Akamai

WHITEPAPER

# 5 Schritte zur kontinuierlichen API-Sicherheit

# In diesem Bericht



# API-Sicherheit als Herausforderung

APIs (Application Programming Interfaces, Programmierschnittstellen) sind Bestandteil einer jeden digitalen oder Cloud-Initiative, die Ihr Unternehmen startet. So entsteht ein wachsendes Ökosystem von APIs, die umsatzfördernde Innovationen ermöglichen. Das Problem ist: Ihre APIs haben sich auch schnell zu einem Hauptvektor für Angriffe entwickelt.

Cyberkriminelle wissen, dass APIs einen schnellen, direkten Pfad zu den sensibelsten Daten eines Unternehmens bieten können. Es gibt viele Schwachstellen: APIs werden oft mit Fehlkonfigurationen, laxen Authentifizierungskontrollen und unbeabsichtigtem Zugriff auf das Internet in die Produktion gebracht. All dies können Angreifer leicht ausnutzen.

Warum werden diese API-Schwachstellen nicht entdeckt und behoben, bevor Anwendungen für Endnutzer veröffentlicht werden? Wir wollen hier die Ursachen dafür untersuchen und Lösungswege aufzeigen.

Vielleicht kennen Sie den alten Spruch „Jedes Unternehmen ist ein Software-Unternehmen“. Heute müsste der Satz eher so lauten: „Jede Geschäftseinheit in Ihrem Unternehmen ist ein unabhängiger Anwendungsentwickler, der unter Zeitdruck Kundenanforderungen erfüllt.“ Das mag als Formulierung weniger griffig sein, entspricht aber oft der Realität.

Zwar gibt es auch noch die herkömmlichen Rollouts aus der zentralisierten IT-Abteilung. Viele Unternehmen erleben jedoch einen Strudel an Innovationen, die Initiativen einzelner Geschäftsbereiche folgen. Diese Innovationen werden von Dringlichkeit und kommerziellen Zielen bestimmt, weniger von gemessenen Prozessen. Die Notwendigkeit, schnell zu handeln und Marktchancen zu nutzen, hat die umfassende Berücksichtigung sicherheitsrelevanter Effekte in den Hintergrund gedrängt. Gelegentlich wird der Ausdruck „Cybersicherheitsschulden“ verwendet, um die Folgen zu beschreiben. Entwickler, die sich nicht in einer zentralisierten IT-Organisation angesiedelt sind (und möglicherweise sogar einem Geschäftsbereich unterstellt sind), können schnell neue Anwendungen, Website-Tools und generative KI-gestützte Dienste aufsetzen und interne Kontrollen umgehen. In vielen Fällen haben Sicherheitsteams keinen Einblick in diese Projekte und können daher die Risiken nicht gründlich bewerten.

Dies ist seit mehreren Jahren die Realität mit Blick auf bekannte Angriffsvektoren. Daher fordern Branchenexperten Unternehmen mit Nachdruck auf, die Verteidigung gegen Ransomware zu verstärken, Passwörter zu schützen und weitere Maßnahmen zu ergreifen. Viele Unternehmen haben den Schutz von APIs jedoch nicht mit der entsprechenden Dringlichkeit behandelt. Das ist problematisch, da APIs in jede Anwendung und jeden Online-Dienst eingebettet sind, die ein Unternehmen erstellt. Die APIs tauschen dann permanent Daten aus, meist ohne einen angemessenen Schutz erhalten.

## Finanzmodell

Budgets haben sich verändert, da sie von zentralisierten IT-Ausgaben auf Betriebsausgaben für Geschäftsbereiche übergegangen sind. Die Budgetprozesse haben sich aber nicht in der Weise entwickelt, wie es dem erhöhten Sicherheitsrisiko entsprechen würde. Geschäftseinheiten verstehen möglicherweise nicht vollständig, wie viel an Mitteln sie für Sicherheitsbelange bereitstellen sollen. Die Folge: Häufig werden gar keine Mittel für den Schutz von Daten zugewiesen.

## Cloudmigration

Anwendungen werden in Public- und Private-Cloud-Umgebungen verschoben. Das Verschieben von Daten und Workloads erhöht die Komplexität, reduziert die Kontrolle und fügt der Umgebung Drittparteien hinzu. Unternehmen benötigen zusätzliche Sicherheitspraktiken, um diese Risikofaktoren abzumildern. Möglicherweise verfügen sie aber nicht über die erforderlichen Fähigkeiten, Erfahrungen oder Ressourcen, um die entsprechenden Mechanismen effektiv zu implementieren.

## Containerisierung

Die Umstellung auf Mikroservices führt zu einer exponentiellen Zunahme der Angriffsfläche. Diese Instanzen können schnell instanziiert und dann zusammenbrechen. Es handelt sich um eine Umgebung, die schwer zu sichern ist. Das liegt an ihrer hohen Dynamik und daran, dass die älteren Tools, auf die viele Unternehmen angewiesen sind, für statischere Umgebungen konzipiert wurden. Dies ist ein weiteres Beispiel dafür, dass APIs allgegenwärtig und sehr risikobehaftet sind. Die heutige, auf Containerisierung und Mikroservices basierende Anwendungsarchitektur ist auf eine Vielzahl von APIs angewiesen, um zu funktionieren. Selbst wenn Unternehmen über API-Bestandslisten verfügen und die genaue Anzahl der APIs in ihren Umgebungen kennen, wissen sie oft nicht, welche APIs vertrauliche Daten zurückgeben.

## Agile Entwicklung

Die Geschwindigkeit, mit der Entwickler neue Anwendungen, Dienste und Funktionen einführen, ist ein bedeutender Risikofaktor. Entwicklungsteams begegnen dem Termindruck mit CI/CD-Methoden (kontinuierliche Integration/kontinuierliche Bereitstellung) und automatisierten Funktionen für Entwicklung, Integration und Tests, die eine effiziente Arbeit ermöglichen.

Doch wer übernimmt das Risikomanagement? Die Umstellung auf DevOps bedeutet häufigere Codeänderungen, die außerhalb der Kontrolle des Sicherheitsteams liegen. Immer mehr Unternehmen wechseln zu einem Shift-Left-Modell für die Entwicklung von Anwendungen insgesamt. Das ist ein Schritt in die richtige Richtung. Dieselbe Philosophie des frühzeitigen und häufigen Testens muss jedoch auch auf die APIs innerhalb der Anwendungen angewendet werden. Hier haben die Unternehmen einen erheblichen Nachholbedarf.

Wo sollten Sie anfangen? Kontinuierliche Bereitstellung erfordert kontinuierliche Sicherheit. Im Folgenden finden Sie fünf Schritte, mit denen Sie in den umfassenden, ständig verfügbaren API-Schutz einsteigen können, während Ihr Unternehmen weiter mit hoher Geschwindigkeit Innovationen vorantreibt.

# Die 5 Schritte zur kontinuierlichen API-Sicherheit

## 1. Entwickeln einer Kultur der kontinuierlichen Sicherheit

Die API-Sicherheit zu verstehen und zu verwalten ist keine einfache Aufgabe. Ihr Führungsteam muss eine Sicherheitskultur für das gesamte Unternehmen fördern, insbesondere jedoch für den Zyklus der Softwareentwicklung. Wenn Sie bei der Entwicklung einer solchen Sicherheitskultur bereits Fortschritte erzielt haben, sollten Sie auf dieser Grundlage im nächsten Schritt die mit APIs verbundenen Schwierigkeiten und operativen Risiken angehen. Dies führt zu erhöhter Transparenz, verbesserter Governance und effektiverer Zusammenarbeit.

Im Folgenden sind einige praktische Maßnahmen aufgeführt, die Ihr Unternehmen ergreifen kann, um eine nachhaltige Sicherheitskultur zu entwickeln:

- **Dezentralisieren Sie das Sicherheitsteam.** Integrieren Sie Experten in Entwicklungsgruppen und Produktlinien, um Transparenz und Governance zu verbessern. Fördern Sie flexiblerer Maßnahmen, die sich auf die Kontextinformationen stützen, die diese eingebetteten Experten bereitstellen.
- **Stellen Sie sicher, dass Sicherheitsteams an allen digitalen Rollouts beteiligt sind**, nicht nur durch die Festlegung von Richtlinien, sondern aktiv ab der Einführung des jeweiligen Dienstes. Verantwortliche für Geschäftsbereiche, ihre Teams und Entwickler sollten über offene Kommunikationskanäle zu Sicherheitspersonal verfügen.
- **Ernennen Sie Sicherheitsbeauftragte.** Identifizieren Sie Unterstützer innerhalb der Geschäftseinheiten, um wichtige Beziehungen für schnelles Arbeiten aufzubauen und aufrechtzuerhalten. Mit festen Sicherheitsbeauftragten können Sie der Sicherheitsbotschaft kontinuierlich Nachdruck verleihen und funktionsübergreifende Teams in die Lage versetzen, vom jeweils anderen die Erfüllung von Verpflichtungen einzufordern.
- **Binden Sie alle ein.** Sicherheitsschulungen sind unerlässlich – nicht nur für Entwickler und Ingenieure. Alle am Prozess der Softwareentwicklung und darüber hinaus Beteiligten sollten Sicherheitsschulungen absolvieren.

## 2. Bewerten der API-Sicherheitslage

Viele Unternehmen unterschätzen die Größe ihrer API-Umgebung. Unternehmen mit Bestandsverzeichnissen könnten eine große API-Untergruppe übersehen haben oder wissen vielleicht auch nicht, welche APIs die größten Risiken darstellen. Durch die Erstellung einer vollständigen und genauen Bestandsliste können Sie die gesamte API-Angriffsfläche bewerten.

Anhand der folgenden Empfehlungen können Sie einen vollständigen Einblick in Ihre API-Sicherheitslage erhalten:

- **Erstellen Sie ein vollständiges Bestandsverzeichnis.** Verschaffen Sie sich ein klares und genaues Bild von den potenziellen Risiken Ihres Unternehmens und ermitteln Sie, wie seine wahre Oberfläche übergreifend für alle APIs und Webanwendungen aussieht. Verwenden Sie ein API-Erkennungstool, das alle APIs lückenlos findet und inventarisiert, einschließlich der folgenden:
  - Shadow-APIs
  - Zombie-APIs
  - Inaktive APIs
- **Identifizieren Sie alle APIs und ihre Risiken.** Machen Sie sich mit den Arten von sensiblen Daten vertraut, mit denen die jeweilige API interagiert. Klären Sie, wie sie geleitet wird, mit welchen physischen Ressourcen sie verknüpft ist und zu welcher Geschäftseinheit oder Anwendung sie gehört.
- **Prüfen Sie die Ressourcenzuweisungen für das Sicherheitsteam.** Analysieren Sie die Anzahl der APIs, die jedes AppSec-Teammitglied verwalten muss. Bestimmen Sie, ob mehr Technik oder mehr Schulungen die Sicherheitslage aufrechterhalten oder verbessern können.

## 3. Problembehebung, Automatisierung und Integration

Unternehmen müssen den Zugriff auf APIs, die API-Verwendung und das Verhalten von APIs verstehen. Die Analyse von APIs ist jedoch eine komplexe Angelegenheit. Das Verständnis der API-Sicherheitslandschaft in all ihrer Komplexität erfordert in der Regel Prozesse wie das Parsen von Protokollen, das Erfassen von Katalogdaten, das Überprüfen von Konfigurationen, das Testen der Sicherheit und das Bewerten von Gerätekonfigurationen. Ohne die richtigen Werkzeuge kann die Problembehebung mühsam sein, entweder weil sie technisch anspruchsvoll ist oder weil sie einen erheblichen Zeit- und Arbeitsaufwand erfordert.
Die Behebung von Mängeln mit dem Ziel, bekannte Schwachstellen zu beseitigen und das unmittelbare Risiko zu mindern, kann jedoch häufig automatisiert oder halbautomatisch erfolgen. Auch danach ist nur wenig oder gar keine menschliche Interaktion erforderlich.

Hier sind einige Hinweise, wie Sie Angriffe verhindern und Fehlkonfigurationen beheben können:

- **Sorgen Sie für eine Integration in bestehende IT-Workflow-Management-Systeme.** Sie müssen sicherstellen, dass identifizierte Probleme umgehend den entsprechenden Teams zugewiesen werden. Integrationen sollten Automatisierungs-Workflows auslösen, die Probleme mit APIs innerhalb des Unternehmens lösen.
- **Stellen Sie stufenweise auf automatisierte Problembehebung um.** Lassen Sie zunächst Menschen neue Abhilfemaßnahmen genehmigen, bevor diese umgesetzt werden. Stellen Sie die Koordination mit den Geschäftseinheiten sicher, um halbautomatische Problembehebungen zu erreichen. Entwicklern zu sagen, dass der Code schlecht ist, reicht nicht aus. Sie benötigen umsetzbare Erkenntnisse, die sie nutzen können. Sonst verschwenden Sie Ihre Zeit und die Zeit der Entwickler. Wenn Probleme bekannt sind und wiederholt auftreten, sollten Sie eine vollständige Automatisierung anwenden, um die Problembehebung zu beschleunigen.
- **Erkennen Sie schädliches Verhalten.** Verwenden Sie historische Erkenntnisse zu Taktiken der API-Ausnutzung, um ungewöhnliches Verhalten zu ermitteln, das einen beabsichtigten Angriff verraten könnte. Nutzen Sie automatisierte oder halbautomatische Reaktionen, um Angriffe abzuwehren.
- **Sorgen Sie für eine Integration in bestehende SIEM-Systeme (Security Information and Event Management).** Diese Integration stellt sicher, dass das ganze Team API-Sicherheitsdaten verwenden kann.

## 4. Shift-Left-Ansatz für API-Sicherheit

Bei der API-Entwicklung sind Tests wichtig. Es geht aber auch darum, *wann* Sie Ihre APIs testen. Im traditionellen Modell finden die Tests relativ kurz vor der Bereitstellungsphase statt. Diese Tests sind zwar wichtig, aber unzureichend, sodass schwerwiegende Sicherheitslücken entstehen können. „Shift Left" ist ein Ansatz, bei dem verschiedene Aufgaben in eine frühere Phase des Entwicklungsprozesses verschoben werden. Beim Shift-Left-Ansatz sind Sicherheit und Tests ein integraler Bestandteil jeder Phase der API-Entwicklung. Damit ist sichergestellt, dass Entwickler während des gesamten Lebenszyklus der API Schwachstellen entdecken können. Auf diese Weise können Unternehmen Innovationen beschleunigen und ihren Wettbewerbsvorteil stärken – mit API-Sicherheit als Grundlage.

Hier sind einige Vorschläge, die Ihnen bei der Einführung von Shift-Left-API-Tests helfen werden:

- **Definieren Sie Ziele.** Da „Shift Left" organisatorische und kulturelle Veränderungen erfordert, sollte das Führungsteam als Erstes Ziele für den Prozess definieren. Schließlich muss gewährleistet sein, dass alle neuen Tools oder Prozesse, die in den Entwicklungszyklus eingeführt werden, für die bestehenden Entwicklungs- und Testmethoden des Teams funktionieren.
- **Analysieren Sie die Lieferkette.** Sie müssen wissen, wie und wo Ihr Unternehmen Apps und Software entwickelt, bevor Sie ein umfassendes Shift-Left-Sicherheitsprogramm konzipieren. Das Risikopotenzial der Lieferkette in puncto Sicherheit hängt weitgehend von der Sicherheitskompetenz anderer Akteure in der Kette ab. Anhand einer entsprechenden Analyse können Entwickler auch leichter ermitteln, an welchen früheren Punkten im Lebenszyklus Tests durchgeführt werden könnten.
- **Automatisieren Sie Sicherheitsprozesse.** Wenn Entwicklungsteams Mikroservices einführen, muss sichergestellt sein, dass Ihre integrierten Sicherheitsexperten von Anfang an API-Sicherheitstools verwenden. Dies dient der Überwachung auf Risiken, die mit der Containerisierung einhergehen.
- **Verwenden Sie konsistente Werkzeuge.** Bitten Sie Sicherheitsteams, die primäre Schnittstelle des Entwicklungsteams zu übernehmen und sich an die von den Entwicklern bevorzugten Tools, Umgebungen und ihre Sprache anzupassen. Beispielsweise können Schwachstellen und Erkenntnisse in dieselben Produkt-Backlogs für neue funktionale Anwendungsanforderungen eingetragen werden, die auch für normale Nutzerberichte verwendet werden.
- **Machen Sie das AppSec-Team zu einer Quelle der Innovation.** Nutzen Sie durchgängige Bereitstellungsprinzipien, um sicherheitsspezifische Mikroservices zu entwickeln, die Risiken minimieren und Ihrem Unternehmen Handlungsoptionen bieten, die andere nicht haben.

## 5. Kontinuierliche Tests

Wie wir gerade festgestellt haben, verschiebt ein Shift-Left-Sicherheitsansatz Tests auf der Zeitachse nach links, sodass das Team Tests früher im Lebenszyklus durchführt. Im Gegensatz dazu werden bei einem Shift-Right-Ansatz Tests mit realen Nutzern und Szenarien durchgeführt, was in der Entwicklungsumgebung nicht möglich ist. Shift-Right-Tests in Produktionsumgebungen gewährleisten Softwarestabilität und -Performance unter realen Bedingungen. Sie verbessern auch das Nutzererlebnis, da sie Feedback und Bewertungen von Anwendungsnutzern erfassen. Die Wahrheit ist: Keiner der Ansätze ist besser als der andere. Um potenzielle Risiken zu minimieren, muss ein Unternehmen kontinuierlich testen.

Ihr Unternehmen kann die folgenden Tipps nutzen, um eine nachhaltige Sicherheitskultur zu entwickeln:

- **Führen Sie aktiv API-Tests durch.** Im Rahmen des API-Softwareentwicklungszyklus sollten API-Sicherheitstests eingesetzt werden, um potenzielle Probleme vor und nach der Produktion zu beheben. Überprüfen Sie die Integrität jeder API vor und nach ihrer Bereitstellung.
- **Überwachen Sie den API-Traffic kontinuierlich.** Verfolgen Sie die API-Nutzung und analysieren Sie Metadaten des API-Traffics. Die Traffic-Analyse in Echtzeit identifiziert neue APIs und Änderungen an vorhandenen APIs. Der Analyseprozess muss automatisiert, wiederholbar und umsetzbar sein.
- **Erkennen Sie Schwachstellen und Fehlkonfigurationen.** Die Tests müssen kontinuierlich durchgeführt werden, parallel zur Entwicklung laufen und eine fortlaufende Kommunikation zwischen den Kunden, Entwicklern und Testern beinhalten. Sie müssen Probleme erkennen, damit diese behoben werden können, bevor jemand sie ausnutzt. Verzögerungen bei der Analyse verschaffen Hackern zusätzliche Zeit, um die Schwachstellen auszunutzen. Wichtig ist auch die Berichterstattung über Änderungen an Richtlinien oder Funktionen und Aktualisierung von SIEM-Systemen.
- **Protokollieren Sie den API-Traffic.** Für den Fall, dass Sie forensische Berichte für bestimmte API-Schlüssel, Token, IP-Adressen und Nutzeridentitäten erstellen müssen, sollten Sie den API-Traffic protokollieren.

# Zusammenfassung

API-Sicherheitsbedrohungen stellen für viele Unternehmen eine reale und akute Gefahr dar. APIs werden häufig nicht verwaltet. So rutschen sie durch das Radar konventioneller Tools und existieren auf Dauer mit Fehlkonfigurationen, mangelnder Authentifizierung und Codierungsfehlern. Infolgedessen sind nicht verwaltete APIs ein vorrangiges Ziel für Angreifer und können kompromittiert werden, ohne dass das Unternehmen es merkt.

Die Lösung für das Problem ist kontinuierliche Sicherheit. Sie ist die ganze Zeit über in die Entwicklerprozesse und in die APIs selbst integriert, während die APIs erstellt und in die Produktion verschoben werden. Unternehmen sollten vier Best Practices beachten:

1. Entwickeln Sie eine neue Kultur, um AppSec-Experten in das Engineering-Team Ihres Unternehmens einzubinden.
2. Entdecken Sie den vollständigen API-Bestand, um das Risikoprofil Ihres Unternehmens in Bezug auf API-Sicherheit in den Griff zu bekommen.
3. Priorisieren Sie Problembehebungen, automatisieren Sie nach Möglichkeit Korrekturen und integrieren Sie die API-Sicherheit nahtlos in aktuelle Systeme für die Anwendungssicherheit.
4. Durchgängige Wachsamkeit und API-Tests gewährleisten, dass neue Sicherheitsrisiken schnell erkannt und minimiert werden.

Obwohl dieser Ansatz eine neue Denkweise, andere Prozesse und eine teamübergreifende Zusammenarbeit erfordert, lassen sich die Herausforderungen bewältigen.

**Erfahren Sie mehr über** API-Angriffsmethoden, häufige API-Schwachstellen und darüber, wie Sie Ihr Unternehmen schützen können**.**

**Erfahren Sie, wie wir Sie unterstützen können, und vereinbaren Sie eine individuelle** Demo zu Akamai API Security**.**

Akamai

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: Oktober 2024.