API-SICHERHEITSSTUDIE 2024

Behörden

API-Angriffe nehmen zu. Erfahren Sie, wie Regierungsbehörden dieses wichtige Sicherheitsproblem angehen – und was Ihre Organisation tun kann, um sich zu schützen.

Behörden auf der ganzen Welt stehen immer mehr unter dem Druck, digitale Dienste zu sichern – und das in einer Zeit, in der APIs Vorrang haben. Im Jahr 2024 meldeten 86 % der Organisationen des öffentlichen Sektors einen API-Sicherheitsvorfall – ein deutlicher Anstieg von 76,8 % im Vorjahr. Durch diesen Anstieg liegt der öffentliche Sektor über dem Branchendurchschnitt von 84 %, was das wachsende Ausmaß der Herausforderung unterstreicht. Von der Erfüllung der Anforderungen der Datenschutzgrundverordnung (DSGVO) bis hin zur Durchsetzung der Datenspeicherung in mehreren Systemen und der Bewältigung von staatlichen Sicherheitsbedrohungen – Behörden sehen sich dem universellen Bedarf nach mehr Transparenz, stärkerer Governance und integrierter Ausfallsicherheit gegenüber.

Die wahren Kosten von API-Sicherheitsvorfällen für Behörden

Regierungsbehörden setzen zunehmend APIs ein, um digitale Dienste zu ermöglichen, die gemeinsame Nutzung von Daten zwischen Behörden zu erleichtern und die Infrastruktur zu modernisieren. Dieser Trend hat jedoch auch eine Vielzahl neuer Schwachstellen eingeführt, die von Cyberkriminellen ausgenutzt werden können. Schlechte Authentifizierungsmechanismen, API-Fehlkonfigurationen und unzureichende Kenntnis kritischer Risikoindikatoren haben Regierungsbehörden besonders anfällig für API-Sicherheitsverletzungen gemacht. Die Folgen dieser Vorfälle gehen weit über den Datendiebstahl hinaus, da sie Risiken für die Betriebskontinuität, die Einhaltung gesetzlicher Vorschriften und das öffentliche Vertrauen darstellen.

Woher wissen wir das? Akamai hat mehr als 1.200 IT- und Sicherheitsexperten – von Chief Information Security Officers bis hin zu Experten für Anwendungssicherheit – befragt, um mehr über deren Erfahrungen mit API-Bedrohungen zu lernen.

Hier haben wir unsere Ergebnisse nach Antwortenden in behördlicher Tätigkeit gefiltert, die Folgendes als Hauptauswirkungen ihrer API-Sicherheitsvorfälle nannten:

- „Erhöhter Stress und/oder Druck für das Team/die Abteilung“ (28,5 %)
- „Rufschädigung unserer Abteilung bei Führungskräften und/oder dem Vorstand“ (27,2 %)
- „Geldbußen von Regulierungsbehörden“ (25,2 %)

Diese miteinander zusammenhängenden Konsequenzen sind leicht nachzuvollziehen, da Ihre Kollegen für die Behebung von API-Vorfällen mit Kosten von 717.500 $ rechnen – 21,3 % höher als der Durchschnitt in allen acht untersuchten Branchen.

Lesen Sie weiter und informieren Sie sich über die genaue Lage in Ihrer Branche mit der API-Sicherheitsstudie 2024.

Immer mehr Angriffe bei schlechterer Transparenz

Auf die Frage nach den Hauptursachen für API-Sicherheitsvorfälle haben Ihre Kollegen zwei wichtige Schwachstellen identifiziert:

- Fehlende API-Authentifizierungskontrollen (25,2 %)
- Herkömmliche Tools zum Schutz von APIs (25,2 %)

Trotz zunehmender Belege für die Folgen von API-Bedrohungen – von hohen Kosten für die Behebung von Problemen bis hin zu Vertrauensverlust – deuten unsere Ergebnisse darauf hin, dass viele Teams innerhalb von Behörden die API-Sicherheit noch immer nicht zur obersten Priorität gemacht haben. Tatsächlich befindet sich die API-Sicherheit mit 17,9 % nur auf Platz sechs der Prioritäten im Bereich Cybersicherheit für das kommende Jahr.

86,1 % der Regierungsorganisationen gaben an, dass es 2024 zu einem API-Sicherheitsvorfall kam – ein deutlicher Anstieg gegenüber 76,8 % im Jahr 2023

717.500 $ sind die durchschnittlichen finanziellen Kosten eines API-Sicherheitsverstoßes für Regierungsorganisationen in den USA und sie übersteigen damit den Branchendurchschnitt von 591.404 $

66,9 % der Regierungsbehörden führen einen API-Bestand, aber nur 18,5 % haben einen vollständigen Überblick darüber, welche APIs sensible Daten verarbeiten, wodurch kritische Informationen gefährdet werden

Die drei wichtigsten Folgen

1. Erhöhter Stress und Druck auf Sicherheitsteams
2. Beschädigter Ruf des Teams bei Führungskräften und Vorstand
3. Strafen für Verstöße gegen die Vorschriften

Quelle:
API-Sicherheitsstudie 2024

Für Regierungsbehörden sind die Kosten von API-Angriffen hoch – einschließlich finanzieller und menschlicher Auswirkungen. Wenn Sie aufgrund von Verstößen das Vertrauen auf der Führungsebene verlieren, kann dies zu einer verstärkten Überprüfung, Betriebsunterbrechungen und mehr Arbeit für Teams führen, die bereits überlastet sind und Schwierigkeiten haben, Compliance-Anforderungen zu erfüllen.

Akamai

Genau wie im Privatsektor ist es für Regierungsbehörden schwierig, zwischen echten und böswilligen API-Aktivitäten zu unterscheiden. Dies ist zum Teil auf die geringe Transparenz in Bezug auf die Schwachstellen von APIs zurückzuführen. Während 66,9 % Ihrer Kollegen angeben, dass sie über eine vollständige Übersicht ihrer APIs verfügen, wissen nur 18,5 % dieser Teilmenge, welche APIs vertrauliche Daten zurückgeben – einschließlich personenbezogener Daten (PII) wie Personenkennzeichen, biometrische Daten und Kontaktinformationen.

Stellen Sie sich vor, was mit einer nicht autorisierten API geschehen kann, die von einer Abteilung oder Tochtergesellschaft einer Regierungsbehörde ohne Zusammenarbeit oder Überwachung mit den zentralen IT- oder Sicherheitsteams bereitgestellt wird.

Diese API könnte:

- entwickelt worden sein, um ohne angemessene Autorisierungskontrollen Zugriff auf persönliche oder finanzielle Daten der Bürger zu ermöglichen und vertrauliche Informationen potenziell preiszugeben
- durch eine neue Version ersetzt, aber nicht ordnungsgemäß außer Betrieb genommen worden sein, sodass ein veralteter und anfälliger Endpoint bleibt
- außerhalb der Sichtbarkeit der zentralen IT- und Sicherheitsteams agieren und herkömmliche Überwachungstools und Compliance-Prüfungen umgehen
- von Cyberkriminellen ausgenutzt werden, um unbefugten Zugriff auf Behördensysteme zu erhalten, was möglicherweise zu Datenschutzverletzungen, Identitätsdiebstahl oder Finanzbetrug führen kann

Dies ist nicht nur rein hypothetisch: Die Cybersicherheitslandschaft stellt US-Regierungsbehörden vor erhebliche Herausforderungen. Laut dem Cybernews Business Digital Index haben viele Regierungsbehörden und Abteilungen Schwierigkeiten, einen zuverlässigen Sicherheitsstatus aufrechtzuerhalten. Fast 4 von 10 (38,8 %) erhalten bei ihren Bewertungen „kritische Risiken“ und 75 % sind von einer Datenschutzverletzung betroffen.

Diese Statistiken spiegeln die komplexe Realität wider, mit der Sicherheitsteams von Behörden konfrontiert sind. Sie müssen Ziele, Altsysteme und sich entwickelnde Bedrohungen unter einzigartigen Einschränkungen und Kontrollen abwägen. Angesichts der zunehmenden Herausforderungen, insbesondere im Bereich der API-Sicherheit, benötigen Behörden Partner, die ihre spezifischen Anforderungen kennen und Lösungen anbieten können, die auf behördliche Umgebungen zugeschnitten sind.

Auswirkungen von API-Vorfällen auf Vertrauen, Kosten und Belastung innerhalb des Teams

Angesichts der Häufigkeit und der Kosten von API-Angriffen ist es nicht überraschend, dass die Sicherung von APIs für Behörden weltweit immer wichtiger wird. In den Vereinigten Staaten standardisiert die Initiative Data.gov, die von der General Services Administration verwaltet wird, APIs über Bundesbehörden hinweg, um so Konsistenz, Sicherheit und Interoperabilität zu verbessern. Ähnliche Anstrengungen sind weltweit im Gange – von offenen Datenframeworks in der Europäischen Union und im Vereinigten Königreich bis hin zu Initiativen zur digitalen Transformation im asiatisch-pazifischen Raum und im Nahen Osten, wo Regierungen standardisierte APIs einführen, um einen sicheren und nahtlosen Datenaustausch zu gewährleisten.

Viele dieser Initiativen entsprechen regionalen Vorschriften wie der DSGVO in Europa, dem „Notifiable Data Breaches“-Ansatz (System für meldepflichtige Datenschutzverletzungen) in Australien und dem My Number Act in Japan (Gesetz für den Schutz der individuellen Nummer zu sozialversicherungs- und steuerrechtlichen Zwecken). Durch die Durchsetzung gemeinsamer Standards und Frameworks arbeiten Regierungen daran, einen sicheren Datenaustausch zu gewährleisten und gleichzeitig die Risiken aufgrund von Drittanbieterintegrationen und unbefugtem Zugriff zu verringern.

	Behörden	Durchschnitt aller Branchen
USA	717.500,50 $	591.404,01 $
Vereinigtes Königreich	378.140,69 £	420.103,18 £
Deutschland	296.975,79 €	403.453,26 €

Q3. Wie hoch sind insgesamt die geschätzten finanziellen Auswirkungen von API-Sicherheitsvorfällen, die Sie erlebt haben? Bitte berücksichtigen Sie alle damit verbundenen Kosten wie Systemreparaturen, Ausfallzeiten, Anwaltskosten, Bußgelder und andere damit verbundene Kosten.

Es ist klar, dass Regierungsbehörden sich der Folgen von API-Bedrohungen bewusst sind. Erstmalig haben wir die Teilnehmer in den drei untersuchten Ländern gebeten, die geschätzten finanziellen Folgen der API-Sicherheitsvorfälle aus den letzten 12 Monaten mitzuteilen.

Auch wenn die finanziellen Auswirkungen beträchtlich sind, haben die Befragten deutlich gemacht, dass zu den negativen Folgen nicht nur anfallende Kosten gehören.

Die wichtigsten Auswirkungen von API-Sicherheitsvorfällen sind anderer Natur. Wie bereits erwähnt, nannten unsere Befragten „erhöhter Stress und/oder Druck für das Team/die Abteilung“ und „Rufschädigung unserer Abteilung bei Führungskräften und/oder dem Vorstand“ als die beiden wichtigsten Punkte.

Diese Folgen haben dauerhafte Auswirkungen. Verstöße untergraben das Vertrauen, was die künftige Finanzierung gefährden und das Vertrauen der Öffentlichkeit schwächen kann. Gleichzeitig können Produktivitätsverluste in bereits stark angespannten Behörden Burnout und eine geringere Mitarbeiterbindung bewirken.

Aber der Druck beschränkt sich nicht etwa auf einige wenige Regionen. Obwohl sich dieser Bericht auf ausgewählte Märkte konzentriert, ist die API-Sicherheit für Organisationen des öffentlichen Sektors weltweit zu einem kritischen Thema geworden, da Behörden im asiatisch-pazifischen Raum, Lateinamerika und darüber hinaus ähnliche Herausforderungen bei der Sicherung digitaler Infrastrukturen, der Einhaltung von Compliance-Standards und dem Schutz vertraulicher Daten vor sich entwickelnden Bedrohungen bewältigen müssen.

Risiken und Stress durch proaktive API-Sicherheit reduzieren

API-Angriffe auf Regierungen nehmen an Umfang, Ausmaß, Raffinesse und Kosten zu. Dies betrifft auch GenKI-gestützte Bot-Angriffe, die sich schnell anpassen, um herkömmliche API-Sicherheitstools und andere Netzwerkschutzmaßnahmen zu umgehen. Viele Sicherheitsteams in Ihrer Branche erleben diese Bedrohungen an vorderster Front und spüren die Folgen sowohl finanziell als auch bei ihren Mitarbeitern. Doch auch wenn Unternehmen die Bedeutung von API-Bedrohungen verstehen, bleibt die Frage offen: Was können wir dagegen tun?

Wenn Sie jetzt Maßnahmen ergreifen, um Ihre APIs – und die über diese ausgetauschten Daten – besser zu schützen, kann Ihr Unternehmen seine Einnahmen und vertrauliche Daten sichern und die Belastungen für Sicherheitsteams verringern. Gleichzeitig wird das hart erarbeitete Vertrauen von Vorständen und Regierungsvertretern gewahrt. Zu diesen Maßnahmen gehören der Aufbau von Wissen in Ihrem Team über moderne API-Bedrohungen und die Kompetenzen, die zum Schutz dagegen benötigt werden.

Um den vollständigen Bericht zu lesen und mehr über Best Practices für Schutz und Transparenz von APIs zu erfahren, laden Sie die **API-Sicherheitsstudie 2024** herunter.

Wünschen Sie ein Gespräch über Ihre spezifischen Herausforderungen sowie darüber, wie Akamai Sie unterstützen kann?

Individuelle Demo für Akamai API Security anfragen

Akamai schützt die Anwendungen, die Ihr Unternehmen vorantreiben, an jedem Interaktionspunkt – ohne die Performance oder das Kundenerlebnis zu beeinträchtigen. Unsere globale Plattform liefert Skalierbarkeit sowie transparente Einblicke in Bedrohungen. So können wir mit Ihnen gemeinsam Bedrohungen erkennen und abwehren, damit Sie Markenvertrauen aufbauen und Ihre Vision umsetzen können. Möchten Sie mehr über die Cloud-Computing-, Sicherheits- und Bereitstellungslösungen von Akamai erfahren? Dann besuchen Sie uns unter akamai.com und akamai.com/blog oder folgen Sie Akamai Technologies auf X und LinkedIn. Veröffentlicht: Mai 2025.