디바이스를 암묵적으로 신뢰하는 네트워크에 제한 없이 접속하게 만들 수 있습니다. 랜섬웨어 공격자는 종종 CL0P처럼 기업화된 그룹으로 활동하며, 감염된 자산을 악용한 후 네트워크를 통해 측면으로 이동해 또 다른 취약한 자산을 발견하고 악용합니다. 공격자는 MOVEit SQL 인젝션 취약점 등의 제로데이 취약점을 통해 자동화된 스크립트를 사용하고, 시스템을 암호화하고, 데이터를 탈취하고, 몸값을 요구함으로써 빠르게 접속 권한을 획득하고 공격을 확산시킬 수 있습니다.

Akamai의 제로 트러스트 솔루션은 금융 기관이 중요 시스템을 식별 및 격리하고 이러한 시스템에 대한 네트워크 접속을 제한할 수 있도록 지원합니다. 이와 같은 접근 방식은 랜섬웨어 공격의 발생 가능성, 공격의 영향, 공격 복구에 소요되는 시간을 최소화합니다. Akamai는 초기에 악성 도메인과 IP 주소를 추적 및 모니터링하고 적절한 격리 블록을 구축해 많은 공격이 실행되지 못하도록 차단합니다.

이후에는 네트워크 트래픽에 대한 거의 실시간에 가까운 가시성을 바탕으로 트래픽을 프로세스 및 서비스 수준까지 관찰하고 제어합니다. 보안 운영 센터와 네트워크 운영 센터 팀은 이런 심층적인 인사이트를 통해 당면한 특정 위협을 정확하게 식별하고 표적으로 삼을 수 있습니다.

다음으로, 공격이 성공하더라도 Akamai Guardicore Segmentation에 내재된 마이크로세그멘테이션을 통해 공격 범위가 엄격하게 제한됩니다. 모든 접속 요청의 인증정보와 권한을 지속적으로 확인하며, Akamai Enterprise Application Access로 보호되는 애플리케이션에 대한 연결을 거부합니다.

또한 사용자에게 필요하지 않은 애플리케이션, 서버, 기타 리소스는 자동으로 검색되지 않도록 숨겨져 공격자의 측면 이동이나 접속 확장을 방지합니다. 마지막으로 Akamai Hunt의 비정상 탐지 기능은 비정상적인 행동을 표시해 데이터가 유출되거나 암호화되기 전에 공격을 식별할 수 있도록 보안팀에 알림을 보냅니다.

디지털 혁신 간소화

민첩성, 확장성, 현대화를 실현하기 위해 많은 금융 기관이 애플리케이션을 클라우드로 이전하고 있습니다. 그러나 이러한 전환에는 여러 가지 새로운 과제가 수반됩니다.

금융 기관은 우선 탐지되지 않았거나 알려지지 않은 리소스와 연결을 전환할 수 없습니다. 또한 클라우드 전환은 공격표면을 확장할 뿐만 아니라, 멀티클라우드 및 로컬 하이브리드 클라우드 통합으로 인해 애플리케이션이 중단되어 기존에 구축된 보안 레이어에 틈이 생기는 경우가 많습니다. 더불어 소프트웨어 배포형 인프라(컨테이너, 가상 머신 등)는 자동으로 너무 빠르게 배포되므로 레거시 솔루션으로는 효과적으로 보호하거나 모니터링하기 어렵습니다.

제로 트러스트 솔루션은 금융 기관이 보다 강력한 보호 기능과 운영 오버헤드 감소를 통해 클라우드 기반 애플리케이션을 보다 쉽게 배포할 수 있도록 지원합니다. Akamai의 제로 트러스트 솔루션은 모든 데이터 흐름을 추적해 잠재적인 공격표면을 신속히 식별하고 비즈니스 중단 없이 정책을 적용합니다.

식별이 완료되면 보안 및 운영팀이 Akamai의 중앙 집중식 제어 기능을 사용해 애플리케이션을 세그멘테이션 및 보호하고 데이터 흐름을 모니터링할 수 있습니다. Akamai는 세그멘테이션된 제어 기능을 제공하는 동시에 운영 비용과 복잡성을 줄여줍니다. 금융 기관의 보안 및 운영팀은 범용 정책을 적용해 인프라를 신속하고 민첩하게 최신화할 수 있습니다. 이는 진화하는 위협에 대한 강력한 방어막을 제공하는 최소 권한 제로 트러스트 세그멘테이션의 강력한 보안을 통해 달성할 수 있습니다.

금융 기관은 제로 트러스트를 무시할 수 없습니다.

레거시 기술에 대한 공격은 대규모 데이터 유출로 이어지고, 수백만 달러의 손실을 초래하고, 고객과 파트너의 신뢰를 무너뜨릴 수 있습니다. 공격은 점점 더 정교해지고 빨라지고 있으며, 기술 생태계에 대한 완벽한 가시성이 확보되지 않으면 금융 기관의 백도어가 열린 채 방치될 수 있습니다.

Akamai는 네트워크에 대한 가시성을 높이고, 지능적으로 사용자 접속을 제한하고, 지속적으로 위협을 추적하고, 보안 검토가 필요한 비정상을 표시합니다. Akamai 제로 트러스트 포트폴리오를 통해 금융 기관의 요구사항에 부합하는 방법에 대해 자세히 알아보시기 바랍니다.

Akamai와 함께 디지털 금융 보안에 대해 자세히 알아보세요

자세히 보기

TechnologyAdvice | Akamai

Akamai는 구축 및 전송되는 장소에 상관 없이 만들어지는 모든 것에 보안 기능을 내장하도록 지원함으로써 고객 경험, 직원, 시스템, 데이터를 보호합니다. Akamai 플랫폼은 글로벌 위협에 대한 가시성을 바탕으로 제로 트러스트 지원, 랜섬웨어 차단, 앱 및 API 보안 또는 DDoS 공격 차단을 목표로 보안 체계를 조정하고 발전시켜 지속적으로 안심하고 혁신하며 확장하고 가능성을 현실로 구현할 수 있도록 지원합니다. Akamai의 클라우드 컴퓨팅, 보안, 콘텐츠 전송 솔루션에 관해 자세히 알아보려면 akamai.com와 akamai.com/blog를 확인하거나 X(기존의 Twitter) LinkedIn에서 **Akamai Technologies를 팔로우하시기 바랍니다**.