2024년 API 보안 영향 연구

보험 업계

API 인시던트가 증가하고 있습니다. 보험 서비스 업계가 이 중요한 보안 문제를 어떻게 해결하고 있으며, 기업에서 보안을 유지하기 위해 어떤 조치를 취할 수 있는지 알아보세요.

차량 사고부터 비즈니스 장비 손상까지 재난이 발생하면 보험 가입자는 보험사로부터 보상 청구를 제출하고 지원을 받기 위해 디지털 서비스에 의존합니다. 이러한 서비스 뒤에서는 보험사의 API가 보험 가입자의 삶을 데이터 형태로 담은 민감한 정보를 처리하고 있습니다.

고객 신뢰가 매우 중요한 보험사들은 점점 심각해지는 API 취약점에 직면하고 있습니다.

Akamai의 종합 조사에 따르면, 지난 12개월 동안 보험 업계 전문가의 76.7%가 API 보안 인시던트를 경험했으며, 미국 내 보험사는 이 문제를 해결하는 데 평균 625,634달러를 지출했습니다. 이는 상당한 재정적 부담입니다.

그러나 그보다 더 우려되는 것은 비즈니스에 미치는 영향입니다. API 인시던트 이후 보험사가 가장 크게 우려하는 문제는 "고객 신뢰 하락과 고객 이탈"(28%)인 것으로 나타났습니다. 고객이 손쉽게 보험사를 바꿀 수 있는 치열한 경쟁 시장에서, 이와 같은 평판 손상은 단기적인 비용을 넘어 장기적인 영향을 초래할 수 있습니다.

2024년 API 보안 영향 연구에서 업계 인사이트를 확인해보세요

공격이 증가하는 가운데 가시성 확보가 핵심 과제

보험사가 API 공격으로 인해 지불해야 하는 재정적 비용은 상당히 높습니다. 미국에서 보험 업계의 평균 대응 비용(62만 5634달러)이 전체 산업 평균(59만 1404달러)을 웃돕니다. 그렇다면 이러한 인시던트는 왜 발생할까요?

보험 업계 보안팀은 주요 원인으로 다음을 지목했습니다.

1. 휴면 또는 좀비 등 관리되지 않은 API(22%)
2. 의도하지 않게 인터넷에 노출된 API(21.3%)
3. 기존의 API 보안 툴이 위협을 탐지하지 못함(20%)
4. 권한 부여 취약점(19.3%)
5. API 설정 오류(18.7%)

많은 기업이 API 공격의 원인은 파악하고 있지만, 리스크의 핵심 지표 중 하나인 API가 호출될 때 민감한 데이터를 반환하는지 여부에 대한 가시성은 부족한 상황입니다. 보험사의 56.7%는 자사 API의 전체 목록을 보유하고 있다고 답했지만(전체 업계 평균인 69.7%보다 낮음), 민감한 데이터를 반환하는 API가 무엇인지 파악하고 있는 기업은 단 20.7%에 불과했습니다.

개인 정보 및 금융 정보처럼 고도로 규제되는 데이터를 처리하는 업계 특성상, 이러한 가시성 부족은 컴플라이언스와 보안 모두에 심각한 영향을 미칠 수 있습니다.

보험사의 76.7%가 지난 12개월 동안 API 인시던트를 경험

API 목록을 모두 갖고 있는 **보험사 중에서도 20.7%만이** 민감한 데이터를 반환하는 API를 알고 있음

62만 5634달러 = 지난 12개월 동안 **API 보안 인시던트로 인해 미국 보험사에 발생한 재정적 영향**

상위 3대 영향

1. 고객의 신뢰 하락과 고객 이탈(28%)
2. 리더십에서 보는 팀의 평판 손상(25.3%)
3. 문제 해결에 소요된 비용(24.7%)

출처:
Akamai, API 보안 영향 연구, 2024년

Akamai

API 보호를 어렵게 만드는 몇 가지 트렌드도 함께 확인됐습니다.

- **지속적인 API 확산**: 디지털 이니셔티브가 추진될 때마다 API는 계속해서 증가하고 진화하며, 그에 따라 정확한 목록을 유지하는 것이 점점 더 어려워지고 있습니다.
- **일관되지 않은 표준**: 많은 보험사들은 여러 사업부에 걸쳐 다수의 개발팀을 운영하고 있고, 중앙 집중화된 보안 설계 가이드라인 없이 운영되고 있습니다.
- **보이지 않는 리스크**: API는 민감한 보험 계약자 데이터를 전송하지만, 대부분의 기업은 어떤 API가 실제로 민감한 정보를 반환하는지 파악하지 못하고 있습니다.

예를 들어, 보안팀의 적절한 감독 없이 특정 부서에서 API를 배포한 경우를 생각해 보세요. 해당 API는 적절한 통제 없이 데이터를 공유하도록 설계되었거나, 시스템 업그레이드 이후에도 비활성화되지 않고 남아 있어 민감한 고객 데이터의 노출 가능성을 초래할 수 있습니다.

API 인시던트가 컴플라이언스, 고객 신뢰, 조직 내부의 스트레스에 미치는 영향

보험사들이 API 위협의 재정적 파급력에 민감하게 반응하는 것은 당연합니다. 이번 Akamai 조사에서 응답자들은 지난 12개월 동안 겪은 API 보안 인시던트의 추정 비용을 공유했습니다.

	보험 업계	모든 업계 평균
미국	$ 625,633.70	$ 591,404.01
영국	£ 493,000.50	£ 420,103.18
독일	€ 373,918.72	€ 403,453.26

재정적 영향도 상당하지만, 설문에 참여한 업계 관계자들은 이 비용이 단순한 매출 손실을 넘어 평판 하락의 문제까지 포함된 결과임을 명확히 밝혔습니다. API 보안 인시던트의 가장 큰 영향으로 꼽힌 항목은 다음과 같습니다.

- 28%: 고객의 신뢰 하락과 고객 이탈
- 25.3%: 리더십과 이사회 내 팀의 평판 손상
- 24.7%: 문제 해결에 소요된 비용

선제적인 API 보안을 통해 리스크와 스트레스 줄이기

보험사를 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.

기업은 지금 API와 API가 교환하는 데이터의 보안을 강화하기 위한 조치를 취해 매출을 보호하고 보안팀의 부담을 덜어주는 동시에 이사회와 고객 모두의 어렵게 얻은 신뢰를 유지할 수 있습니다. 기업이 취할 수 있는 조치에는 지능형 API 위협에 대한 내부 팀의 지식과 이를 방어하는 데 필요한 기능을 구축하는 것이 포함됩니다.

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 탐지하고, 리스크 체계를 이해하고, 행동을 모니터링해 내부에 숨어 있는 위협을 차단합니다.
- **Akamai Account Protector**: 실시간으로 사용자 행동을 모니터링하고 변화하는 리스크 프로필에 적응해 계정 개설 도용을 차단합니다.

Akamai

Akamai Security는 성능이나 고객 경험에 영향을 주지 않으면서 상호 작용이 일어나는 모든 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. 2025년 5월 발행.