2024년 API 보안 영향 연구

리테일 및 이커머스 업계

API 위협 증가를 바라보는 업계 동료들의 관점과 경험

리테일 및 이커머스 기업의 디지털 이니셔티브를 지원하는 API가 공격받고 있습니다. 공격자들은 점점 더 혁신적인 방법을 사용해 보호되지 않은 API의 데이터에 접속해 신용카드 데이터를 훔치고, 로열티 프로그램에서 자금을 빼내고, 크리덴셜 스터핑 공격을 실행할 수 있게 되었습니다. 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.

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

이 요약본은 업계 조사 결과를 정리한 것으로, 응답자의 68%가 지난 12개월 동안 API 보안 인시던트를 경험했다고 답했습니다. 그 영향은 무엇이었을까요? 업계 동료들은 팀원들의 스트레스 수준 증가와 고위 경영진 및 이사회 사이의 신뢰도 하락을 가장 많이 꼽았습니다. 리테일 및 이커머스 전문가들이 API 인시던트 해결에 52만 6531달러의 비용이 들었다고 응답한 것을 고려하면 이러한 답변은 이해할 수 있는 결과입니다.

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

공격은 증가하고 가시성은 감소

리테일 및 이커머스 응답자의 상당수가 API 보안 인시던트를 경험했지만, 이 업계의 평균인 68%는 설문 조사에 참여한 8개 업계 전체에서 보고된 84%보다 낮은 수치였습니다. 한편, 동종 업계 종사자들이 향후 12개월 동안 가장 우선시할 보안 우선순위는 'GenAI 기반 공격 방어'와 '공격자로부터 API 보호'인 것으로 나타났습니다.

API 우선순위 지정과 공격 방지 사이에 연관성이 있을까요? 리테일 및 이커머스 기업의 보안팀은 API 보안의 중요성을 인식하고 있으며, 이러한 노력으로 인시던트가 감소하고 있을 가능성이 있습니다. 하지만 이번 조사 결과에 따르면 이들 보안팀이 모든 API 악용 사례를 파악하고 있는 것은 아닙니다.

정상 API 활동과 악성 또는 사기성 API 활동을 구분하는 것은 리테일 및 이커머스 기업에 여전히 어려운 과제입니다. 리스크에 대한 가시성 확보 또한 어려운 과제입니다. 업계 동료의 67%가 전체 API 인벤토리를 보유하고 있다고 답했지만, 이 가운데 29%만이 수많은 API 중 어떤 API가 민감한 데이터를 반환하는지 파악하고 있습니다. 여기에는 개인 식별 정보(PII)나 신용카드 정보가 포함됩니다.

사업부에서 리테일 기업의 중앙 IT팀이나 보안팀의 협업이나 감독 없이 배포한 API에 어떤 일이 발생할 수 있는지 생각해 보세요. 다음과 같은 API가 해당할 수 있습니다.

- 적절한 권한 확인 제어 없이 고객의 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 고객의 로열티 계정에 접속해 현금을 사용하는 사기꾼에게 악용됨

68% = 지난 12개월 동안 API 보안 인시던트를 경험한 리테일 및 이커머스 기업의 비율[1]

29% = 전체 API 인벤토리를 보유한 리테일 및 이커머스 기업 중 어떤 API가 민감한 데이터를 반환하는지 알고 있는 비율[1]

52만 6531달러 = 지난 12개월 동안 API 보안 인시던트를 경험한 리테일 및 이커머스 기업의 재정적 영향[1]

상위 3가지 영향[1]

1. 팀의 압박감 또는 **스트레스 증가**
2. 문제 해결을 위한 **비용 발생**
3. 고위 경영진 또는 이사회에서 **부서의 평판 손상**

44% = 커머스 기업을 겨냥한 웹 공격 중 API를 표적으로 삼은 비율[2]

출처:
1. Akamai, 'API 보안 영향 연구', 2024
2. Akamai 인터넷 보안 현황 보고서(SOTI) - '숨어 있는 API 위협에 대한 공격 트렌드 분석', 2024년

Akamai

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.

리테일 및 이커머스 보안팀이 꼽은 API 인시던트의 주요 원인

1. 생성형 AI 툴(예: LLM)의 API - 24.7%
2. API가 인터넷에 의도치 않게 노출됨 - 24.0%
3. API 설정 오류 - 22.0%
4. 웹 애플리케이션의 탐지 실패 - 21.3%
5. API 게이트웨이의 탐지 실패 - 20.7%
6. API 코딩 오류로 인한 취약점 - 20.0%
7. 유명한 기술 툴 및 서비스 - 20.0%
8. 네트워크 방화벽의 탐지 실패 - 18.7%
9. 권한 확인 취약점 - 17.3%
10. 인터넷에서 다운로드한 소프트웨어 솔루션 - 16.7%
11. API 인증 제어 부족 - 16.0%
12. 미드 티어 소프트웨어 솔루션 - 14.7%
13. 관리되지 않는 API(예: 좀비) - 13.3%

Q. 기업에서 경험한 API 보안 인시던트의 원인은 무엇인가요? (최대 3개 선택), n=1,207

API 인시던트가 컴플라이언스, 비즈니스 비용, 팀 스트레스에 미치는 영향

2024년 5월 Gartner® API 보안 시장 가이드에는 '현재 데이터에 따르면, 평균적인 API 유출 사고에서 유출되는 데이터는 평균적인 보안 유출에서보다 10배 이상 더 많은 것으로 나타났다.'라고 언급되어 있습니다.[3] 많은 기업들이 준수하고 있는 PCI DSS v4.0 규정에 API 보안 관련 요구사항이 추가된 것은 당연한 일입니다. 기업과 규제 기관은 자체 API뿐만 아니라 파트너 및 공급업체의 API를 통해 어떤 종류의 데이터가 이동하는지 파악해야 하기 때문에 이커머스에서 써드파티 리스크를 관리하는 데 또 다른 어려움이 더해졌습니다.

규제 기관의 신뢰를 잃으면 조사가 강화되고 컴플라이언스 요구사항을 충족하기 위해 고군분투하는 팀에 더 많은 업무가 가중될 수 있습니다. 또한 고액의 벌금형으로 이어질 수도 있습니다. 이러한 비용을 고려할 때, 리테일 및 이커머스 기업들은 API 위협으로 인한 재정적 결과를 심각하게 인식하고 있는 것이 분명합니다. 처음으로 설문 조사에 참여한 3개국의 응답자들에게 지난 12개월 동안 경험한 API 보안 인시던트로 인한 예상 재정적 영향을 공유해 달라고 요청했습니다.

[3] GARTNER는 Gartner, Inc. 및/또는 미국 내외에 있는 Gartner 계열사의 등록 상표 및 서비스 마크이며, 이 문서에 대한 사용 허가를 받았습니다. All rights reserved.

	리테일 및 이커머스	전체 업계 평균
미국	$526,531	$591,404
영국	£258,815	£420,103
독일	€348,467	€403,453

Q. 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. n=1,207

재정적 영향도 상당하지만, 연구 참여자들은 그 비용이 수익에 미치는 영향은 훨씬 더 크다는 점을 강조했습니다. API 보안 인시던트의 가장 큰 영향을 나열해 달라는 질문에 응답자들은 비용이 아니라고 답했습니다. 리테일 및 이커머스 응답자들은 인적 피해, 즉 팀에 대한 스트레스와 압박을 강조했습니다.

리테일 및 이커머스 기업에 대한 API 보안 인시던트의 상위 5가지 영향

1. 팀 또는 부서 스트레스나 압박 증가 - **28.7%**
2. 문제 해결을 위한 비용 발생 - **28.0%**
3. 고위 경영진 또는 이사회에서 부서의 평판 손상 - **25.3%**
4. 팀 또는 부서에 대한 기업의 내부 조사 증가 - **23.3%**
5. 규제 기관의 벌금 - **25.3%**

Q. API 보안 인시던트가 기업에 어떤 비용 및/또는 영향을 초래했나요? (최대 3개 선택), n=1,207

다음 단계: 선제적인 API 보안을 통해 리스크와 스트레스 줄이기

리테일 및 이커머스 기업을 대상으로 한 API 공격은 그 범위와 규모, 정교함이 점점 더 커지고 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 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.

귀사의 도전 과제를 Akamai가 어떻게 도울 수 있는지에 대해 대화할 준비가 되셨나요?

맞춤 Akamai API 보안 데모 요청하기

Akamai

Akamai 보안은 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 관한 자세한 정보를 보려면 akamai.com과 akamai.com/blog를 방문하거나 X(기존의 Twitter)와 LinkedIn에서 Akamai Technologies를 팔로우하시기 바랍니다. 2024년 11월 발행.