API-SICHERHEITSSTUDIE 2024

Gesundheitsbranche

API-Angriffe nehmen zu. Erfahren Sie, wie die Gesundheitsbranche Herausforderungen bei der API-Sicherheit bewältigt – und wie Sie sich gegen neue Bedrohungen schützen können.

In einer Branche, in der das Vertrauen von Patienten und Mitgliedern von größter Bedeutung ist, stehen Gesundheitsorganisationen vor einer wachsenden Herausforderung für die Sicherheit: API-Schwachstellen.

Elektronische Patientenakten, Telemedizin und vernetzte medizinische Geräte sind zu den wichtigsten Zielen für Cyberkriminelle geworden – und geschützte Gesundheitsdaten (Protected Health Information, PHI), auf die über ungesicherte APIs zugegriffen wird, können zu HIPAA-Verstößen, einer Beeinträchtigung des Datenschutzes der Patienten und einem Vertrauensverlust führen, dessen Wiederaufbau Jahre dauern kann.

Das Ausmaß dieser Herausforderung ist beträchtlich. In der groß angelegten Befragung von Akamai berichteten 84,7 % der medizinischen Fachkräfte von API-Sicherheitsvorfällen innerhalb des letzten Jahres. Das ist sogar etwas höher als der branchenübergreifende Durchschnitt von 84 %.

Am besorgniserregendsten sind jedoch die Auswirkungen auf das Vertrauen: Die Befragten aus der Gesundheitsbranche gaben an, dass sie „Verlust von Vertrauen und Rufschädigung“ (28,7 %) als eine ihrer größten Sorgen im Zusammenhang mit API-Vorfällen betrachten. In einer Welt, in der Patienten problemlos den Gesundheitsdienstleister wechseln können, kann eine solche Rufschädigung über die unmittelbaren Kosten hinaus anhaltende Auswirkungen haben.

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

Immer mehr Angriffe bei schlechterer Transparenz

API-Angriffe haben erhebliche finanzielle Auswirkungen, wobei Gesundheitsorganisationen im Durchschnitt 510.600 $ für die Bewältigung dieser Vorfälle aufwenden.

Trotz dieser Risiken zeigen die Daten eine beunruhigende Diskrepanz bei den Prioritäten. Auf die Frage nach ihren wichtigsten Prioritäten im Bereich Cybersicherheit in den nächsten 12 Monaten stuften Gesundheitsorganisationen die „Sicherung von APIs vor Bedrohungsakteuren“ auf Platz 11 (16,7 %) von 12 ein. Stattdessen konzentrieren sie sich darauf, eine sichere Authentifizierung für Mitarbeiter, die auf Systeme zugreifen (24,7 %), und die Verwaltung von Entwicklergeheimnissen (22,7 %) zu gewährleisten.

Die Unterscheidung zwischen legitimen und schädlichen API-Aktivitäten ist für Gesundheitsdienstleister weiterhin eine Herausforderung. 65 % Ihrer Kollegen geben an, über vollständige API-Bestände zu verfügen – aber nur 24 % davon wissen, welche APIs sensible Daten verarbeiten – ein besorgniserregender Rückgang gegenüber 40 % im Jahr 2023. Für die Gesundheitsbranche, in der Datenschutz nicht nur gute Praxis, sondern gesetzlich vorgeschrieben ist, stellt diese Sichtbarkeitslücke ein erhebliches Risiko dar.

Stellen Sie sich vor, was mit einer API geschehen kann, die von einer klinischen Abteilung ohne angemessene Überwachung durch die zentralen IT- oder Sicherheitsteams eingesetzt wird. Diese API könnte:

- für die gemeinsame Nutzung von Patientendaten ohne angemessene HIPAA-konforme Kontrollen entwickelt worden sein,
- nach System-Upgrades aktiv geblieben sein und unbekannte Zugriffspunkte geschaffen haben,
- von herkömmlichen Sicherheitstools übersehen worden sein, die nicht dafür ausgelegt sind, nicht verwaltete APIs zu erkennen,
- von Angreifern ausgenutzt worden sein, um auf geschützte Gesundheitsdaten zuzugreifen,
- von einem authentischen Partner missbraucht worden sein, der den Endpunkt für unbeabsichtigte Anwendungsfälle verwendet hat.

84,7 % der Gesundheitsorganisationen haben in den letzten 12 Monaten einen API-Vorfall erlebt.

65 % der Gesundheitsorganisationen verfügen über vollständige API-Bestände, aber nur 24 % davon wissen, welche APIs sensible Daten zurückgeben.

510.600 $ = finanzielle Auswirkungen von API-Sicherheitsvorfällen für Gesundheitsorganisationen in den letzten 12 Monaten

Die drei wichtigsten Folgen

1. **Verlust von Vertrauen und Rufschädigung** (28.7 %)
2. **Produktivitätsverlust** 28,7 %
3. **Verstärkte interne Prüfungen** (27,3 %)

Quelle:
Akamai, „API-Sicherheitsstudie“, 2024.

Akamai

Diese Szenarien sind nicht nur hypothetisch. Da Datenschutzverletzungen in der Gesundheitsbranche Rekordhöhen erreichen und die Kosten für Datendiebstahl durchschnittlich 4,88 Millionen $ betragen,[1] stellen API-Schwachstellen ein wachsendes Compliance- und Sicherheitsrisiko dar. Darüber hinaus spiegelt dieses Szenario wider, was Ihre Kollegen als Hauptursachen für API-Vorfälle anführen.

Auswirkungen von API-Vorfällen auf Compliance, Kosten und Mitarbeiterbelastung

Laut dem im Mai 2024 erschienenen Gartner® Market Guide für API-Schutz[2] zeigen aktuelle Daten, dass eine durchschnittliche API-Verletzung zu mindestens zehnmal mehr geleakten Daten führt als eine durchschnittliche Sicherheitsverletzung.

Es ist kein Wunder, dass sich die HIPAA-Compliance zunehmend auf die API-Sicherheit konzentriert. HIPAA erwähnt zwar nicht ausdrücklich APIs, verlangt aber eine Beschränkung des PHI-Zugriffs auf der Grundlage von Mitarbeiterrollen. Dies erfordert Authentifizierung und Zugriffskontrolle in APIs, die Patientendaten übertragen. Gesundheitsdienstleister und Kostenträger – und deren Aufsichtsbehörden – müssen wissen, welche Arten von Daten nicht nur über ihre eigenen APIs, sondern auch über die APIs ihrer Partner und Lieferanten übertragen werden. Dies stellt eine weitere Herausforderung für die Kontrolle von Risiken Dritter für die Gesundheitsbranche dar.

Verlorenes Vertrauen bei Aufsichtsbehörden kann zu verstärkten Prüfungen und damit zu mehr Arbeit für enorm beanspruchte Teams führen, die Mühe haben, Compliance-Anforderungen zu erfüllen. Auch hohe Geldstrafen können eine Folge sein. Mit Blick darauf ist klar, dass Gesundheitsorganisationen sich über die finanziellen Folgen von API-Bedrohungen im Klaren sind. Erstmalig haben wir die Teilnehmer in den drei untersuchten Ländern gebeten, die geschätzten Kosten von API-Sicherheitsvorfällen aus den letzten 12 Monaten mitzuteilen.

	Gesundheitsbranche	Durchschnitt aller Branchen
USA	510.600 $	591.404 $
Vereinigtes Königreich	363.885 £	420.103 £
Deutschland	643.884 €	403.453 €

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.

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, betonten unsere Befragten „Verlust von Vertrauen und Rufschädigung“ (28,7 %) und „Produktivitätsverlust“ (28,7 %). Diese Folgen haben langfristige Auswirkungen. Das geschädigte Vertrauen der Patienten kann die Einnahmen künftiger Jahre schmälern, während Produktivitätsverluste bei den ohnehin schon angespannten Mitarbeitern des Gesundheitswesens Burnout und niedriges Engagement beschleunigen können.

[1] IBM-Bericht „Cost of a Data Breach“ (Kosten durch Datendiebstahl), 2024

[2] Gartner, Market Guide für API-Schutz, 29. Mai 2024. GARTNER ist eine eingetragene Marke und Dienstleistungsmarke von Gartner, Inc. bzw. seinen Vertragspartnern in den USA und weltweit und wird hierin mit Genehmigung verwendet. Alle Rechte vorbehalten.

Risiken und Stress durch proaktive API-Sicherheit reduzieren

API-Angriffe auf Unternehmen im Gesundheitswesen 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 sichern und die Belastungen für Sicherheitsteams verringern. Gleichzeitig wird das hart erarbeitete Vertrauen von Vorständen und Kunden gewahrt. Zu diesen Schritten gehören der Aufbau von Wissen in Ihrem Teams 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 Ihnen helfen 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: 03/25.