2024년 API 보안 영향 연구

금융 서비스 업계

API 인시던트가 증가하고 있습니다. 금융 서비스 업계가 이 중요한 보안 문제를 어떻게 해결하고 있으며, 기업에서 보안을 유지하기 위해 무엇을 할 수 있는지 알아보세요.

지난해 88.7%의 금융 서비스 기업이 자사 데이터를 처리하고 고객과 파트너를 중요한 서비스에 연결하는 API에 대한 공격을 경험했습니다. 공격자들은 더 혁신적인 방법을 사용해 보호되지 않는 API의 데이터에 접속하고 계정 잔액 및 거래 내역 등 개인 및 금융 정보를 유출할 수 있습니다.

보안팀은 그 영향을 체감하고 개선 방법을 모색하고 있습니다. 하지만 잘못된 설정이나 비즈니스 로직 취약점이 쉽게 발견되고 악용될 수 있는 API와 같은 또 다른 공격 기법에 대응하는 것은 부담스러울 수 있습니다.

이것을 어떻게 알고 있을까요? Akamai는 CISO부터 애플리케이션 보안 담당자까지 1200명 이상의 IT 및 보안 전문가를 대상으로 API 관련 위협에 대한 경험을 알아보기 위해 설문 조사를 실시했습니다.

여기서 API 보안 인시던트의 가장 큰 영향이 '규제 기관의 벌금' 및 '팀 및 부서에 대한 스트레스 및/또는 압박 증가'라고 말한 금융 서비스 업계 응답자들의 조사 결과는 제외했습니다. 업계 동료들이 API 인시던트 해결 비용을 83만 2800달러로 책정했는데 이는, 설문에 응한 8개 업계의 평균 대비 40% 높고 다른 어떤 업계보다 높은 수준임을 감안할 때 이러한 결과는 당연해 보입니다.

업계 인사이트를 얻으려면 2024년 API 보안 영향 연구를 계속 읽어보세요.

공격이 증가하면서 가시성 감소

업계 전반에 걸쳐 84%의 기업이 API 보안 인시던트를 경험했지만 금융 서비스 기업은 더 빈번하게 표적이 되었습니다(평균 88.7%). 업계 동료들은 이런 공격을 일으키는 2가지 핵심 취약점으로 위협을 포착하지 못하는 네트워크 방화벽(26.5%) 및 대규모 언어 모델(LLM)과 같은 생성형 AI 툴의 API 내 취약점(23.2%)을 언급했습니다.

빈번한 인시던트 발생부터 높은 해결 비용과 규제 기관의 벌금에 이르기까지 API 위협에 대한 증거가 증가하고 있음에도 불구하고 Akamai의 조사 결과에 따르면 많은 금융 서비스 팀이 아직은 API 보안을 최우선으로 고려하지 않고 있습니다. 실제로 API 보안은 올해 사이버 보안 우선순위에서 9위(18.5%)에 머물렀습니다.

특히 API의 많은 리스크에 대한 가시성과 관련해 금융 부문에서는 정상 API와 악의적 또는 사기성 API 활동을 구분하는 것이 여전히 어려운 과제입니다. API의 전체 인벤토리를 보유하고 있다고 응답한 업계 동료는 73.5%이지만, 개인 식별 정보(PII) 및 카드 보유자의 신용 기록에서 대형 상업 은행 고객의 재무 기록에 이르기까지 민감한 데이터를 반환하는 API를 알고 있는 이 하위 집단의 비율은 28.5%에 불과합니다.

88.7% = 지난 12개월 동안 API 보안 인시던트를 경험한 금융 서비스 기업의 비율

28.5% = 전체 API 인벤토리를 보유한 금융 서비스 기업 중 어떤 API가 민감한 데이터를 반환하는지 알고 있는 비율

83만 2800달러 = 지난 12개월 동안 API 보안 인시던트를 경험한 금융 서비스 기업의 재정적 영향

상위 3가지 영향

1. 보안팀의 스트레스 및/또는 압박 증가
2. 규제 기관의 벌금
3. 평판과 신뢰 하락

출처:
Akamai, 'API 보안 영향 연구', 2024

Akamai

금융 서비스 사업자의 부서 또는 자회사에서 회사의 중앙 IT팀 또는 보안팀의 협업이나 감독 없이 배포한 섀도 API에 어떤 일이 발생할 수 있는지 생각해 보세요. 다음과 같은 API가 해당할 수 있습니다.

- 적절한 권한 확인 제어 없이 고객의 거래 데이터를 반환하도록 구축되었으며 잘못된 설정에 대한 적절한 테스트를 하지 않음
- 새 버전으로 교체되었지만 비활성화되지 않아 인터넷에 계속 노출되어 있음
- 관리되지 않는 API를 탐지할 수 없는 기존 툴의 레이더망을 빠져나감
- 실제 고객 계정에 접속해 자산을 훔치는 사이버 범죄자에 의해 악용됨

이는 그저 가상의 이야기가 아닙니다. LexisNexis® Risk Solutions의 2023년 True Cost of Fraud™ 연구에 따르면, 사기 손실의 50%는 사기범들이 API를 악용해 대규모로 계좌를 개설하는 신규 계좌 개설 악용에서 비롯된 것으로 밝혀졌습니다. 또한 이 시나리오는 실제 IT 및 보안 업계에서 API 인시던트의 주요 원인으로 꼽는 내용을 반영하고 있습니다.

API 인시던트가 컴플라이언스, 비즈니스 비용, 팀 스트레스에 미치는 영향

2024년 5월 Gartner®의 API 보안 시장 가이드*에는 '현재 데이터에 따르면, 평균적인 API 유출 사고에서 유출되는 데이터는 평균적인 보안 유출에서보다 10배 이상 더 많은 것으로 나타났다.'라고 언급되어 있습니다. 많은 기업들이 준수하고 있는 PCI DSS v4.0 규정에 API 보안 관련 요구사항이 추가된 것은 당연한 일입니다. 이제 이 표준에 따라 특히 API가 매일 수백만 건의 금융 거래를 지원하는 업계를 비롯해 기업은 출시 전에 API 코드를 검증하고, 정기적으로 취약점을 테스트하며, API 기반 구성요소가 안전하게 사용되는지 확인해야 합니다.

규제 당국의 신뢰를 잃으면, 컴플라이언스를 달성하기 위해 노력하는 팀의 업무 부담이 증가하고, 이에 대한 감시가 강화될 수 있습니다. 또한 고액의 벌금형으로 이어질 수도 있습니다.

이를 고려하면 금융 서비스 회사들이 API 위협으로 인한 결과에 대해 잘 알고 있다는 것을 알 수 있습니다. 처음으로 설문조사에 참여한 3개국의 응답자들에게 지난 12개월 동안 경험한 API 보안 인시던트로 인한 예상 재정적 영향을 공유해 달라고 요청했습니다.

	금융 서비스 업계	모든 업계 평균
미국	$832,800	$ 591,404
영국	£297,189	£ 420,103
독일	€604,405	€ 403,453

Q3. API 보안 인시던트를 경험한 경우, 해당 인시던트로 인해 발생한 총 재정적 영향은 얼마였나요? 시스템 수리, 다운타임, 법률 비용, 벌금, 기타 관련 비용 등 모든 관련 비용을 포함해 주세요.

선제적인 API 보안을 통해 리스크와 스트레스 줄이기

금융 서비스 기업을 대상으로 한 API 공격은 범위, 규모, 정교함, 비용 면에서 증가하고 있습니다. 여기에는 기존 API 보안 툴 및 기타 경계 방어 체계를 우회하기 위해 빠르게 적응하는 GenAI 기반 봇 공격이 포함됩니다. 업계의 많은 보안팀이 이러한 위협을 직접 경험하고 있으며 금전적, 인적 피해를 입고 있습니다. 하지만 기업이 API 위협의 심각성을 이해하더라도 여전히 '무엇을 할 수 있을까?'라는 의문이 남습니다.

기업들은 API와 API가 교환하는 데이터의 보안을 강화하는 조치를 취해 매출을 보호하고 보안팀의 부담을 덜어줄 수 있습니다. 또한 이와 함께 최신 API 위협에 대한 팀의 지식과 이를 방어하는 데 필요한 기능을 구축함으로써 이사회와 고객 모두의 어렵게 얻은 신뢰를 유지할 수 있습니다.

보고서 전문을 읽고 API 가시성 및 보안을 위한 모범 사례에 대해 알아보려면 **2024년 API 보안 영향 연구**를 다운로드하세요.

현재 직면한 도전 과제 해결을 Akamai가 어떻게 지원할 수 있는지 궁금하신가요?

맞춤 Akamai API Security 데모 요청하기

Akamai는 여기에서 논의한 위협과 관련된 리스크를 줄일 수 있도록 설계된 솔루션을 제공합니다.

- Akamai API Security: API를 검색하고, 리스크 체계를 평가하며, 행동을 분석하고, 위협이 내부에 침투하는 것을 방지
- Akamai Account Protector: 실시간으로 사용자 행동을 모니터링하고 변화하는 리스크 프로필에 적응해 계정 개설 도용 차단

Akamai

Akamai Security는 성능이나 고객 경험에 영향을 주지 않으면서 모든 상호 작용 지점에서 비즈니스의 원동력이 되는 애플리케이션을 보호합니다. 글로벌 플랫폼의 규모와 위협에 대한 가시성을 활용해 고객과 협력함으로써 위협을 예방, 탐지, 방어하고 브랜드 신뢰를 쌓고 비전을 실현할 수 있도록 지원합니다. Akamai의 클라우드 컴퓨팅, 보안, 콘텐츠 전송 솔루션에 관해 자세히 알아보려면 akamai.com 및 akamai.com/blog를 확인하거나 X 및 LinkedIn에서 Akamai Technologies를 팔로우하시기 바랍니다. 03월 25일 발행.