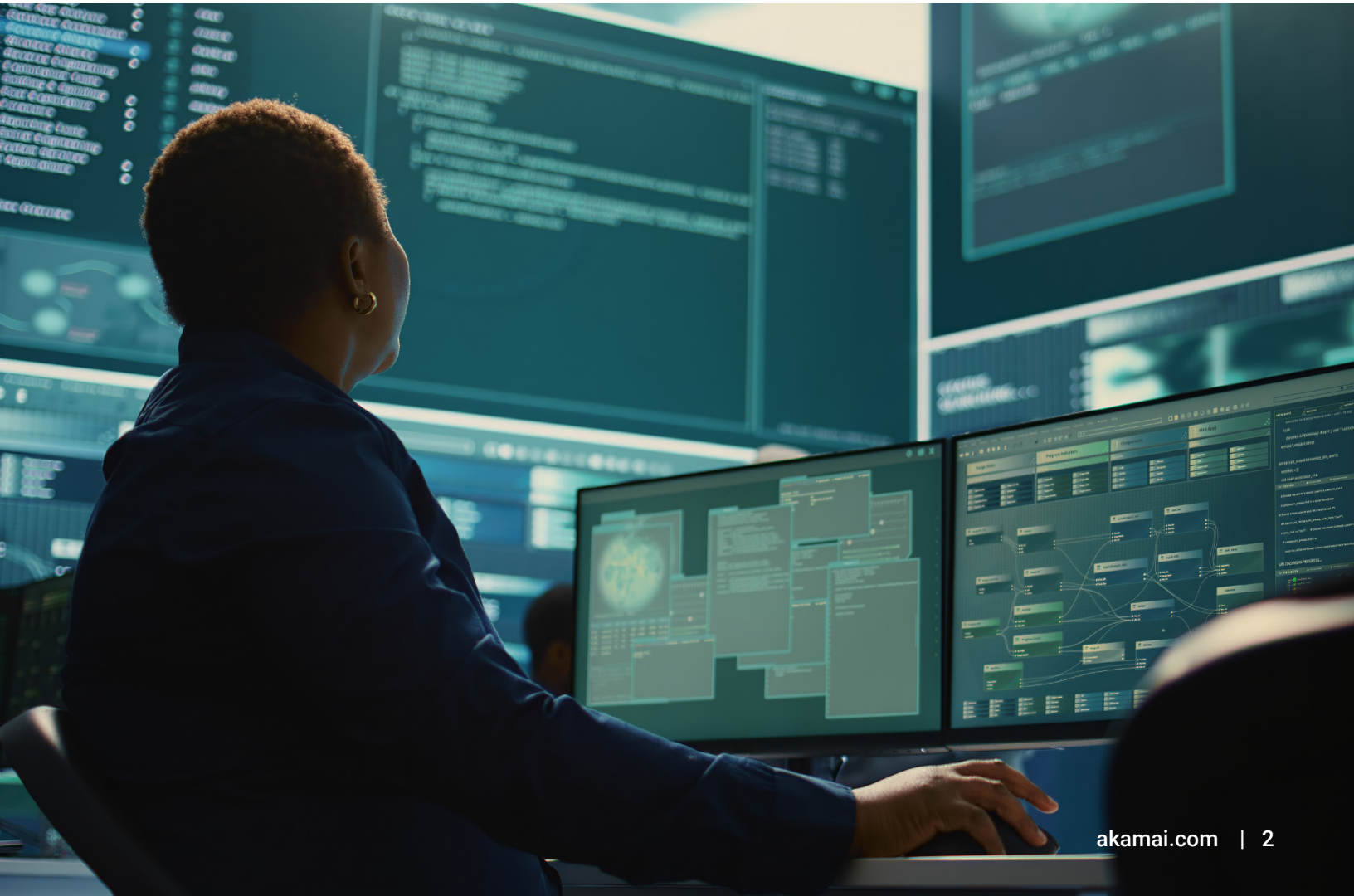
Akamai

WHITEPAPER

API-Sicherheit und -Compliance

Implizite und explizite Anforderungen an den Datenschutz

In diesem Bericht



Einführung

Für den Nachweis der Compliance mit Datenschutzvorschriften mussten in der Vergangenheit große Mengen an Energie und Ressourcen aufgewendet werden, um mit – meist bekannten – Risiken Schritt zu halten. Aber das ändert sich. Die moderne Angriffsfläche entwickelt sich schnell und umfasst Bedrohungen, die die meisten Compliance-Unternehmensprogramme nicht vollständig berücksichtigen. Das liegt zum Teil daran, dass die Aufsichtsbehörden selbst nicht immer Schritt halten können und nicht alle Facetten des Schutzes, der zur Vermeidung von Verstößen erforderlich ist, klar benennen können.

Das ist auch beim API-Schutz der Fall. Jedes Mal, wenn ein Kunde, ein Partner oder ein Lieferant digital mit Ihrem Unternehmen in Kontakt tritt, arbeitet eine API hinter den Kulissen, um einen schnellen Informationsaustausch zu ermöglichen, der häufig sensible Daten umfasst. Angreifer wissen nun, dass sie ihre Strategie zum Diebstahl dieser Daten vereinfachen können, indem sie sich direkt auf APIs konzentrieren.

Möglicherweise haben Sie bereits neue Formulierungen in Vorschriften gesehen, die darauf hinweisen, dass APIs inventarisiert, bewertet oder gesichert werden müssen. Doch selbst wenn keine spezifischen API-Formulierungen enthalten sind – die Tatsache, dass sie zu einem eindeutigen Angriffsvektor geworden sind, *impliziert*, dass angemessener API-Schutz erforderlich ist.

Die Entstehung von APIs als zentrales Compliance-Problem ist nicht überraschend. Exponierte oder falsch konfigurierte APIs sind weit verbreitet, leicht zu missbrauchen und häufig ungeschützt. Und nur eine erfolgreich angegriffene API kann dazu führen, dass Millionen von Datensätzen gestohlen werden. Die Zahlen sprechen für sich:

- 78 % der Unternehmen haben laut bereits einen API-Sicherheitsvorfall erlebt.[1]
- 44 % wurden von Regulierungsbehörden wegen API-Sicherheitsvorfällen mit Geldstrafen belegt.[2]

Wie wirkt sich das auf Ihren Compliance-Ansatz aus? Sie müssen Aufsichtsbehörden vermitteln, dass Ihr Unternehmen Maßnahmen zum Schutz aller Zugriffspunkte für sensible Daten ergreift. Das bedeutet, dass Sie demonstrieren müssen, dass Ihr Unternehmen folgende Punkte erfüllt:

- Jede API berücksichtigen, einschließlich schwer fassbarer Shadow-APIs
- Alle API-Schwachstellen entdecken und beheben
- Maßgeschneiderte Kontrollen anwenden, um API-basierte Datenschutzverletzungen zu verhindern

Dieses Whitepaper untersucht die Art der zunehmenden API-Risiken, hebt sechs Beispiele für Vorschriften und Frameworks hervor, die (entweder explizit oder implizit) API-Schutz erfordern, und gibt Ratschläge, wie die Compliance-Anforderungen durch bewährte API-Best-Practices erfüllt werden können.

1., 2. Akamai Technologies, „Das Problem mit der API-Sicherheit“, 2023

API-Risiken verstehen

APIs stehen im Kern der digitalen Produkte, Services und Cloud-Umgebungen Ihres Unternehmens. Ihr ständiger Zugriff auf Daten macht sie sowohl zu einem Umsatztreiber als auch zu einem Betriebsrisiko. Das Problem ist, dass die meisten Unternehmen – selbst solche mit ausgereiften Sicherheitsprogrammen – API-bezogene Bedrohungen nicht so stark priorisieren wie andere Bedrohungen, darunter Phishing oder Ransomware.

Einige Unternehmen verlassen sich für grundlegenden API-Schutz auf API-Gateways und Web Application Firewalls (WAFs), doch diese bieten nicht dasselbe Maß an Transparenz, Echtzeitschutz und kontinuierlichen Tests, wie es spezielle API-Sicherheitslösungen können. Diese Tools reichen aus folgenden Gründen nicht aus:

- API-Gateways und WAFs können nur *verwalteten* API-Traffic beobachten, der durch sie weitergeleitet wird.
- Nicht-verwaltete APIs können sie nicht schützen. Und Analysten prognostizieren, dass Letztere bis 2025 fast die Hälfte des API-Ökosystems eines typischen Unternehmens ausmachen werden.
- Infolgedessen sind Sicherheitsteams nicht vollständig darauf vorbereitet, den am schnellsten wachsenden Teil ihrer Angriffsfläche zu schützen. Denn sie wissen nur wenig darüber, wohin APIs geleitet werden, wie sie konfiguriert sind, welche Arten von sensiblen Daten sie austauschen und welche Risiken sie mit sich bringen.

Der Schutz von Nutzerdaten hat für Regulierungsbehörden Priorität und sie verhängen schwere Geldstrafen gegen Unternehmen, die die Daten ihrer Kunden nicht angemessen vor unberechtigtem Zugriff schützen. Nur 4 von 10 Sicherheitsexperten mit vollständigen API-Beständen wissen, welche ihrer APIs vertrauliche Daten zurückgeben[3], und viele API-Aufrufe stammen von Angreifern, die nach Schwachstellen suchen. Das legt nahe, dass Datenverletzungen über APIs noch weiter zunehmen werden – vor allem, weil API-Angriffe derzeit recht einfach durchzuführen sind.

3. Akamai Technologies, „Das Problem mit der API-Sicherheit“, 2023

Vier API-Angriffe mit Compliance-Auswirkungen

Wie kann ein API-Verstoß die Compliance eines Unternehmens beeinträchtigen? Hier einige Beispiele:

- Eine beliebte Projektmanagement-Anwendung wurde von einem Angreifer kompromittiert, der einen API-Endpunkt ohne Authentifizierungskontrollen ausnutzte. Der Angreifer verschaffte sich Zugang zur API, erhielt unbefugten Zugriff auf Informationen von Millionen von Nutzern und legte Monate später über 21 GB an Daten im Internet offen – einschließlich E-Mail-Adressen und Vorstandsmitgliedschaften.
- Mehr als elf Millionen Kundendatensätze eines großen Telekommunikationsunternehmens wurden veröffentlicht, vermeintlich wegen einer API, die unwissentlich über das öffentliche Internet zugänglich war und keine Authentifizierung erforderte. Angreifer haben sich Zugriff zur API verschafft, haben erkannt, dass ihr eine eindeutige Kennung fehlte, haben ihre ID-Nummer erraten und konnten so ganz leicht vertrauliche Daten abrufen.
- Berichten zufolge wurde ein Social-Media-Unternehmen in den letzten Jahren zweimal von einem Scraping-Angriff getroffen, der durch unsachgemäße API-Nutzung ermöglicht wurde. In erster Linie wurden private Daten aus 500 Millionen Nutzerprofilen ausgelesen und dann verkauft. Anschließend erstellte ein Angreifer eine Datenbank mit Telefonnummern und Gehaltsdaten, die von 700 Millionen Nutzern gestohlen wurden.
- Dieselbe Technik wurde auch gegen ein anderes Social-Media-Unternehmen eingesetzt, um Daten von Millionen von Nutzern zu stehlen. Das Unternehmen erhielt eine Geldstrafe von fünf Milliarden US-Dollar, weil ein Drittanbieter die API des Unternehmens genutzt hatte, um vertrauliche Daten zu sammeln. Es spielte keine Rolle, dass es der Anbieter war, der die API ausgenutzt hatte: Das Unternehmen *selbst* wurde mit einer Geldbuße belegt, weil es seine Anwendung nicht überwacht hatte.

Sechs Beispiele für Vorschriften und Frameworks, die API-Sicherheit erfordern

In vielen Vorschriften und Frameworks werden APIs nicht unbedingt namentlich genannt, aber die Anforderungen konzentrieren sich eindeutig auf den Schutz der Anwendungen und der Infrastruktur, in denen APIs betrieben werden. Zum Beispiel:

- Der PCI DSS v4.0 (Payment Card Industry Data Security Standard) sieht vor, dass Unternehmen nachweisen, dass ihre Software die Funktionen externer Komponenten auf sichere Weise nutzt. Das umfasst beispielsweise APIs, die Zahlungsdaten von einer mobilen App an das System einer Bank übertragen.
- Das NIST Secure Software Development Framework bietet Anweisungen zur Entwicklung gut geschützter Software, zum kontinuierlichen Schutz und zur Reaktion auf Schwachstellen. APIs bilden das Herzstück der Software-Entwicklung.

In vielen Fällen werden in den Vorschriften lose definierte Ziele für den Schutz von Daten vorgeschlagen, darunter die Forderung der Datenschutz-Grundverordnung (DSGVO) nach „angemessenen Sicherheitsmaßnahmen“. Ihre APIs erhalten möglicherweise Millionen von Aufrufen pro Tag, die solche Daten anfordern – von Kunden *und* Angreifern. Sie müssen bestimmen, welche Sicherheitskontrollen erforderlich sind – und dann demonstrieren, wie sie funktionieren.

Werfen wir einen genaueren Blick auf Vorschriften und Frameworks, die direkte Auswirkungen auf Ihr API-Ökosystem haben.

1. PCI DSS v4.0

Der PCI DSS wurde vom Payment Card Industry Security Standards Council (PCI SSC) aufgestellt und ist zu einem globalen Standard zum Schutz von Zahlungsdaten geworden. Wenn Ihr Unternehmen gängige Kreditkarten akzeptiert und Karteninhaberdaten elektronisch verarbeitet, speichert oder überträgt, müssen Sie diesen Standard einhalten.

Die Anforderungen der ursprünglichen Version decken Sicherheitsgrundlagen ab, die heute genauso wichtig sind wie bei der Veröffentlichung von PCI DSS im Jahr 2006: Unternehmen dürfen nur Personen Zugriff auf System- und Karteninhaberdaten gewähren, die ihn zwingend benötigen, und müssen die Zugriffsanforderungen nach Rolle definieren.

Doch mit PCI DSS v4.0 müssen sie auch ihre Compliance-Programme anpassen, um auf Angreifer reagieren zu können, die häufig Tausende von APIs in Zahlungstechnologien ins Visier nehmen. Insgesamt konzentriert sich PCI DSS v4.0 auf vier Hauptziele:

1. Weiterhin die Sicherheitsanforderungen der Zahlungsbranche erfüllen
2. Sicherheit als kontinuierlichen Prozess verstehen
3. Unternehmen Flexibilität bei der Erfüllung der Anforderungen ermöglichen (z. B durch neue Tools oder Kontrollen)
4. Validierungsmethoden und -prozesse optimieren

Anforderung 6.2.3 in PCI DSS v4.0 konzentriert sich auf die Notwendigkeit, dass Unternehmen ihren maßgeschneiderten Anwendungscode (d. h. Code, der von einem Drittanbieter entwickelt wurde, statt handelsüblicher Standardanwendungen) prüfen müssen, um sicherzustellen, dass keine Schwachstellen in die Produktion gelangen. Speziell im Zusammenhang mit APIs enthält diese Anforderung eine Anleitung, um zu bestätigen, dass die Software eines Unternehmens die Funktionen externer Komponenten (wie Bibliotheken, Frameworks, APIs usw.) sicher verwendet. Anforderungen wie diese unterstreichen die Schlüsselrolle, die APIs in der umfassenderen Software-Lieferkette spielen – und sie machen deutlich, was es braucht, um APIs zu schützen.

APIs sind in modernen Anwendungsumgebungen zur Standardmethode für Konnektivität und Datenaustausch geworden. Deshalb ist es unerlässlich, APIs sowohl vor der Produktion („Shift Left“) als auch nach der Produktion („Shield Right“) zu schützen, um Ihr digitales Unternehmen gegen Angriffe zu rüsten. Im Folgenden finden Sie einige Best Practices für API-Sicherheit, die Sie bei der Einhaltung von Anforderung 6.2.3 unterstützen:

- Überprüfen Sie die Verwendung API-basierter Komponenten und ihrer Sicherheitsstatus (z. B. indem Sie Fehlkonfigurationen finden, die zu Schwachstellen führen, darunter auch die Verwendung schwacher Verschlüsselungscodes).
- Überprüfen Sie die normale und erwartete API-Verwendung und implementieren Sie Kontrollmechanismen, um Cyberkriminelle daran zu hindern, Ihre Systeme zu missbrauchen (überprüfen Sie beispielsweise das Verhalten der Anwendung, um Logikschwachstellen zu erkennen).
- Erkennen Sie Frameworks von Drittanbietern, die Ihre APIs unterstützen, und ermitteln Sie, ob diese veraltet und anfällig sind.
- Erstellen Sie einen vollständigen Bestand aller APIs, einschließlich der verschiedenen Versionen, die Sie ausführen. So erhalten Sie Einblicke in Backdoors und mögliche nicht dokumentierte Funktionen, die Sie verwalten müssen.
- Überprüfen Sie die Sicherheit Ihres API-Codes und achten Sie darauf, dass keine API-bezogenen Schwachstellen in die Produktion gelangen.
- Implementieren Sie Best Practices für sichere API-Programmierung, mit denen Sie einen programmatischen Ansatz zur kontinuierlichen und sicheren Codebereitstellung verfolgen können.

2. Datenschutz-Grundverordnung (DSGVO)

Die DSGVO ist eine Rechtsvorschrift der Europäischen Union, um den Datenschutz für Personen innerhalb der EU zu stärken und zu vereinheitlichen. Sie ist jedoch nicht auf Unternehmen mit Sitz in der EU beschränkt: Jedes Unternehmen, das Konsumgüter oder Dienstleistungen in der EU anbietet, muss sich daran halten.

Die Verordnung schreibt vor, dass personenbezogene Daten Informationen sind, die mit einer Person in Verbindung gebracht werden können. Die gemäß der DSGVO regulierten Daten können den Namen einer Person, ihre Kontaktinformationen, Bank- und Finanzdaten sowie medizinische Informationen umfassen. Auf der technischeren Seite umfassen die abgedeckten Daten auch Standortdaten wie IP-Adressen und Web-Cookies.

Was bedeutet das für die API-Sicherheit? Egal, ob Sie Anwendungen, Microservices oder IoT-Geräte (Internet of Things) entwickeln – die APIs, die sich im Zentrum dieser Technologien befinden, tauschen wahrscheinlich DSGVO-regulierte Daten aus. Deshalb müssen Unternehmen, die über das Internet zugängliche APIs entwickeln, den Datenschutz von Anfang an in das API-Design einfließen lassen – und nicht erst danach.

Befolgen Sie das Prinzip der geringstmöglichen Berechtigungen, das sicherstellt, dass Nutzer nur über die Berechtigungen verfügen, die sie zwingend für die Ausführung ihrer Aufgaben benötigen.

Artikel 25 der DSGVO *thematisiert die geringstmögliche Berechtigung*. Unternehmen sind verpflichtet, „technische und organisatorische Maßnahmen [zu treffen], die sicherstellen, dass durch Voreinstellung nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden.“ Im Gegenzug sollten API-Entwickler Kontrollmechanismen zur Nutzerauthentifizierung und -autorisierung implementieren, um die vertraulichen Daten, die ihre APIs durchlaufen, zu schützen. API-Entwicklungsteams müssen außerdem sicherstellen, dass Daten während der Übertragung vertraulich bleiben, indem sie sichere Kommunikationsprotokolle verwenden, um den Informationsaustausch zwischen Client und Server zu verschlüsseln.

Wie sieht es jedoch mit dem bestehenden Ökosystem von APIs aus, das Unternehmen in den letzten Jahren oder sogar Jahrzehnten aufgebaut hat? Ein erheblicher Teil der Unternehmens-APIs wird nicht verwaltet, wurde vergessen oder läuft einfach kontinuierlich ohne Kontrolle. In diesen Fällen erfordert die Einhaltung der DSGVO Folgendes:

- Erkennung jeder API in Ihrer IT-Umgebung
- Bewertung ihrer Risikofaktoren (z. B. die Art der Daten, die sie ausgetauscht haben, sowie die Frage, wer oder was auf diese Daten zugreifen kann)
- Beseitigung von Schwachstellen wie Fehlkonfigurationen oder schwachen Authentifizierungsmechanismen
- Kontinuierliche Tests von APIs auf ihre Resilienz gegenüber gängigen und neuen Angriffsmethoden

3. Digital Operational Resiliency Act (DORA)

Angesichts der Rolle des EU-Finanzsektors als kritischer Infrastrukturbetreiber sollen die Anforderungen von DORA Unternehmen in EU-Mitgliedstaaten dabei helfen, Cyberangriffen standzuhalten und sich davon zu erholen. Mit DORA verfügt der Sektor über ein verbindliches, umfassendes Risikomanagement-Framework für die Informations- und Kommunikationstechnologie (IKT). Das Gesetz zielt darauf ab, die Anforderungen für Finanzunternehmen in der EU zu harmonisieren und zu verschärfen, da die derzeitige Landschaft eine Vielzahl verschiedener Vorschriften und Standards umfasst.

Insgesamt sind mehr als 22.000 Finanzinstitute und IT-Dienstleister in der EU von DORA betroffen. Dazu gehören auch Dritte, die EU-Finanzunternehmen IKT-Systeme und -Dienste bereitstellen, einschließlich Cloud-Dienst-Anbietern. Das Gesetz fordert von Finanzinstituten, IKT-Risikostrategien für Dritte zu entwickeln und eine Due-Diligence-Prüfung durchzuführen, um die Eignung der Anbieter zu gewährleisten.

DORA enthält mehrere Anforderungen, die sich auf API-Sicherheit auswirken, darunter auch digitale Betriebsstabilität: Diese erfordert von Unternehmen, regelmäßige Testprogramme zu implementieren, die potenzielle Lücken, Schwachstellen und/oder Mängel in der digitalen Betriebsstabilität identifizieren. Das umfasst beispielsweise Netzwerksicherheitstests, Penetrationstests, Tests von Webanwendungen und vieles mehr. Es ist wichtig, obligatorische Prüfungen basierend auf bedrohungsorientierten Penetrationstests (Threat-led Penetration Tests, TLPTs) durchzuführen – je nach Größe, Risiko und Geschäftsprofil des Finanzunternehmens. Ebenso wichtig ist es, Ihre APIs regelmäßig auf Schwachstellen zu testen.

DORA erläutert Beispiele für Sicherheitstests, die Tests von webbasierten Anwendungen und APIs umfassen. Dazu gehört auch der Einsatz öffentlicher Ressourcen wie des Open Worldwide Application Security Project (OWASP). Insbesondere die OWASP Top 10 der API-Sicherheitsrisiken helfen Unternehmen dabei, Konfigurationsfehler, Schwächen, Logikfehler und Codeprobleme zu identifizieren, die es Angreifern ermöglichen, auf Unternehmensressourcen zuzugreifen, sie zu manipulieren oder sie anderweitig zu kontrollieren.

4. Health Insurance and Portability and Accountability Act (HIPAA)

HIPAA konzentriert sich auf Datenschutz- und Sicherheitsregeln zum Schutz geschützter Gesundheitsdaten (Protected Health Information, PHI) in elektronischen Gesundheitsakten (Electronic Health Record, EHR), computergestützten Arztbestellplattformen und anderen IT-Systemen im Gesundheitswesen. Jeder US-Gesundheitsdienstleister, Planadministrator und jede Verrechnungsstelle, der/die PHI elektronisch speichert oder überträgt, muss den HIPAA einhalten. Das beinhaltet die Gewährleistung der Vertraulichkeit, Integrität und Verfügbarkeit von PHI und den Schutz vor unbefugter Offenlegung und unsachgemäßer Verwendung.

HIPAA ist ein Beispiel für eine Verordnung, die erhebliche Auswirkungen auf APIs hat, auch wenn APIs in ihren Anforderungen nicht ausdrücklich erwähnt werden.

Denken Sie an einen Technologieanbieter, der Patientenportale für rund um die Uhr verfügbare Kliniken erstellt. Eine grundlegende Funktion dieser Portale ist die Fähigkeit, Patienten effizienten und sicheren Zugriff auf Daten zu ihren Arztbesuchen, Testergebnissen, Zahlungen und mehr zu ermöglichen. APIs ermöglichen diesen Datenaustausch. Sowohl die Klinik als auch der Anbieter sind verpflichtet, die HIPAA-Anforderungen einzuhalten.

Die HIPAA-Datenschutzregel legt fest, dass betroffene Unternehmen Richtlinien und Verfahren entwickeln und umsetzen müssen, die PHI-Zugriff und -Nutzung auf Grundlage der spezifischen Rollen ihrer Mitarbeiter einschränken. Daher müssen die API-Entwickler eines Unternehmens technische Sicherheitsvorkehrungen wie Authentifizierung, eindeutige Nutzer-IDs und rollenbasierte Zugriffskontrollen integrieren, um sicherzustellen, dass die geringstmöglichen Berechtigungen vergeben werden.

Auch Transparenz ist für HIPAA-Unternehmen von entscheidender Bedeutung – sei es ein Anbieter, dessen IT-Team maßgeschneiderte APIs erstellt, oder ein Drittanbieter, der APIs für den ersten Anbieter entwickelt. Unternehmen benötigen Echtzeitbewertungen und Berichte über die Risikolage jeder API, einschließlich der Arten von PHI, die sie übertragen. Das ist nicht nur für die Compliance relevant, sondern auch für die Erfüllung der HIPAA-Anforderung, dass Unternehmen auf Personen reagieren müssen, die Informationen darüber anfordern, wann, wo, warum und wem ihre PHI offengelegt wurden.

5. Richtlinie zur Netz- und Informationssicherheit (NIS2)

Die EU hat im Januar 2023 Version 2.0 der NIS-Richtlinie in Kraft gesetzt, die auf den Leitlinien der ursprünglichen Version für die Sicherung der IT-Infrastruktur und die Meldung von Vorfällen aufbaut. Obwohl APIs in v2.0 nicht ausdrücklich erwähnt werden, haben die Anforderungen erhebliche Auswirkungen auf den Schutz und die Verwaltung von APIs, da sie für viele digitale Dienste in Unternehmen, die der Richtlinie unterliegen, unverzichtbar sind. NIS2 umfasst Folgendes:

- Ein breiteres Spektrum von Sektoren – so wurden beispielsweise Cloud-Dienst-Anbieter und Social-Media-Unternehmen in die bestehende Liste aufgenommen, die auch Betreiber kritischer Infrastrukturen umfasst. In diesen Sektoren, in denen APIs intensiv für Integration und Servicebereitstellung verwendet werden, wird die API-Sicherheit zu einer Priorität.
- Ein neuer Schwerpunkt auf dem Schutz der Lieferkette – Unternehmen müssen Risiken bewerten und ihre IT-Lieferketten und Drittanbieter-Beziehungen schützen. Da APIs häufig zur Integration externer Services verwendet werden, ist die Gewährleistung ihrer Sicherheit entscheidend für die Compliance.
- Die Anforderung, ein Informationssicherheitsmanagement-System aufzubauen, das Personen, Richtlinien und Technologien bewertet, um sensible Ressourcen zu schützen und die betriebliche Resilienz zu gewährleisten. Da APIs schnell wachsende Angriffsvektoren sind, müssen sie in Risikomanagement-Strategien einbezogen werden.
- Die Meldung größerer Cybersicherheitsvorfälle, darunter auch API-Angriffe. Daher müssen Unternehmen Mechanismen zur Überwachung, Erkennung und Meldung von API-bezogenen Vorfällen einrichten.

6. Leitlinien für US-Aufsichtsbehörden im Finanzdienstleistungssektor

Der Federal Financial Institutions Examination Council (FFIEC) erstellt die Leitlinien und Standards für die Regulierungsbehörden zur Überwachung der US-Finanzbranche. Dazu gehören die US-Notenbank, die FDIC, das OCC und die NCUA. Aufgabe des FFIEC ist es, Verbraucher und Investoren vor Betrug, Missbrauch und Fehlverhalten zu schützen. Obwohl es sich nicht um eine Verordnung handelt, sind die Leitlinien des FFIEC entscheidend, um zu gewährleisten, dass Finanzunternehmen wissen, wie sie die empfohlenen Sicherheitsmaßnahmen erreichen können.

Dieser Fall ist ein Beispiel für ein Dokument, das spezifische Anweisungen zum Schutz von APIs sowie zum Schutz von Verbrauchern vor Betrug und Identitätsdiebstahl enthält. Hier eine Übersicht:

- **Bestandsaufnahme:** Der FFIEC empfiehlt eine Bestandsaufnahme aller Informationssysteme, die Authentifizierung und Zugriffskontrollen erfordern – dazu gehören auch APIs. Das gilt nicht nur für Finanzinstitute, sondern auch für deren Drittanbieter wie Cloud-Dienst-Anbieter.
- **Authentifizierung:** Die API sollte nur autorisierten Nutzern Zugriff gewähren. Es ist wichtig, alle Nutzer (z. B. Kunden) zu identifizieren, für die Zugriffskontrollen erforderlich sind. Außerdem ist es wichtig, Nutzer zu identifizieren, die erweiterte Kontrollen wie Multi-Faktor-Authentifizierung erfordern.
- **Autorisierung:** Die API sollte autorisierten Nutzern nur Zugriff auf spezifische Ressourcen gewähren. Der FFIEC empfiehlt die Implementierung mehrschichtiger Sicherheit, z. B. Überwachung, Protokollierung und Reporting von Aktivitäten, um unbefugten Zugriff zu identifizieren und zu verfolgen.
- **Risikomanagement:** Es gibt eine Reihe wirksamer Risikomanagement-Verfahren, die der FFIEC in seinen neuesten Leitlinien festlegt. APIs werden jedoch explizit in der Kategorie „Bestandsaufnahme der Informationssysteme“ erwähnt, was bedeutet, dass Sie eine genaue Bestandsaufnahme Ihrer APIs benötigen.

Vielleicht ist ein Unternehmen hinsichtlich bekannter Bedrohungen wie Phishing oder Ransomware auf dem Laufenden, doch der FFIEC fordert, dass Unternehmen *jede* Cyberbedrohung identifizieren, bei der eine „angemessene Wahrscheinlichkeit [besteht], dass die Informationssysteme [und Daten] von Finanzinstituten betroffen werden“. Wie bereits in der Einführung erwähnt, sind 78 % der Unternehmen mit API-Sicherheitsvorfällen konfrontiert. API-Schutz wird also früher oder später entscheidend für die Compliance sein, da sich die Anforderungen der Finanzaufsichtsbehörden ständig weiterentwickeln.

Compliance-Herausforderungen mit optimalem API-Schutz meistern

Die heutige Bedrohungslandschaft erfordert eine umfassende API-Sicherheitslösung, die API-Erkennung, Sicherheitsmanagement, Laufzeitschutz und API-Sicherheitstests bietet. Dieser umfassende Ansatz ergänzt jede bereits vorhandene WAF und jedes API-Gateway.

1. API-Erkennung

Es ist nicht ungewöhnlich, APIs zu haben, von denen niemand weiß. Die meisten Unternehmen haben wenig bis gar keinen Einblick in einen Großteil ihres API-Traffics – oft weil sie annehmen, dass all ihre APIs über ein API-Gateway weitergeleitet werden. Aber das stimmt nicht. Ohne eine vollständige und genaue Bestandsaufnahme ist Ihr Unternehmen einer Reihe von Risiken ausgesetzt. Erforderliche Kernfunktionen:

- APIs finden und in Bestand aufnehmen, unabhängig von Konfiguration oder Typ
- Inaktive, veraltete und Zombie-APIs entdecken
- Vergessene, ungenutzte oder anderweitig unbekannte Schatten-Domains identifizieren
- Blinde Flecken beseitigen und potenzielle Angriffspfade ermitteln

2. API-Sicherheitsmanagement

Wenn ein vollständiger API-Bestand vorhanden ist, müssen Sie verstehen, welche Arten von Daten durch Ihre APIs fließen und wie sich dies auf die Einhaltung gesetzlicher Vorschriften auswirkt. API-Sicherheitsmanagement bietet eine umfassende Ansicht von Traffic, Code und Konfigurationen, um die API-Sicherheitslage Ihres Unternehmens zu beurteilen. Erforderliche Kernfunktionen:

- Infrastruktur automatisch scannen, um Fehlkonfigurationen und versteckte Risiken aufzudecken
- Nutzerdefinierte Workflows erstellen, um wichtige Stakeholder über Schwachstellen zu informieren
- Ermitteln, welche APIs und internen Nutzer auf sensible Daten zugreifen können
- Erkannten Problemen einen Schweregrad zuweisen, um Abhilfemaßnahmen zu priorisieren

3. API-Laufzeitsicherheit

Sie kennen wahrscheinlich das Konzept „Gehen Sie davon aus, dass Ihre Umgebung angegriffen wird“. API-spezifische Sicherheitsverletzungen und Angriffe sind langsam ebenso unvermeidlich wie andere Cybersicherheitsrisiken. Für alle APIs, die in der Produktion aktiv sind, müssen Sie in der Lage sein, Angriffe in Echtzeit zu erkennen und zu blockieren. Erforderliche Kernfunktionen:

- Daten auf Manipulation und Datenlecks, Richtlinienverstöße, verdächtiges Verhalten und API-Angriffe überwachen
- API-Traffic ohne zusätzliche Änderungen am Netzwerk oder schwer zu installierende Agents analysieren
- In bestehende Workflows (Ticketerstellung, SIEM usw.) integrieren, um Sicherheits-/Betriebsteams zu warnen
- Angriffe und Missbrauch in Echtzeit mit teil- oder vollautomatischen Abhilfemaßnahmen verhindern

4. API-Sicherheitstests

API-Entwicklungsteams stehen unter dem Druck, so schnell wie möglich arbeiten zu müssen. Geschwindigkeit ist für jede entwickelte Anwendung von entscheidender Bedeutung – denn so können leichter Schwachstellen oder Konstruktionsfehler auftreten und bleiben anschließend eher unentdeckt. Wenn APIs in der Entwicklung getestet werden, bevor sie in die Produktion gehen, sinken nicht nur die Risiken, sondern auch die Kosten für die Behebung anfälliger APIs erheblich. Erforderliche Kernfunktionen:

- Eine Vielzahl automatisierter Tests durchführen, die schädlichen Traffic simulieren
- Schwachstellen entdecken, bevor APIs zum Einsatz kommen, um das Risiko eines erfolgreichen Angriffs zu verringern
- Ihre API-Spezifikationen anhand etablierter Governance-Richtlinien und -Regeln überprüfen
- API-fokussierte Sicherheitstests on demand oder im Rahmen einer CI/CD-Pipeline ausführen

So kann Akamai API Security die Komplexität der API-Compliance minimieren

APIs sind eine der Hauptursachen für die Verstöße, die durch die aktuellen Vorschriften verhindert werden sollen. Was ist erforderlich, um Ihr Unternehmen zu schützen, während APIs – und ihre Risiken – immer weiter zunehmen? Die vorhandenen Tools, die viele Unternehmen für den grundlegenden API-Schutz verwenden, bieten zwar gewissen Schutz, doch er reicht nicht aus. Wenn Sie nach einer besseren Möglichkeit suchen, die APIs Ihres Unternehmens zu schützen und die Compliance nachzuweisen, können wir Ihnen gerne dabei helfen.

Bei allen Anforderungen und Richtlinien, die in diesem Whitepaper behandelt werden, bietet Akamai API Security den Schutz, den Unternehmen benötigen – nicht nur um Vorschriften einzuhalten, sondern auch um Daten und das Vertrauen Ihrer Kunden zu schützen.

Die umfassende Lösung von Akamai schützt APIs von der Anfangsphase der Entwicklung bis hin zur Postproduktion und gibt Ihnen die Möglichkeit, die wichtigsten Best Practices einzuhalten:

- API-Erkennung
- Kontrolle der Sicherheitslage
- Laufzeitschutz
- Sicherheitstests

Erfahren Sie mehr über APIs und darüber, wie Sie sie vor Angriffen schützen können.

Erfahren Sie, wie Akamai API Security Ihr Unternehmen unterstützen kann.

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. Gemeinsam mit Ihnen können wir auf diese Weise 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 (ehemals Twitter) und LinkedIn. Veröffentlicht: 09/24.