2024년 API 보안 영향 연구

정부

API 인시던트가 증가하고 있습니다. 정부가 이 중요한 보안 문제를 어떻게 해결하고 있는지, 그리고 기업이 보안을 유지하기 위해 무엇을 할 수 있는지 알아보세요.

전 세계 정부 기관은 API 우선 시대에 디지털 서비스 보안을 강화해야 한다는 압박을 점점 더 크게 받고 있습니다. 2024년에 공공 부문 기관의 86.1%가 API 보안 인시던트를 보고했는데 이는 전년도의 76.8%에서 급증한 수치입니다. 이로 인해 공공 부문은 전체 업계 평균인 84%보다 수치가 더 높아지면서 문제의 심각성을 강조하고 있습니다. GDPR(General Data Protection Regulation) 준수부터 멀티클라우드 시스템에서의 데이터 저장 요건 준수, 주권적 보안 위협 대응까지 기관들은 더 큰 가시성, 강력한 거버넌스, 내재적 안정성을 확보해야 하는 보편적인 과제에 직면해 있습니다.

정부 API 보안 인시던트의 실제 비용

정부 기관들은 디지털 서비스 제공, 기관 간 데이터 공유 촉진, 인프라 현대화를 위해 점점 더 많은 API를 도입하고 있습니다. 그러나 이 과정에서 공격자들이 악용하려 하는 새로운 취약점도 다수 등장했습니다. 취약한 인증 메커니즘, API 설정 오류, 주요 리스크 지표에 대한 인식 부족 등이 정부 기관을 API 보안 침해에 특히 취약하게 만들고 있습니다. 이러한 인시던트의 영향은 단순한 데이터 유출을 넘어 운영 연속성, 규제 컴플라이언스, 공공 신뢰에까지 리스크를 초래합니다.

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

이 중 정부 부문 응답자의 답변을 따로 분석한 결과, API 보안 인시던트의 주요 영향으로 다음을 꼽았습니다.

- "팀 및 부서 스트레스나 압박 증가"(28.5%)
- "부서에 대한 고위 경영진 또는 이사회의 평판 손상"(27.2%)
- "규제 기관의 벌금"(25.2%)

업계 동료들이 API 인시던트 해결 비용을 71만 7500달러로 추산했는데, 이 수치가 설문에 응한 8개 업계 평균 대비 21.3% 높은 것임을 감안하면 이러한 결과는 충분히 이해할 수 있습니다.

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

공격이 증가함에 따라 가시성은 점점 더 중요한 문제로 부상하고 있습니다

API 보안 인시던트의 주요 원인을 묻는 질문에 동료들은 두 가지 핵심 취약점을 지적했습니다.

- API 인증 제어 부족(25.2%)
- API 보안을 위해 사용되는 기존 툴(25.2%)

Akamai의 조사 결과에 따르면, 높은 복구 비용부터 신뢰도 하락까지 API 위협의 영향에 대한 증거가 쌓이고 있음에도 많은 정부 기관 팀이 여전히 API 보안을 최우선 과제로 삼고 있지 않습니다. 실제로 내년 사이버 보안 우선순위에서 API 보안은 17.9%로 6위를 차지했습니다.

2024년 **정부 기관의 86.1%가** API 보안 인시던트를 경험했다고 보고했으며 이는 2023년의 76.8%에서 크게 증가한 수치입니다.

미국 정부 기관의 API 보안 침해 **평균 재정적 비용은 71만 7500달러**로 전체 업계 평균인 59만 1404달러를 웃돌았습니다.

정부 기관의 66.9%가 API 인벤토리를 관리하고 있으나, 민감한 데이터를 처리하는 API를 완전히 파악한 곳은 18.5%에 불과해 중요한 정보가 리스크에 노출되어 있습니다.

상위 3대 영향

1. 보안팀의 스트레스와 압박 증가
2. 팀에 대한 리더와 이사회의 신뢰 하락
3. 규정 준수 위반에 따른 규제 벌금

출처:
2024년 API 보안 영향 연구

API 공격은 재정적, 인적 측면 모두에서 정부 기관에 막대한 비용을 초래합니다. 유출로 인해 리더십의 신뢰를 잃게 되면 추가적인 감시 강화, 운영 차질, 그리고 이미 과중한 업무와 컴플라이언스 요구사항을 감당하고 있는 팀에 더 큰 부담이 가중될 수 있습니다.

Akamai

민간 부문과 마찬가지로 정부 기관 역시 정상적인 API 활동과 악성 활동을 구분하는 데 어려움을 겪고 있습니다. 이는 부분적으로 API의 취약 지점을 정확히 파악할 수 있는 가시성이 부족하기 때문입니다. 응답자의 66.9%는 API의 전체 인벤토리를 보유하고 있다고 응답했지만, 그 중 18.5%만이 주민등록번호, 생체 인식 데이터, 연락처 정보 같은 개인 식별 정보(PII)를 포함한 민감한 데이터를 반환하는 API를 파악하고 있었습니다.

정부 기관의 부서나 산하기관이 중앙 IT 또는 보안팀의 협업이나 최신 감독 없이 무단으로 API를 배포할 경우 어떤 문제가 발생할 수 있을지 생각해 보세요.

해당 API는 다음과 같은 위험을 초래할 수 있습니다.

- 적절한 권한 제어 없이 시민의 개인 또는 금융 데이터에 접속을 허용하도록 설계되어 민감한 정보를 노출시킬 수 있습니다.
- 새 버전으로 교체된 후에도 제대로 폐기되지 않아 구형 엔드포인트가 악용될 수 있습니다.
- 중앙 IT 및 보안팀의 감시 범위를 벗어나 기존 모니터링 툴과 컴플라이언스 점검을 회피합니다.
- 악성 공격자가 정부 시스템에 무단 접속해 데이터 유출, 신원 도용, 금융 사기 등을 일으킬 수 있습니다.

이는 단순한 가설이 아닙니다. 미국 정부 기관의 사이버 보안 환경은 실제로 심각한 도전 과제에 직면해 있습니다. Cybernews Business Digital Index에 따르면, 많은 정부 기관과 부서가 강력한 보안 체계를 유지하는 데 어려움을 겪고 있으며, 전체 기관 중 거의 10곳 중 4곳(38.8%)이 평가에서 "중대 리스크" 등급을 받았고, 75%가 데이터 유출을 경험했습니다.

이러한 통계는 정부 보안팀이 직면한 복잡한 현실을 반영합니다. 이들은 미션 목표, 레거시 시스템, 진화하는 위협 사이에서 균형을 잡아야 하며, 독특한 제약 조건과 감시 하에 운영되고 있습니다. 이러한 도전 과제가 심화되면서 특히 API 보안 분야에서 정부 기관의 고유한 요구사항을 이해하고 이에 맞춘 솔루션을 제공할 수 있는 파트너가 필요해졌습니다.

API 인시던트가 신뢰도, 비용, 팀 스트레스에 미치는 영향

API 공격의 빈도와 비용을 고려하면 전 세계 정부 기관이 API 보안에 대한 우선순위를 높이는 것은 당연한 흐름입니다. 미국에서는 일반 서비스 관리청이 운영하는 Data.gov 이니셔티브를 통해 연방 기관 간 API를 표준화해 일관성, 보안, 상호 운용성을 강화하고 있습니다. 전 세계적으로 유사한 노력들이 진행 중입니다. 유럽 연합과 영국에서의 오픈 데이터 프레임워크부터 아시아 태평양 및 중동 지역에서의 디지털 전환 이니셔티브까지 정부는 안전한 데이터 교환을 보장하기 위해 표준화된 API를 도입하고 있습니다.

이러한 이니셔티브의 많은 부분은 EU의 GDPR, 호주의 데이터 유출 통지 제도, 일본의 마이넘버 법 같은 지역별 규제와도 발맞추고 있습니다. 정부는 공통 표준과 프레임워크를 적용해 써드파티 통합 및 무단 접속으로 인한 리스크를 줄이는 동시에 안전한 데이터 교환을 보장하기 위해 노력하고 있습니다.

	정부	모든 업계 평균
미국	$717,500.50	$591,404.01
영국	£378,140.69	£420,103.18
독일	€296,975.79	€403,453.26

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.

정부 기관들이 API 위협의 심각성을 인식하고 있다는 것은 분명합니다. 처음으로 설문 조사에 참여한 3개국의 응답자들에게 지난 12개월 동안 경험한 API 보안 인시던트로 인해 예상되는 재정적 영향을 공유해 달라고 요청했습니다.

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. 앞서 언급한 바와 같이 응답자들은 "팀 및 부서 스트레스나 압박 증가"와 "부서에 대한 고위 경영진 또는 이사회의 평판 손상"을 가장 큰 문제로 꼽았습니다.

이러한 영향은 장기적으로 영향을 미칩니다. 데이터 유출은 공공의 신뢰를 약화시키고, 향후 자금 조달을 어렵게 만들 수 있습니다. 또한 이미 과중한 업무를 수행 중인 기관에서는 생산성 저하로 인해 번아웃과 직원 이탈이 심화될 수 있습니다.

이러한 압박은 특정 지역에만 국한되지 않습니다. 본 보고서는 일부 시장을 대상으로 하지만, API 보안은 전 세계 공공 부문 기관에 걸쳐 공통된 문제로 대두되고 있습니다. 아시아 태평양, 라틴 아메리카의 기관들 역시 디지털 인프라 보호, 컴플라이언스 기준 충족, 진화하는 위협으로부터 민감한 데이터 보호라는 유사한 과제에 직면하고 있습니다.

선제적인 API 보안을 통해 리스크와 스트레스 줄이기

정부를 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 매출과 민감한 데이터를 보호하고 보안팀의 부담을 덜어주는 동시에 이사회와 정부 리더로부터 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.

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

맞춤 Akamai API Security 데모 요청하기

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. 05월 25일 발행.