Akamai 고객 사례

API를 발견하고 보호하는 금융 기업

숨겨진 API를 발견하고, API 리스크를 평가 및 방어하고, 규제 요구사항을 준수해 디지털 이니셔티브를 안전하게 추진한 은행의 사례

완전한 가시성 확보 | 보안 체계 강화 | 안전한 디지털 이니셔티브

금융 서비스 업계는 끊임없이 진화하는 시장에서 경쟁력을 유지하기 위해 디지털 전환을 빠르게 도입하고 있습니다. 금융 기관은 인공 지능 및 빅 데이터 애널리틱스와 같은 디지털 기능을 사용해 혁신적인 상품을 제공하고, 비용을 절감하고, 고객에게 더욱 개인 맞춤화되고 효율적인 서비스를 제공할 수 있습니다.

동시에 디지털 전환은 사이버 공격의 리스크도 증가시킵니다. 이렇게 증가하는 문제에 대응하려면 모든 디지털 전환 전략에 사이버 보안을 반드시 포함시켜야 합니다. 금융 서비스 기업은 악성 공격자로부터 고객의 데이터와 자산을 보호하기 위해 시스템의 보안과 안정성을 확보해야 합니다.

아시아의 유명한 시중 은행 한 곳은 API 보안 체계를 강화하기 위해 서둘러 Noname Security(현재 Akamai가 인수한 기업)를 찾았습니다. API 유출은 놀라운 속도로 이루어지고 있습니다. Tech Wire Asia는 "오늘날 사이버 인시던트 13건 중 1건은 API 보안 취약점이 원인일 수 있다."라고 지적했으며, "API 취약점으로 인해 기업이 연간 최대 750억 달러의 비용을 지출하고 있다."고 강조했습니다.

해당 은행 7000억 달러가 넘는 총 자산, 5000여 곳의 기업 고객, 자산 관리에서 세계적인 명성을 가지고 있기 때문에 가능한 한 빨리 모든 API 취약점을 해결해야 했습니다.

Financial Services

위치

아시아

업계

금융 서비스

솔루션

Akamai API Security

Akamai

API와 그 리스크에 대한 가시성 개선의 필요성

해당 기관은 이미 인증 및 트래픽 제어를 위한 API 관리 플랫폼을 배포했지만, API 남용과 사이버 공격을 방지할 수 있는 능력에 대해서는 의구심이 있었습니다. API 게이트웨이는 기본적인 필수 API 보안 제어 기능을 제공하지만, 안타깝게도 API 관련 위협으로부터 기업을 적절히 보호하기에는 충분하지 않습니다.

예를 들어, 흔히 BOLA로 불리는 손상된 오브젝트 수준 권한은 게이트웨이에 정상적인 API 트래픽으로 보입니다. API 요청과 응답 사이의 맥락을 고려하지 않기 때문에 BOLA 공격은 탐지되지 않고 통과해 중요한 백엔드 서비스에 접속할 수 있습니다. 이 취약점은 기업을 BOLA 악용에 취약하게 만들 뿐만 아니라 다른 공격과 비즈니스 로직 남용에 대한 문을 열어줄 수 있습니다.

또 다른 가시성 제한은 정확한 API 인벤토리를 유지하는 것과 관련이 있습니다. 대부분의 대기업과 마찬가지로 해당 은행도 자체 환경에서 알려지지 않은 API로 인해 어려움을 겪고 있었습니다. 일반적으로 대부분의 기업은 수천 개의 API를 관리하며, 이 중 상당수는 API 게이트웨이와 같은 프록시를 통해 라우팅되지 않습니다. 이를 악성 API 또는 좀비 API라고 합니다. 이러한 API는 전 직원이 배포했거나 기업이 API 보안에 대해 진지하게 생각하기 전에 배포되었을 가능성이 높습니다. 그러한 API의 존재 이유와 상관없이 은행의 API 게이트웨이는 이를 확인할 수 없고 은행은 보유한 API의 수를 쉽게 과소평가하게 됩니다.

API 보안 관련 도전 과제 해결

해당 기업은 전체 환경에 걸쳐 API 체계 관리, 런타임 보호, 테스트를 위한 솔루션을 포함한 완전한 Noname API Security Platform(현재 Akamai API Security의 일부)을 배포했습니다. 세계에서 가장 잘 알려지지 않은 위협 기법에 대한 취약점을 탐지하고 해결할 수 있게 되면서 고객의 보안 체계가 기하급수적으로 개선되었습니다.

이제 플랫폼 내에서 알려지지 않은 API를 발견하고 공개해 완벽한 가시성과 리스크 방어를 실현할 수 있습니다. 해당 기관은 Akamai API Security가 민감한 데이터를 분류해 GDPR, HIPAA 등과 같은 규정을 준수할 수 있도록 지원함으로써 API 확산을 획기적으로 줄이고 컴플라이언스를 개선했습니다.

또한 해당 은행은 이제 실시간으로 공격을 차단하고 고객 데이터 자산을 보호할 수 있는 역량을 갖추게 되었습니다. 런타임 보호 솔루션은 지능적으로 잠재적 위협을 탐지하고 우선순위를 지정하는 동시에 API 활동을 지속적으로 모니터링합니다. Akamai 플랫폼은 웹 애플리케이션 방화벽, API 게이트웨이, 보안 정보 및 이벤트 관리, 정보 기술 서비스 관리, 기타 워크플로우 툴과 통합해 위협을 수동, 부분 자동 또는 자동으로 해결할 수 있습니다.

결과

API는 해커들이 선호하는 공격 기법으로 빠르게 자리 잡았으며 공격은 줄어들 기미가 보이지 않습니다. 일례로 2022년에 '금융 서비스에 대한 공격 건수는 전년 대비 257% 증가'했습니다. 해당 금융 서비스 기업은 Akamai API Security를 통해 이러한 트렌드를 피하고 대응할 수 있는 역량을 갖추게 될 것입니다. 특히, 고객의 보안팀은 API의 위험성을 더 잘 이해하고 더욱 안전한 시스템을 구축할 수 있게 될 것입니다.

 | 2024년 8월 발행