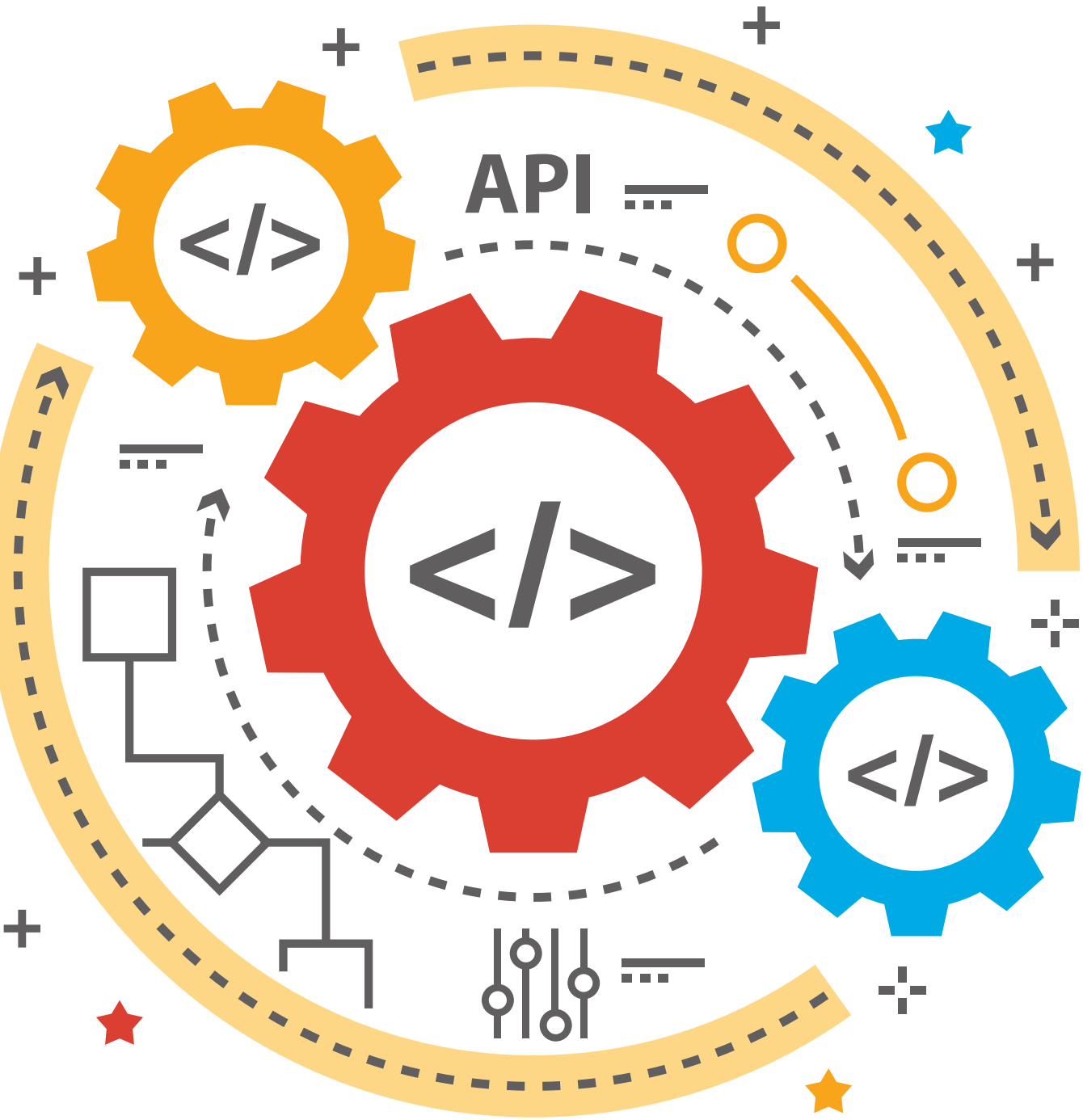
STUDIE

API SECURITY 2024



fastly

Simon Hülsbömer,
Senior Research Manager

Das sichere Bindeglied

Bei aller Konzentration auf die Sicherheit von Anwendungen und Services in einer vernetzten Welt wird oft eine entscheidende Stelle vergessen: die Schnittstelle. (Cloud-)Anwendungen und Services kommunizieren sowohl nebeneinander als auch miteinander über diese APIs, die schnell zu großen Sicherheitsrisiken werden, wenn die durchgängige Absicherung fehlt. Und je komplexer die IT-Prozesse werden, desto sensibler werden auch die Schnittstellen.

Mit dem zunehmenden Einsatz von Cloud Computing, Microservices-Architekturen und mobilen Anwendungen gewinnen APIs als Bindeglied zwischen verschiedenen Systemen, Diensten und Plattformen immer weiter an Bedeutung. Dabei öffnen sie gleichzeitig potenzielle Angriffsvektoren für böswillige Akteure. Ein Verstoß gegen die Sicherheit einer API kann verheerende Folgen haben, von Datenlecks und finanziellen Verlusten bis hin zu Rufschäden und rechtlichen Konsequenzen.

Gemeinsam mit Cloud-Provider Fastly hat das Custom Research Team von CSO, CIO und COMPUTERWOCHE europaweit 235 Unternehmen zum Stand ihrer API-Sicherheit befragt. An der Studie teilgenommen haben C-Level-Entscheider (CISOs, CIOs, VP Security, IT-Security-Leiter), IT-Verantwortliche aus Plattform- oder DevSecOps-Teams sowie weitere Sicherheitsexperten, -analysten, -architekten und -Influencer.

Wie relevant das Thema ist, zeigen die Zahlen aus der vorliegenden Studie: 95 Prozent der Befragten geben an, in den vergangenen zwölf Monaten Probleme mit ihrer API-Sicherheit gehabt zu haben. 39 Prozent berichten von API-Schwachstellen, 33 Prozent von Authentifizierungsproblemen innerhalb der APIs. Dennoch haben 84 Prozent bislang keine speziellen Maßnahmen für die Verbesserung der Schnittstellensicherheit getroffen – das liegt vor allem an finanziellen Engpässen und einem Mangel an Know-how.

Eine weitere spannende Erkenntnis: API Security und Web Security verschmelzen miteinander – so setzen fast 90 Prozent der Unternehmen bereits entsprechend kombinierte Security-Lösungen eines Anbieter sein oder planen es zumindest. Das ergibt auch Sinn: API Security und Web Security adressieren vergleichbare, teils identische Angriffsvektoren wie Injection-Angriffe oder Cross-Site Request Forgery. Darüber hinaus werden APIs oft in Webanwendungen verwendet, um Daten von verschiedenen Quellen abzurufen oder Aktionen auszuführen. Eine unsichere API kann daher die Sicherheit der gesamten Webanwendung beeinträchtigen. Umgekehrt können Sicherheitslücken in einer Webanwendung die Sicherheit der APIs, die sie verwendet, gefährden.

Insgesamt arbeiten API-Security und Web-Security Hand in Hand, um die Sicherheit von Anwendungen und Diensten zu gewährleisten. Indem Unternehmen ganzheitliche Sicherheitsstrategien entwickeln, die sowohl APIs als auch Webanwendungen abdecken, können sie potenzielle Sicherheitsrisiken minimieren und eine sichere digitale Umgebung schaffen.

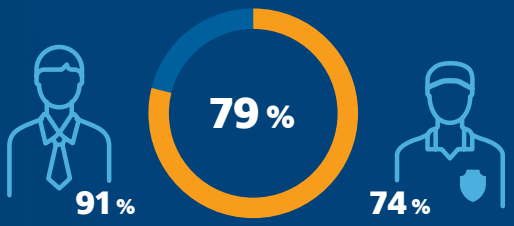
Ihnen eine erkenntnisreiche Lektüre.

Inhalt

API Security 2024

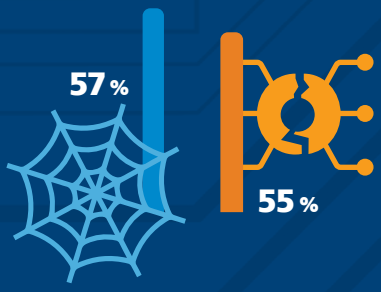
Management Summary

Die wichtigsten Ergebnisse unserer Studie



Sichere APIs sind für die Führungsebene wichtiger als für Sicherheitsexperten

79 % der befragten Unternehmen schreiben API-Sicherheit eine hohe oder sehr hohe Bedeutung zu. **91 %** der C-Level-Führungskräfte und Compliance-Experten sehen das ebenso, während nur **74 %** der Sicherheitsexperten dieser Ansicht sind.



Was API-Risiken angeht, ist Alter ein größerer Anlass für Besorgnis als Manipulation

57 % der Befragten machen sich mehr Gedanken um die Folgen veralteter APIs. An zweiter Stelle steht mit **55 %** der mögliche Integritätsverlust durch APIs. C-Level-Führungskräfte und Compliance-Experten halten veraltete APIs für das größte Risiko, während Sicherheitsexperten eher wegen API-Manipulationen besorgt sind.

API- und Web-Sicherheit werden ein und dasselbe

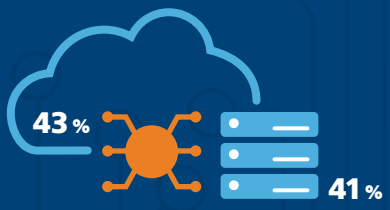
19 % der befragten Unternehmen nutzen bereits eine konsolidierte Lösung für Webanwendungen und API-Sicherheit von einem einzigen Anbieter. **43 %** planen die Einführung innerhalb der nächsten zwei Jahre und weitere **26 %** planen dies, haben aber keinen Zeitrahmen. Nur **2 %** der Unternehmen gaben an, dass sie an einem solchen Ansatz nicht interessiert seien.

Echtzeitprotokollierung und API-Überwachung haben weiterhin Priorität

55 % der befragten Unternehmen betrachten API-Überwachung und -Protokollierung als oberste Priorität für API-Sicherheit. **43 %** gaben API-Analyse und -Evaluierung als ihre Priorität an. Die Verwendung von KI-Technologien wurde nur von **14 %** der Unternehmen als Priorität betrachtet.

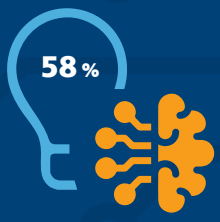
Probleme mit der API-Sicherheit stehen sehr wohl auf der Agenda, aber die meisten Unternehmen schneiden bei der API-Sicherheit zugegebenermaßen ziemlich mittelmäßig ab

95 % der befragten Unternehmen gaben an, dass sie in den vergangenen zwölf Monaten Probleme mit der API-Sicherheit hatten. Von diesen berichten **39 %** über Schwachstellen in ihren APIs und **33 %** über Authentifizierungsprobleme. **84 %** der Unternehmen haben noch keine fortschrittlichen API-Sicherheitsmaßnahmen implementiert. Ein unzureichendes Budget und mangelndes Fachwissen sind die am häufigsten genannten Gründe für die Nichtumsetzung einer umfassenden API-Strategie.



Speziell auf Edge-native und Cloud-native Anwendungen ausgerichtete API-Sicherheit liegt zunehmend im Trend

In Bezug auf die wichtigsten Kriterien für die Auswahl einer API-Sicherheitslösung gaben **43 %** der befragten Unternehmen an, dass sie eine API-Sicherheitslösung für Edge-native Anwendungen bevorzugen, gefolgt von **41 %** der Befragten, die sich für eine Cloud-native Lösung zum Schutz ihrer APIs entscheiden würden.

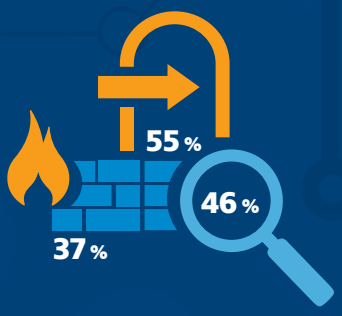


Die Erwartungen an KI sind hoch, aber das Wissen ist gering, da wir derzeit nur einen minimalen Einsatz in der API-Sicherheit sehen

58 % der Befragten glauben, dass der Einsatz von KI in den nächsten zwei bis drei Jahren zu erheblichen Veränderungen bei der API-Sicherheit führen wird. Bei Finanzinstituten und Versicherern steigt diese Zahl auf **75 %**. **16 %** der befragten Unternehmen wissen nicht, ob sie bereits KI für ihre API-Sicherheit einsetzen. Nur **18 %** gaben an, dass sie KI einsetzen, während **66 %** sagten, dass sie es nicht tun.

API-Gateways, Protokolldaten und WAF gehören zu den zuverlässigsten Methoden zur Erkennung von API-Angriffen

55 % der Befragten vertrauen auf Warnungen von einem API-Gateway, um API-Angriffe zu erkennen. **46 %** durchsuchen Protokolldaten auf der Suche nach Hinweisen für mögliche API-Angriffe. **37 %** nutzen Warnmeldungen von einer WAF (Web Application Firewall).



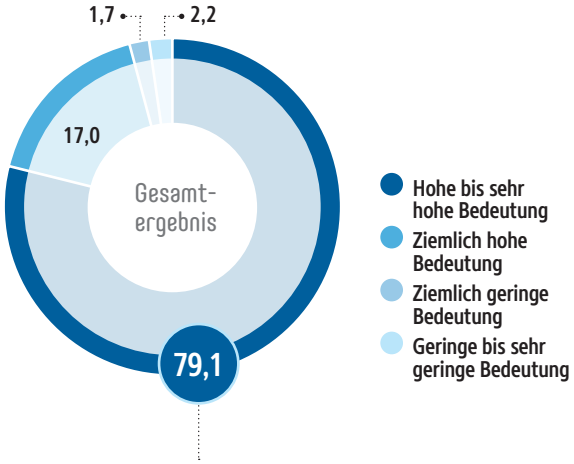
API-Sicherheit hat eine große Bedeutung und wirkt sich auf das Rollout von Anwendungen aus

79 Prozent der befragten Unternehmen schreiben API-Sicherheit eine hohe oder sehr hohe Bedeutung zu. Für nur zwei Prozent der Befragten hat sie eine geringe oder sehr geringe Bedeutung. Ebenso verzögerten 79 Prozent der Befragten die Einführung oder Integration einer neuen Anwendung in die Produktion aufgrund von API-Sicherheitsbedenken.

Die hohe Bedeutung, die der API-Sicherheit beigemessen wird, wird sowohl von C-Level-Führungskräften und Compliance-Verantwortlichen als auch von IT- und Netzwerkmanagern sowie Sicherheitsexperten der befragten Unternehmen geteilt. Während jedoch der Anteil der Befragten auf C-Level- und Compliance-Ebene mit dieser Überzeugung 91 Prozent betrug, waren es bei den Sicherheitsexperten nur 74 Prozent.

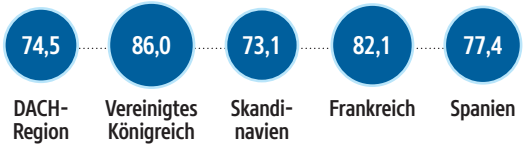
Welche Bedeutung hat API-Sicherheit aktuell in Ihrem Unternehmen?

Angaben in Prozent. Basis: n = 235



Ergebnis-Split nach Funktion im Unternehmen

Ergebnis-Split nach Region



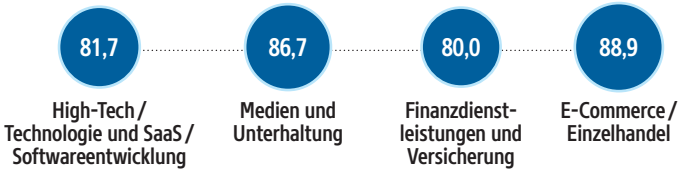
Die Bedeutung der API-Sicherheit ist nicht nur eine Idee in den Köpfen der C-Level-Führungskräfte und der Compliance-Verantwortlichen. Die Mehrheit der Befragten, die sich bezüglich der API-Sicherheit unsicher waren, hat bereits Verzögerungen bei der Inbetriebnahme neuer Anwendungen erlebt.

Vergleicht man die verschiedenen Regionen, in denen die Befragung stattfand, so zeigt sich, dass API-Sicherheit für die Befragten im Vereinigten Königreich besonders wichtig ist: 86 Prozent der Befragten antworteten entsprechend. In Skandinavien messen 73 Prozent der Befragten sicheren APIs die gleiche Bedeutung bei.

Wir haben darüber hinaus nach Branchen unterschieden: 89 Prozent der befragten Groß-, Einzelhandels- und E-Commerce-Unternehmen schreiben API-Sicherheit eine hohe oder sehr hohe Bedeutung zu. Im Vergleich dazu gaben 80 Prozent der Umfrageteilnehmer aus dem Finanz- und Versicherungssektor die gleiche Antwort. Dieses Ergebnis ist überraschend, da Finanzdienstleistungen und Versicherungen streng reguliert sind und man daher erwarten würde, dass sie einen überdurchschnittlichen Fokus auf API-Sicherheit haben.

Schlussfolgerung: Auch wenn der API-Sicherheit eine hohe Bedeutung beigemessen wird, muss die tatsächliche Umsetzung in den einzelnen Unternehmen genauer betrachtet werden, da die Verantwortlichen für diese Umsetzung ein etwas anderes Bild vermitteln können.

Ergebnis-Split nach Branche



DACH-Region = Deutschland, Österreich, Schweiz
Skandinavien = Dänemark, Finnland, Norwegen, Schweden

Sicherheitsprobleme bei Produktions-APIs sind weit verbreitet

92 Prozent der befragten Unternehmen haben in den letzten zwölf Monaten Sicherheitsprobleme mit den APIs in ihren Produktionssystemen entdeckt, fünf Prozent nicht, und drei Prozent wissen es nicht genau. Die meisten API-Sicherheitsprobleme werden auf Schwachstellen zurückgeführt, wie 39 Prozent der Befragten angaben.

Weitere Sicherheitsprobleme, die Unternehmen in ihren Produktions-APIs festgestellt haben, sind Authentifizierungsprobleme, wie eins von drei Unternehmen angab, API-Identitätsprobleme, die drei von zehn Unternehmen entdeckten, und Konfigurationsfehler, wie von 30 Prozent der Befragten berichtet.

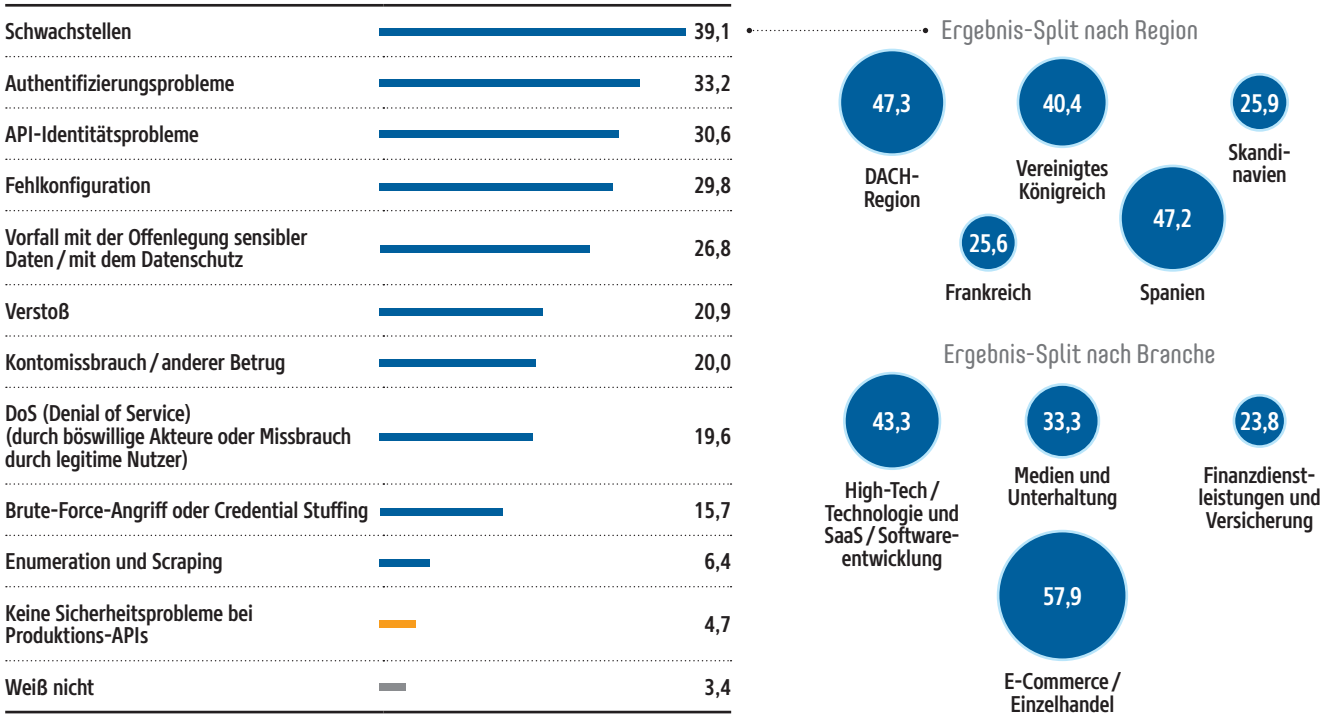
Die Häufigkeit, mit der Schwachstellen in APIs für Produktionssysteme entdeckt werden, ist je nach Region unterschiedlich. Unternehmen in der DACH-Region und in Spanien melden mit 47 Prozent die meisten. Im Vereinigten Königreich liegt diese Zahl immer noch bei 40 Prozent, während in Frankreich und Skandinavien nur 26 Prozent der Befragten API-Schwachstellen melden.

Aufgeschlüsselt nach den verschiedenen Branchen ist es der Groß- und Einzelhandels-/E-Commerce-Sektor, der am häufigsten Schwachstellen in seinen Produktions-APIs findet. 58 Prozent der Befragten gaben dies an. Bei den Finanzdiensleistern und Versicherern sinkt diese Zahl auf 24 Prozent. In diesem Bereich sind es vor allem Authentifizierungsprobleme mit APIs, wie 38 Prozent der Befragten angaben.

Schlussfolgerung: API-Sicherheit ist für IT-Systeme in Produktion von zentraler Bedeutung und muss Teil des Gesamtsicherheitskonzepts sein oder in dieses integriert werden.

Welche Sicherheitsprobleme haben Sie in den vergangenen zwölf Monaten in Ihren Produktions-API festgestellt?

Mehrfachnennungen möglich. Angaben in Prozent. Basis: n = 235



DACH-Region = Deutschland, Österreich, Schweiz
Skandinavien = Dänemark, Finnland, Norwegen, Schweden

3

Veraltete APIs sind die am häufigsten genannte Bedrohung für Webschnittstellen

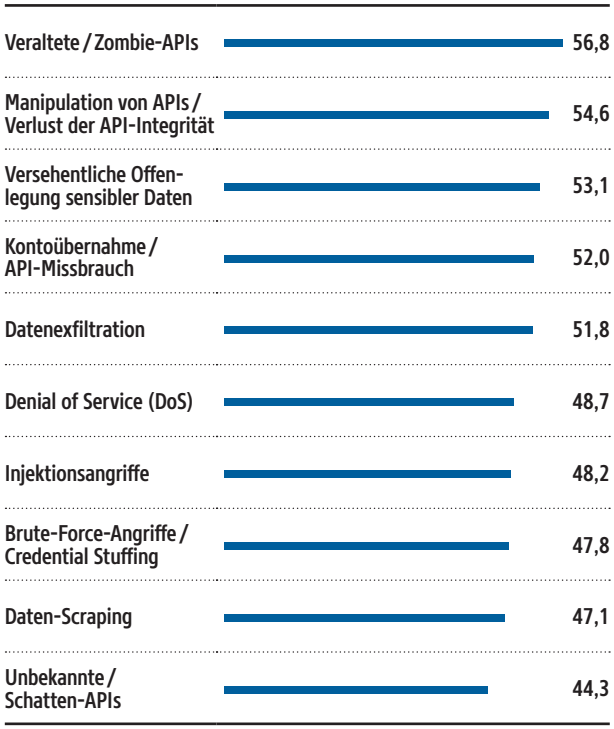
57 Prozent der Antworten erwähnten Zombie-APIs (veraltete APIs), womit dies die von den befragten Unternehmen am häufigsten genannte Bedrohung war. An zweiter Stelle folgt die Manipulation von APIs mit 55 Prozent, an dritter Stelle die versehentliche Weitergabe sensibler Daten über APIs mit 53 Prozent.

Die Wahrnehmung der Bedrohung durch veraltete APIs ist unter den C-Level-Führungskräften und Compliance-Experten mit 74 Prozent überdurchschnittlich hoch. Nur 47 Prozent der Sicherheitsexperten nannten dieses API-Risiko. Selbst die von Sicherheitsexperten am häufigsten genannte Bedrohung, API-Manipulation, wird häufiger im C-Level- und Compliance-Bereich genannt. 55 Prozent der Sicherheitsexperten halten API-Manipulationen für eine Bedrohung, bei den C-Level-Führungskräften und Compliance-Verantwortlichen sind es 65 Prozent.

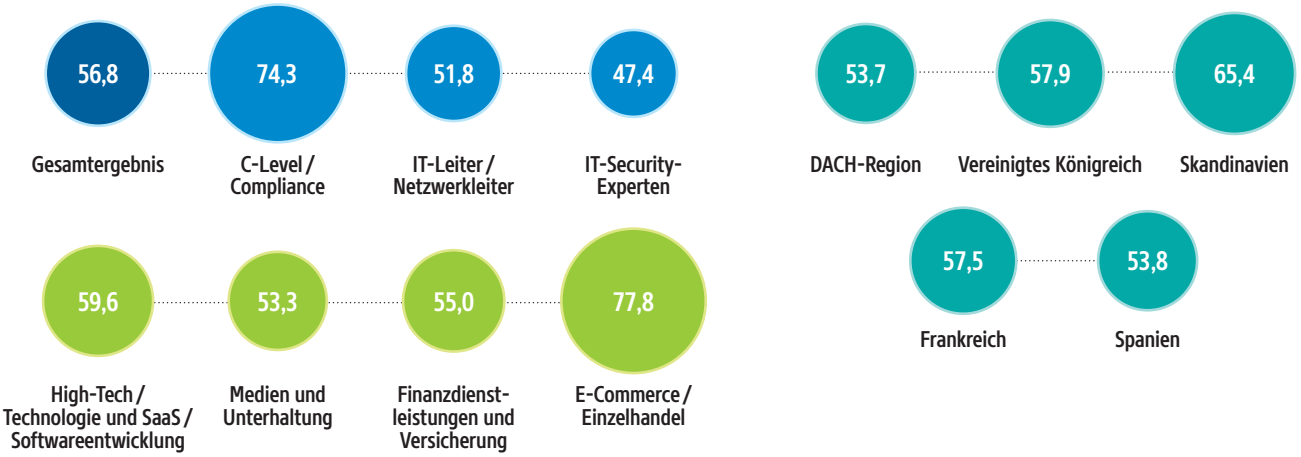
Die Unterschiede bei der Bewertung von API-Risiken sind nicht nur auf die Rolle des Befragten im Unternehmen zurückzuführen. Während die Umfrageteilnehmer im Vereinigten Königreich und in Skandinavien am häufigsten Zombie-APIs angaben, ist API-Manipulation in der DACH-Region ein häufigeres Problem. In Spanien ist die versehentliche Offenlegung sensibler Daten die häufigste Antwort, während es in Frankreich API-Missbrauch und Datenexfiltration sind.

Wie beurteilen Sie die Bedrohungslage im Bereich der API-Sicherheit in Ihrem Unternehmen?

Mehrfachnennungen möglich. Angaben in Prozent. Bewertung auf einer Skala von 1 (sehr große Bedenken) bis 6 (sehr geringe Bedenken). Top 2 Antwortmöglichkeiten (große bis sehr große Bedenken). Basis: n = 235

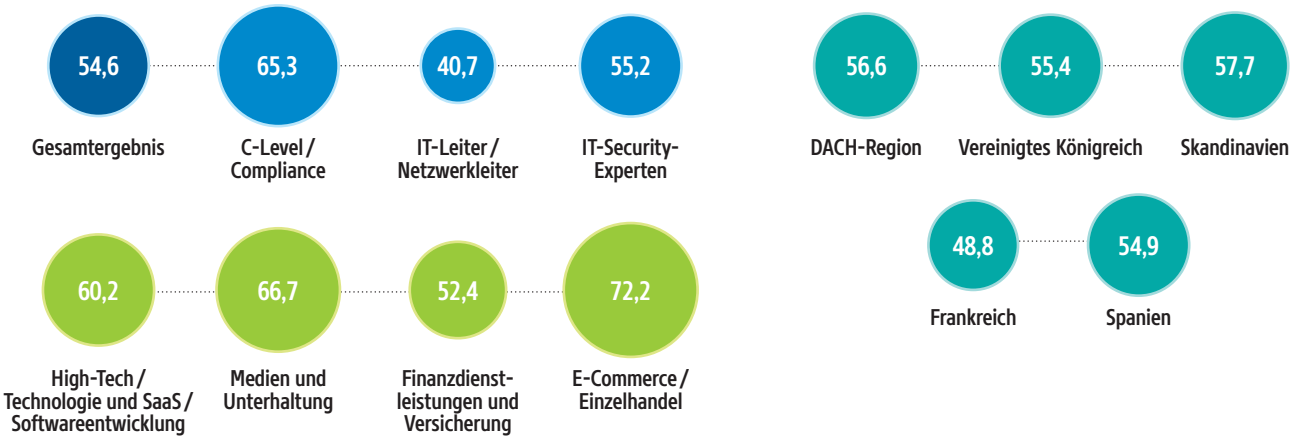


Ergebnis-Split: Veraltete/Zombie-APIs

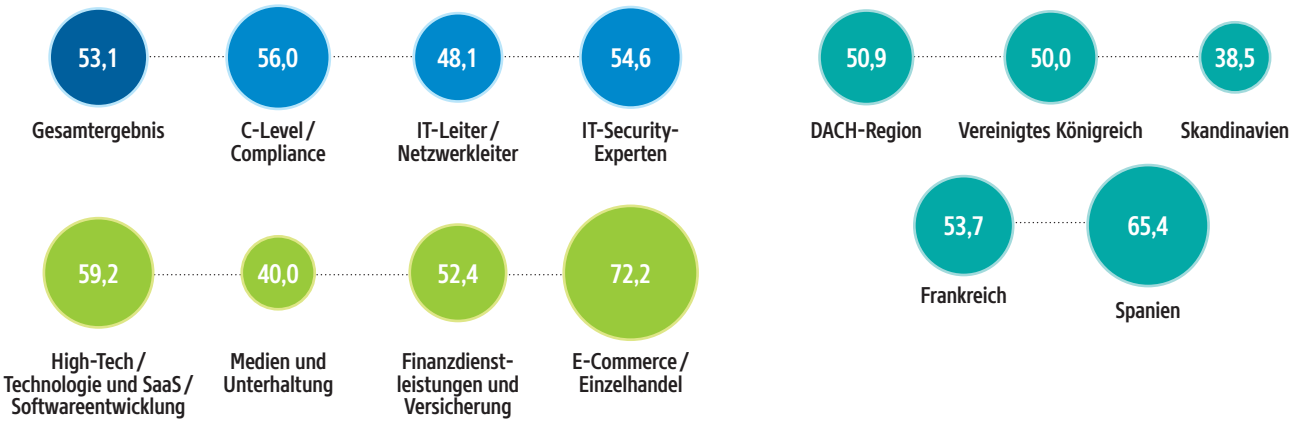


DACH-Region = Deutschland, Österreich, Schweiz
Skandinavien = Dänemark, Finnland, Norwegen, Schweden

Ergebnis-Split: Manipulation von APIs / Verlust der API-Integrität



Ergebnis-Split: Versehentliche Offenlegung sensibler Daten



Auch die Branche, in der ein Unternehmen tätig ist, hat Einfluss darauf, wie API-Bedrohungen bewertet werden: Die am häufigsten genannte Bedrohung, Zombie-APIs, bereitet dem Einzelhandel größere Sorgen, während Medien, Unterhaltung, High-Tech/Technologie und SaaS/Softwareentwicklung eher über API-Manipulation besorgt sind. Für Finanzdienstleister und Versicherer ist jedoch der API-Missbrauch die am häufigsten genannte Bedrohung.

Schlussfolgerung: Unternehmen sollten die Art und Weise, wie sie API-Risiken bewerten, überdenken. Dabei sollten Fachleute aus verschiedenen Disziplinen zusammenarbeiten, nicht nur allein Sicherheitsexperten. Außerdem ist es wichtig, eine genaue Liste der APIs zu haben, damit Zombie-APIs strengeren Beschränkungen unterworfen werden können, bis sie aktualisiert werden.

4

Erweiterte Maßnahmen für API-Sicherheit sind noch immer die Ausnahme und nicht die Regel

Jedes dritte der befragten Unternehmen schätzt die Maßnahmen, die es zur Gewährleistung der API-Sicherheit ergriffen hat, als eher durchschnittlich ein. 26 Prozent geben an, dass ihre API-Sicherheit nur grundlegend ist, und weitere 21 Prozent sind noch in der Planungsphase. Drei Prozent gaben an, dass sie über keinerlei API-Sicherheit verfügen.

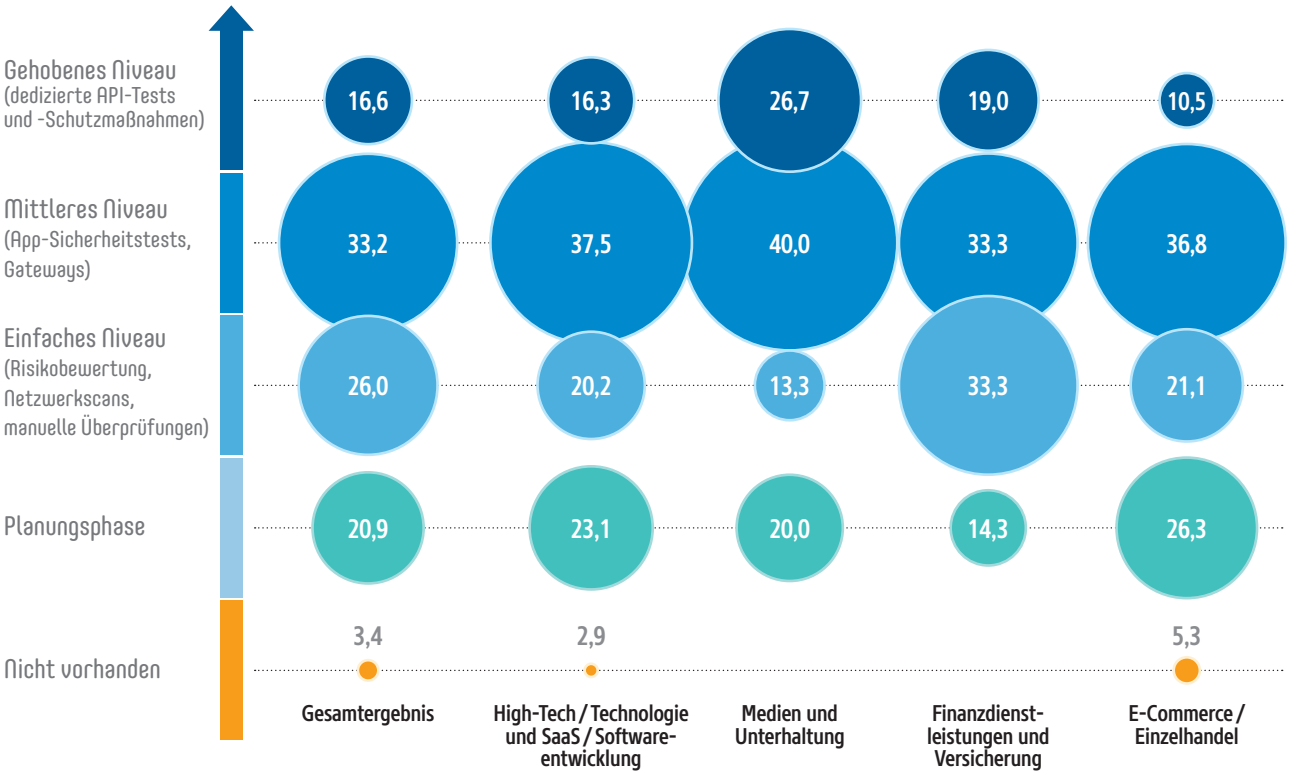
17 Prozent der Befragten gaben an, dass ihre API-Sicherheitsmaßnahmen fortschrittlich sind. Wenn wir jedoch einen Blick auf die Rolle dieser Befragten werfen, sehen wir, dass 20 Prozent der C-Level-Führungskräfte und Compliance-Verantwortlichen glauben, dass ihre eigenen API-Sicherheitsmaßnahmen sehr fortschrittlich sind. Nur 14 Prozent der Sicherheitsexperten kommen zu demselben Schluss.

Im Vergleich der Regionen geben mehr Teilnehmer aus dem Vereinigten Königreich (21 Prozent) an, dass ihre API-Sicherheit fortschrittlich ist. Nur 13 Prozent der Teilnehmer aus der DACH-Region teilen diese Ansicht. Im Branchenvergleich sehen sich vor allem 27 Prozent der Vertreter der Medien- und Unterhaltungsbranche mit einer sehr fortschrittlichen API-Sicherheit ausgestattet. Im Einzelhandelssektor sieht das etwas anders aus. Hier geben nur elf Prozent an, dass sie fortschrittliche API-Sicherheitsmaßnahmen verwenden.

Von diesen geben nur vier Prozent an, dass ein Mangel an geeigneten Tools und Lösungen der Grund dafür ist, dass ihre API-Sicherheitsstrategie nicht optimal umgesetzt werden kann.

Welcher Status hinsichtlich der API-Sicherheit gilt für Ihr Unternehmen?

Angaben in Prozent. Basis: n = 235



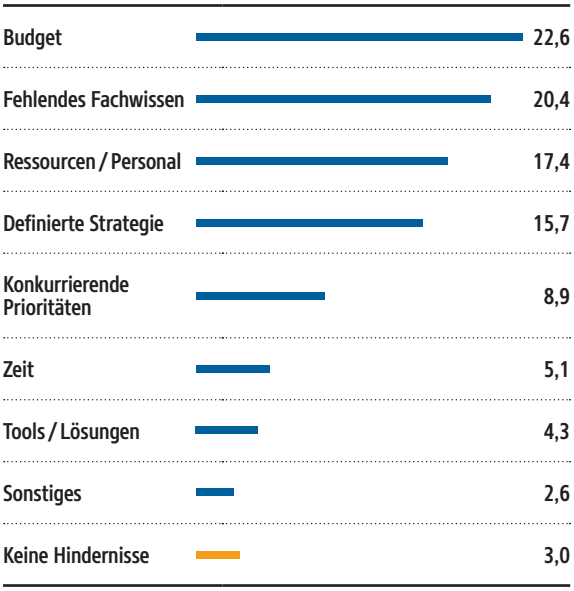
23 Prozent der Befragten geben jedoch an, dass dies auf ein unzureichendes Budget zurückzuführen ist, und weiteren 20 Prozent fehlt es an Fachwissen. Die größte Sorge ist laut 31 Prozent der Antworten, dass nicht genug Zeit auf die Ausarbeitung und Dokumentation von API-Sicherheitsanforderungen verwendet wird.

Auf die Frage nach den wichtigsten Auswahlkriterien bei der Bewertung von API-Sicherheitslösungen gaben die Unternehmen am häufigsten Edge-native Plattform (bei der die Daten lokal auf Edge-Geräten verarbeitet und nur bei Bedarf an die Cloud oder eine zentrale Datenbank gesendet werden) an und dass die API-Sicherheitslösung speziell für die Cloud-native Sicherheit unter Verwendung der neuesten Technologie entwickelt wurde. Hier herrscht relative Einigkeit: Dies sind die häufigsten Nennungen über alle Unternehmensgrößen, Branchen und (fast) alle analysierten EMEA-Regionen hinweg.

Schlussfolgerung: Angesichts der vielen API-Vorfälle in Unternehmen und der Bedeutung, die der API-Sicherheit beigemessen wird, müssen viele Unternehmen die Sicherheitsmaßnahmen noch ernster nehmen als bisher.

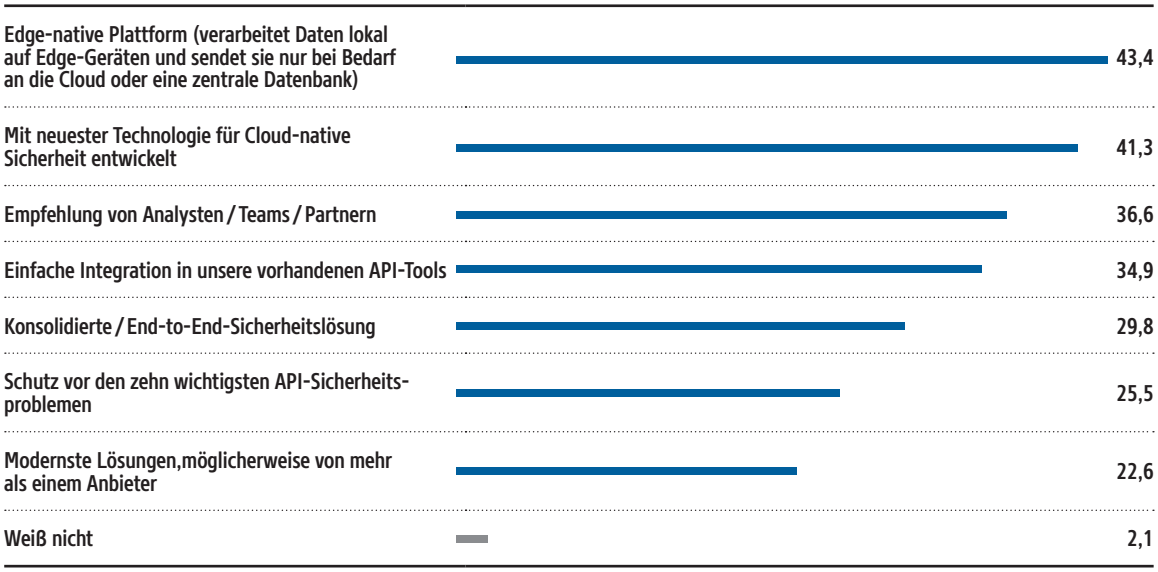
Was ist das größte Hindernis, das Ihr Unternehmen von der Umsetzung einer optimalen API-Sicherheitsstrategie abhält?

Angaben in Prozent. Basis: n = 235



Was sind die wichtigsten Kriterien für Ihr Unternehmen bei der Bewertung von API-Sicherheitslösungen?

Mehrfachnennungen möglich. Angaben in Prozent. Basis: n = 235



5

Insbesondere Finanzdienstleister haben Probleme bei der Erkennung von API-Angriffen

Nur acht Prozent der befragten Unternehmen gaben an, dass sie nicht in der Lage sind, API-Angriffe zu erkennen. Bei Finanzdienstleistern und Versicherern ist das Bild ein anderes: Fast drei von zehn Befragten (29 Prozent) gaben an, dass sie nicht in der Lage sind, Angriffe auf ihre APIs zu erkennen. Von denjenigen, die API-Angriffe entdeckt haben, nutzen 55 Prozent Warnungen, die von einem API-Gateway ausgegeben werden.

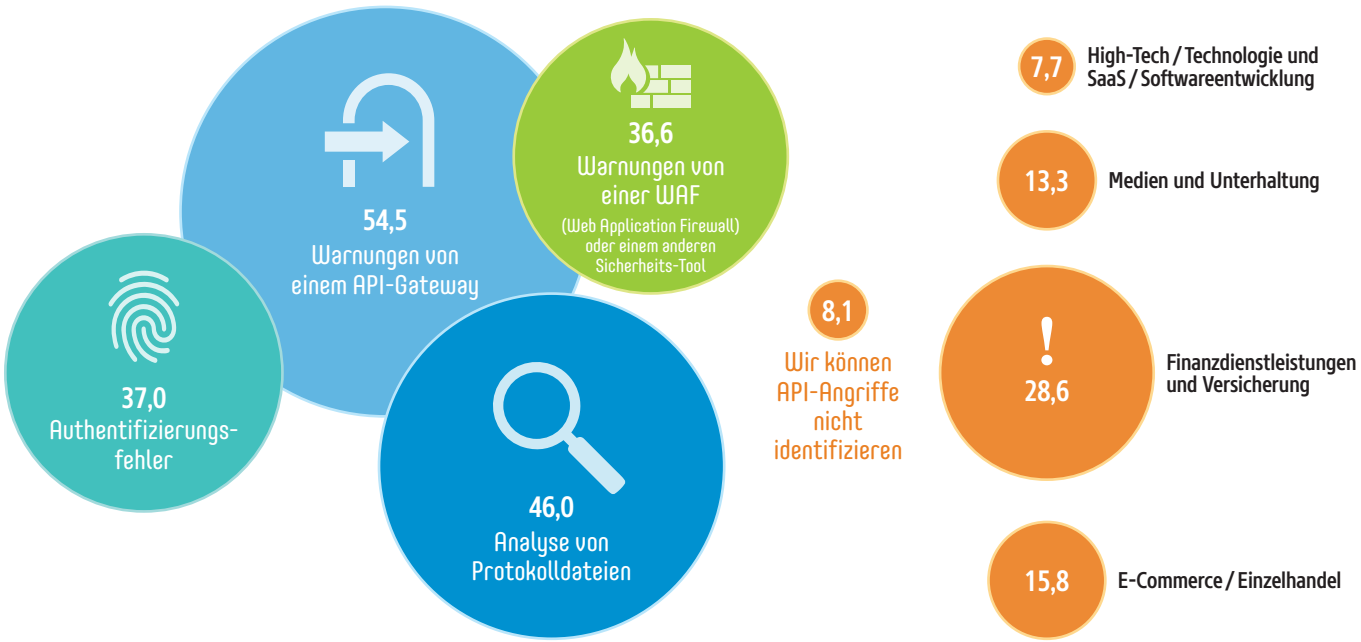
Weitere 46 Prozent nutzen Protokolldaten, um Hinweise auf API-Angriffe zu finden, und 37 Prozent verlassen sich auf Authentifizierungsfehlermeldungen oder Warnungen von einer WAF (Web Application Firewall).

Die Durchsetzung des API-Schemas stellt sicher, dass eingehende HTTP-API-Aufrufe einer bestimmten Struktur oder einem Satz von Regeln folgen, die in einer Spezifikationsdatei festgelegt sind. Die OpenAPI-Spezifikationssprache, die früher als Swagger-Dateien bekannt war, ist eine herstellerneutrale Spezifikationssprache für HTTP-APIs, die Entwicklern eine standardisierte Möglichkeit zur Beschreibung einer API bietet. Sie kann äußerst hilfreich sein, um böswillige Personen zu finden und zu stoppen, die versuchen, eine API zu missbrauchen, indem sie neue Anfragen blockiert oder protokolliert, die nicht Ihren Standards entsprechen.

Warnmeldungen von einem API-Gateway sind in allen untersuchten Regionen das bevorzugte Mittel zur Erkennung von API-Angriffen. Dies gilt auch für die befragten Branchen. Insbesondere in Frankreich gaben 58 Prozent der Unternehmen an, dass sie API-Gateways einsetzen, um vor API-Angriffen gewarnt zu werden. Betrachtet man die verschiedenen Branchen, so liegt der Anteil der Unternehmen, die hauptsächlich auf API-Gateways setzen, im Groß- und Einzelhandel / E-Commerce bei 63 Prozent. Im Einzelhandel geben 16 Prozent der Befragten an, dass sie keine API-Angriffe identifizieren können.

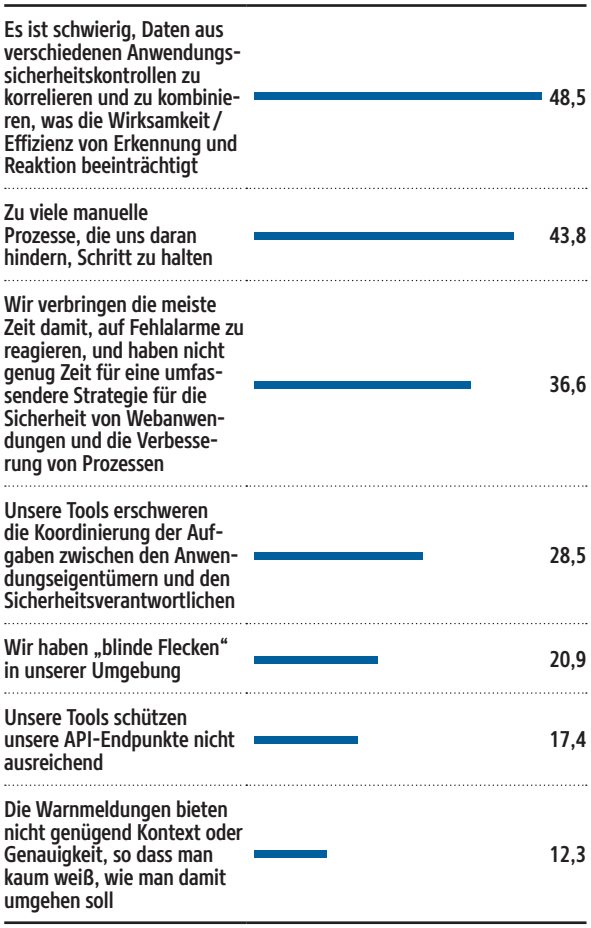
Wie identifizieren Sie einen Angriff auf Ihre APIs?

Mehrfachnennungen möglich. Angaben in Prozent. Basis: n = 235



Was sind Ihrer Meinung nach die größten Herausforderungen für Ihre Organisation in Bezug auf Sicherheitstools für Webanwendungen?

Mehrfachnennungen möglich. Angaben in Prozent. Basis: n = 235



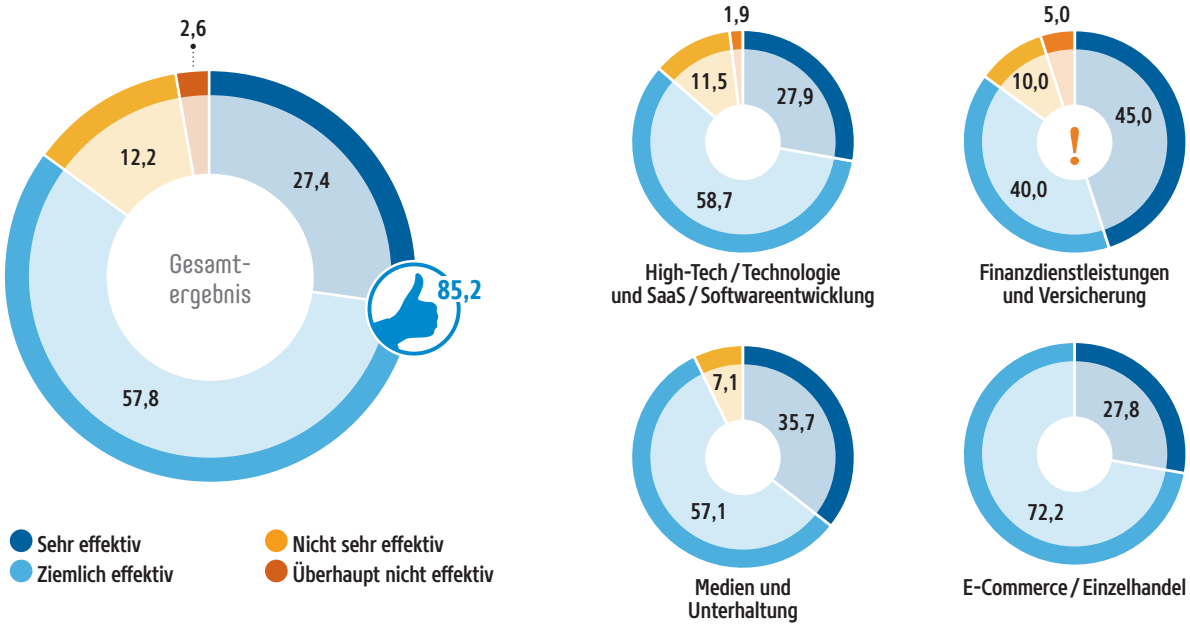
Interessanterweise halten 85 Prozent der befragten Unternehmen ihre API-Sicherheitstools für effektiv, und zwar auch in der Finanz- und Versicherungsbranche. Dies ist etwas überraschend, da 29 Prozent der Befragten aus diesem Sektor zugeben, dass sie keine API-Angriffe identifizieren können.

Darüber hinaus geben 49 Prozent der Befragten an, dass es schwierig ist, Daten aus verschiedenen Anwendungssicherheitskontrollen zu korrelieren und zu kombinieren, was die Wirksamkeit und Effizienz von Erkennung und Reaktion beeinträchtigt.

Schlussfolgerung: Die enorme Menge an Meldungen, die Unternehmen über ihre bevorzugten Lösungen erhalten, macht es schwierig, API-Angriffe zuverlässig zu erkennen. Das gilt insbesondere für die Bewertung von Protokolldaten. Es ist unerlässlich, dass Finanzinstitute, die Transaktionen über APIs durchführen, regelmäßige Sicherheitsbewertungen und eine Planung für die Handhabung von Zwischenfällen vornehmen, um das Risiko zu minimieren. KI-Technologien, die derzeit nur wenig genutzt werden, können hier eine große Hilfe sein.

Wie effektiv verhindern Ihre vorhandenen Sicherheits-Tools API-Angriffe?

Angaben in Prozent. Basis: n = 235



6

Konsolidierte Web- und API-Sicherheit werden Standard

98 Prozent der Unternehmen haben Interesse an einer konsolidierten Webanwendungs- und API-Sicherheitslösung von einem einzigen Anbieter. 19 Prozent der Befragten nutzen bereits eine solche Lösung, 69 Prozent planen deren Einführung und weitere sechs Prozent wollen sich darüber informieren.

Die Verwendung einer konsolidierten Webanwendungs- und API-Sicherheitslösung von einem einzigen Anbieter ist in Spanien weit verbreitet, wo 30 Prozent der befragten Unternehmen entsprechend antworteten. Im Gegensatz dazu sind nur sieben Prozent der Unternehmen in Skandinavien dazu übergegangen, eine konsolidierte Web- und API-Sicherheitslösung zu verwenden.

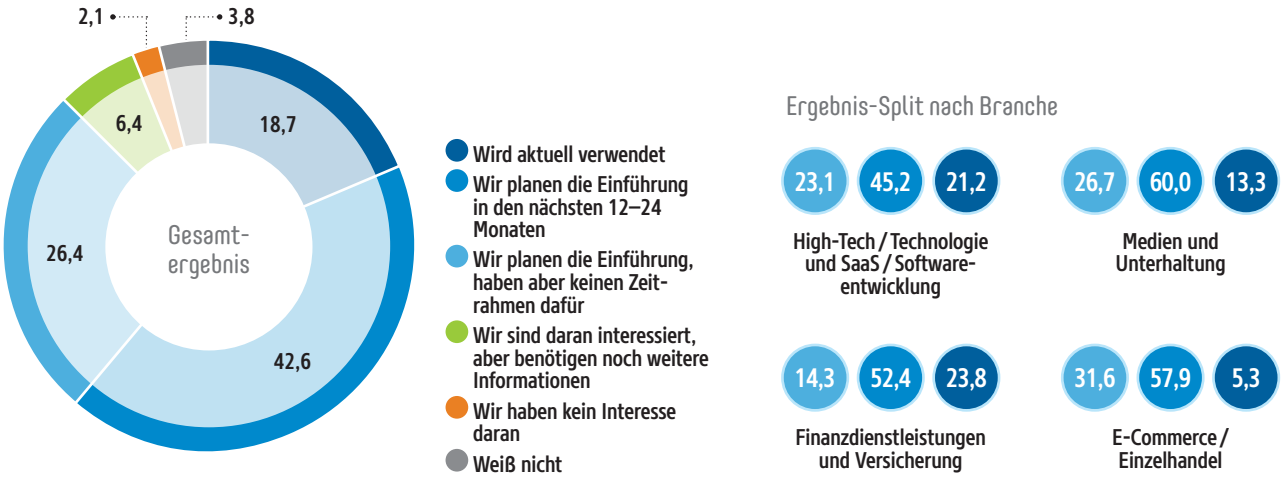
Eine wichtige Säule der bewährten API-Sicherheitspraktiken schreibt vor, dass API-Aktivität durch Überwachung und Protokollierung verdächtiger, ungewöhnlicher oder bösartiger Anfragen und Antworten verfolgt werden muss. Eine konsolidierte Webanwendungs- und API-Sicherheitslösung würde sofortige Entscheidungen treffen, um zu bestimmen, ob bösartige oder anomale Nutzdaten vorhanden sind, und dazu beitragen, die Zeit bis zur Erkennung von bösartigem Datenverkehr zu verkürzen und diesen davon abzuhalten, die API zu erreichen.

Bei der Betrachtung der einzelnen Sektoren zeigen sich auch erhebliche Unterschiede in der Haltung gegenüber der Nutzung einer konsolidierten Webanwendungs- und API-Sicherheitslösung eines einzigen Anbieters. 24 Prozent der befragten Finanzinstitute und Versicherer nutzen derzeit eine solche Lösung, aber nur fünf Prozent der Einzelhandelsunternehmen.

48 Prozent der Befragten gaben an, dass die Flexibilität, verschiedene Anwendungsarchitekturen durch unterschiedliche Bereitstellungsmodelle zu schützen, für sie wichtig ist. Auf C-Level- und Compliance-Ebene steigt diese Zahl auf 59 Prozent, fällt aber bei den Sicherheitsexperten auf 41 Prozent. Laut den Angaben von 51 Prozent der Befragten ist diese Flexibilität regional betrachtet in Spanien besonders beliebt. Unter den befragten Sektoren steigt diese Zahl sogar auf 71 Prozent bei Finanzdienstleistern und Versicherern, die angeben, dass es möglich sein sollte, verschiedene

Womit ist für Ihr Unternehmen die Nutzung von oder das Interesse an einer konsolidierten Webanwendungs- und API-Sicherheitslösung von einem einzigen Anbieter am besten beschrieben?

Angaben in Prozent. Basis: n = 235



Anwendungsarchitekturen mit unterschiedlichen Bereitstellungsmodellen zu schützen.

Interessanterweise zeigen die C-Level- und die Compliance-Ebene eine unterdurchschnittliche Zustimmung in Bezug auf Funktionen für die Automatisierung und Orchestrierung, die Fähigkeit, sehr komplexe Regeln oder Richtlinien anzuwenden, um den Geschäftsanforderungen zu entsprechen, und virtuelles Patching. Während beispielsweise der Durchschnitt aller Befragten, die die Fähigkeit zur Anwendung komplexer Regeln und Richtlinien entsprechend den geschäftlichen Anforderungen für wichtig halten, bei 20 Prozent liegt, beträgt dieser Wert bei C-Level-Führungskräften und Compliance-Verantwortlichen nur zwölf Prozent und bei Sicherheitsexperten 27 Prozent.

Schlussfolgerung: Es besteht ein großes Verlangen nach Konsolidierung der Web- und API-Sicherheit und nach Konzentration auf einen einzigen Anbieter. Es hat jedoch den Anschein, dass C-Level und Compliance die Komplexität unterschätzen, die mit solchen Lösungen bewältigt werden muss. Sicherheitsexperten müssen besser über die internen Prozesse informiert sein, damit die gewünschte Lösung auch den komplexen Anforderungen ihres Unternehmens gerecht werden kann.

Welche der folgenden Eigenschaften einer Sicherheitslösung für Webanwendungen sind Ihrer Meinung nach am wichtigsten?

Angaben in Prozent. Basis: n = 235

Die großen Erwartungen an KI-basierte API-Sicherheit werden nicht von allen geteilt

58 Prozent der befragten Unternehmen erwarten einen hohen oder sehr hohen Einfluss von KI auf die Sicherheit von APIs. Nur vier Prozent haben geringe bis sehr geringe Erwartungen. Unter den Befragten auf C-Level- und Compliance-Ebene liegt die Zahl derer, die sich viel von KI im Bereich API-Sicherheit versprechen, bei 69 Prozent.

Unter den befragten Sicherheitsexperten sind die hohen Erwartungen an die KI-basierte API-Sicherheit weniger stark verbreitet, nur 52 Prozent teilen sie.

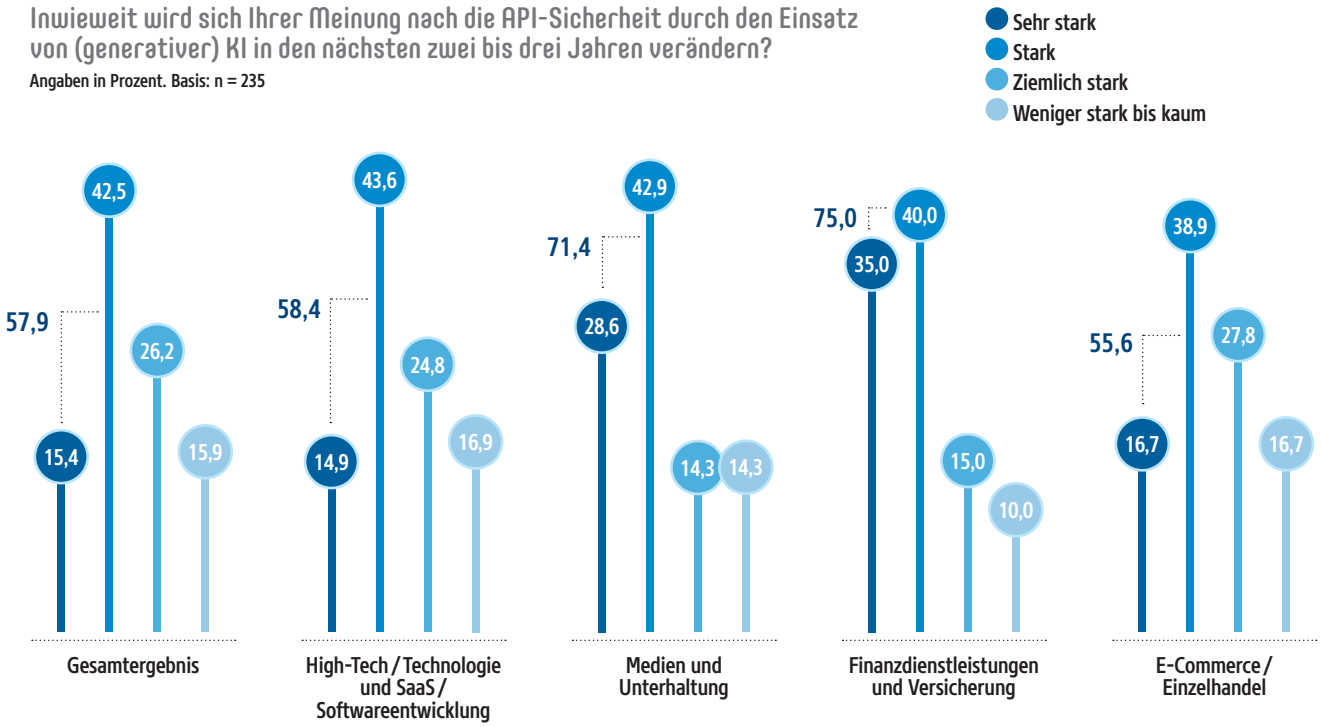
Im regionalen Vergleich glauben die Befragten aus Spanien und der DACH-Region mit 65 Prozent am häufigsten an einen hohen bis sehr hohen Einfluss von KI auf die API-Sicherheit. Besonders niedrig ist der entsprechende Anteil der Befragten in Skandinavien, wo nur 48 Prozent in diesem Sinne antworteten.

Während 56 Prozent der Unternehmen im Bereich Einzelhandel und E-Commerce den Einfluss von KI auf die Sicherheit von APIs als hoch oder sehr hoch einschätzen, sind es bei Finanzinstituten und Versicherungen 75 Prozent.

Schlussfolgerung: Über alle Unternehmensrollen und Branchen hinweg erwartet mindestens die Hälfte aller Befragten einen hohen oder sehr hohen Einfluss von KI auf die Sicherheit von APIs. Dies ist überraschend, wenn man bedenkt, dass KI-basierte Tools – also solche, die Aufgaben ersetzen, für die bisher Menschen erforderlich waren – für die API-Sicherheit noch nicht so weit verbreitet sind, wie es die Erwartungen vermuten lassen könnten. Es scheint Unsicherheiten und Hindernisse bei der Umsetzung zu geben.

Inwieweit wird sich Ihrer Meinung nach die API-Sicherheit durch den Einsatz von (generativer) KI in den nächsten zwei bis drei Jahren verändern?

Angaben in Prozent. Basis: n = 235



Unternehmen gehen auch davon aus, dass API-Schwachstellen durch KI zunehmen

62 Prozent der Unternehmen erwarten, dass KI einen hohen bis sehr hohen Einfluss auf die Zunahme neu identifizierter API-Schwachstellen haben wird, nur ein Prozent sagt, dass sie dies nicht erwarten. Die Zahl der Unternehmen in Skandinavien, die diese Ansicht teilen, ist mit 69 Prozent außergewöhnlich hoch. Nur 56 Prozent der Teilnehmer aus dem Vereinigten Königreich teilen diese Ansicht.

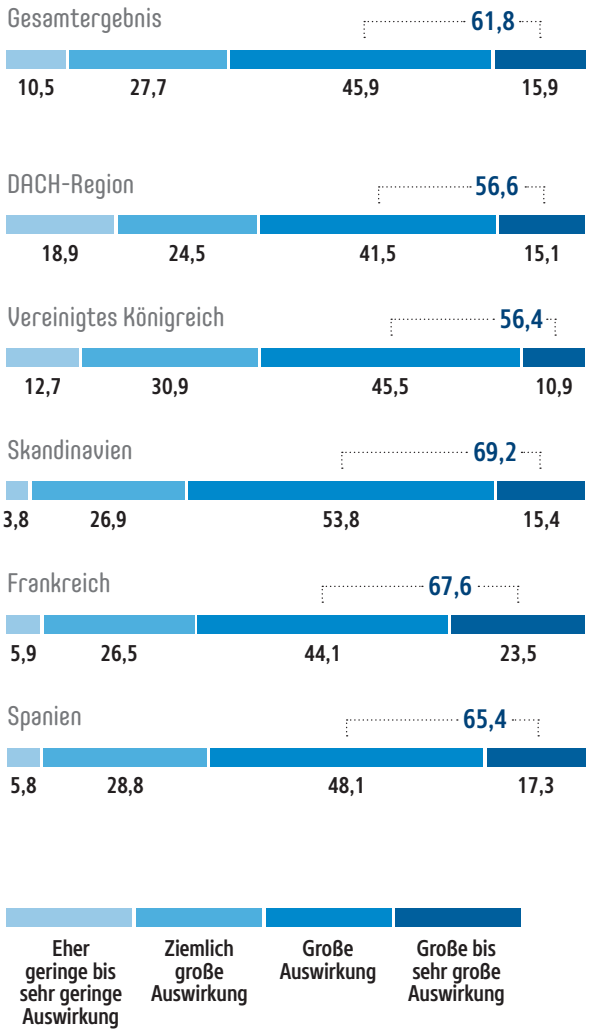
Auch die Rolle der Befragten im Unternehmen führt zu unterschiedlichen Einschätzungen. Von den C-Level-Führungskräften und Compliance-Verantwortlichen sagen 71 Prozent, dass das Wachstum von generativen KI-Tools einen hohen bis sehr hohen Einfluss auf neu auftretende API-Schwachstellen haben wird. Nur 54 Prozent der Sicherheitsexperten sehen dies ebenso.

Betrachtet man die verschiedenen Sektoren, so waren es im Groß- und Einzelhandel / E-Commerce deutlich mehr Befragte, die einen Zusammenhang zwischen dem zunehmenden Einsatz von KI und einer steigenden Zahl von API-Schwachstellen sahen: 72 Prozent gaben dies an. Bei den befragten Unternehmen im Bereich High-Tech / Technologie und SaaS / Softwareentwicklung hingegen sinkt der Anteil der Befragten mit dieser Ansicht auf 59 Prozent.

Schlussfolgerung: Die Mehrheit der befragten Unternehmen denkt auch über die möglichen API-Risiken durch den Einsatz von KI nach. Am Beispiel des Finanzsektors sehen wir jedoch, dass die potenziellen mit KI verbundenen Risiken nicht dazu führen sollten, dass man vor ihrem Einsatz zurückschreckt. Dies ist die Meinung von 70 Prozent der Befragten aus dem Finanzsektor, wo die Auswirkungen von KI auf die Zunahme von API-Schwachstellen als hoch oder sehr hoch eingeschätzt werden. Allerdings sehen drei Viertel der befragten Unternehmen in diesem Sektor auch die positiven Auswirkungen des Einsatzes von KI in der API-Sicherheit.

Welchen Einfluss wird die Zunahme generativer KI(-Tools) auf die Anzahl (und die Auswirkung) der neu auftretenden API-Schwachstellen haben?

Angaben in Prozent. Basis: n = 235



DACH-Region = Deutschland, Österreich, Schweiz
Skandinavien = Dänemark, Finnland, Norwegen, Schweden

Ausblick

API- und Websicherheit sind auf dem Weg zu intelligenter Konsolidierung

APIs sind zu einem der beliebtesten Vektoren für Angriffe zur Übernahme von Konten geworden. Credential Stuffing, Missbrauch von Geschäftslogik und DDoS-Angriffe sind nur einige der bösartigen automatisierten Bot-Angriffe, die eingesetzt werden, um Konten zu übernehmen und Identitätsdiebstahl und Betrug zu begehen. Leicht verfügbare Skripte und Tools machen die Orchestrierung von API-Angriffen einfacher denn je, und herkömmliche Verfahren zur Bot-Abwehr können diese potenziell verheerenden Angriffe nur schwer erkennen. Angesichts der ernsten Bedrohung, die APIs darstellen, muss die Sicherheit von Webanwendungen und APIs besser werden, moderne Methoden wie KI-basierte Tools stärker nutzen und die Verwendung isolierter Systeme vermeiden. Viele Unternehmen haben dies bereits erkannt, müssen sich aber intern besser aufstellen.

Von Oliver Schonschek

Die Sicherheit von Webanwendungen und APIs steht vor einem Umbruch. Wie diese Studie zeigt, mangelt es an Wissen über die Bedeutung von sicheren APIs und Webanwendungen. Wenn Zweifel an der Sicherheit von Produktions-APIs bestehen, ziehen es viele der befragten Unternehmen vor, die Einführung und Integration zu verschieben.

Eine neue Weise der Risikobetrachtung und neue technologische Prioritäten sind erforderlich

Bestimmte Schwachstellen in der API-Sicherheit werden in der Tat als erhebliche Bedrohung angesehen, z. B. die in veralteten APIs. Dagegen stehen andere Risiken wie Brute-Force-Angriffe auf APIs eher im Hintergrund.

Gleichzeitig stellen die Unternehmen Sicherheitsvorfälle bei ihren APIs fest, die unter anderem mit Anmeldungen, Berechtigungen und Identitäten im Zusammenhang stehen. In Anbetracht der hohen Zahl von API-Sicherheitsproblemen, die in Produktions-IT-Systemen festgestellt werden, würden wir eine Zunahme der Sicherheitsmaßnahmen in diesen Bereichen erwarten. Experten schätzen, dass der gesamte Bot-Datenverkehr fast die Hälfte des Internet-Datenverkehrs ausmacht und dass Bots, die Content Scraping, Credential Stuffing und DDoS-Angriffe durchführen können, für über 30 Prozent verantwortlich sind. Eine proaktive Bot-Abwehrstrategie würde dazu beitragen, Bot-Aktivitäten zu verstehen und zu blockieren, bevor sie sich auf Anwendungen und APIs auswirken und zu erheblichen finanziellen Einbußen durch Kompromittierung von Konten, Datendiebstahl, Betrug und erhöhte Infrastrukturkosten führen können.

Aufgrund fehlender Finanzmittel und mangelnden Fachwissens wird sie jedoch nicht realisiert. Dementsprechend geben die meisten Unternehmen, und zwar 84 Prozent der Befragten, zu, dass sie über keinerlei fortschrittliche API-Sicherheit verfügen. Tatsächlich wurden keine technologischen Prioritäten festgelegt, um den Einsatz fortschrittlicherer Methoden für einen besseren API-Schutz zu prüfen. Der Fokus liegt auf der Protokollierung und Überwachung von APIs. Dies ist zwar wichtig, reicht aber nicht aus. Der Einsatz von KI-Technologien wurde nur von 14 Prozent der Unternehmen als Priorität genannt.

Die Erkennung von API-Angriffen muss verbessert werden

Selbst stark regulierte Sektoren wie das Finanz- und Versicherungswesen sind nicht in der Lage, Angriffe auf APIs ausreichend zu erkennen. Dies ist nicht verwunderlich, da Unternehmen immer mehr auf API-Gateways und Protokolldaten setzen, um Hinweise auf API-Angriffe zu erhalten.

Die Menge und die Komplexität der Daten, die Indikatoren für API-Angriffe liefern können, müssen jedoch schneller und in konsolidierter Form ausgewertet werden, damit Cyberangriffe besser erkannt und abgewehrt werden können. Langwieriges Durchsuchen von Protokolldaten und isolierte Warnungen von einzelnen Sicherheitstools können nicht optimal sein.

Aber Verbesserungen sind in Sicht: 88 Prozent der befragten Unternehmen nutzen bereits eine konsolidierte Sicherheitslösung für Webanwendungen und APIs von einem einzigen Anbieter oder planen dies. Dies reduziert den erforderlichen Arbeitsaufwand und verbessert die Sichtbarkeit von API-Risiken und -Angriffen. Anders als isolierte Tools können konsolidierte Lösungen die erforderliche Rundumsicherheit für APIs und Webanwendungen bieten.

Konsolidierung und KI stärken die API-Sicherheit

Die Mehrheit der Unternehmen sieht auch große Vorteile im Einsatz von KI-basierten Tools zur Stärkung der API-Sicherheit. Dies gilt insbesondere für die befragten Unternehmen des Finanz- und Versicherungssektors, die bis heute große Schwierigkeiten haben, API-Angriffe zu erkennen.

Auch die Tatsache, dass rund die Hälfte der Unternehmen eine Edge-native Plattform und Cloud-native Sicherheit als wichtigste (Auswahl-)Kriterien für die Evaluierung von API-Sicherheitslösungen anführen, lässt hoffen.

Dennoch muss das Thema besser verstanden werden. 16 Prozent gaben an, sie wüssten nicht, ob sie bereits KI für ihre API-Sicherheit einsetzen oder nicht. Nur 18 Prozent gaben an, dass sie KI für API-Sicherheit einsetzen, während 66 Prozent sagten, dass sie es nicht tun.

Um die erwarteten Vorteile der KI für die API-Sicherheit nutzen zu können, müssen Unternehmen eine genauere Vorstellung von den KI-basierten Tools haben, die sie bereits einsetzen oder noch einsetzen wollen.

Die potenziellen Risiken, die durch den Einsatz von künstlicher Intelligenz (KI) zunehmen können, müssen Teil der Sicherheitsagenda sein. Wie die Umfrage zeigt, sind sich die befragten Unternehmen der Risiken sehr bewusst, die z. B. dadurch entstehen können, dass Cyberkriminelle KI-Tools nutzen, um schneller und einfacher Schwachstellen in APIs zu finden.

Sechs von zehn Unternehmen erwarten, dass sich KI stark oder sehr stark auf die Anzahl der API-Schwachstellen auswirken wird. Nur ein Prozent erwartet, dass die Auswirkungen der KI auf die steigende Zahl der API-Sicherheitsschwachstellen gering oder sehr gering sein werden.

Schlussfolgerung: Die Mehrheit der befragten Unternehmen in den verschiedenen Sektoren und Regionen hat die Vorteile der Konsolidierung von API- und Web-Sicherheit erkannt und sie bereits umgesetzt oder plant, dies zu tun. Ebenso groß sind das Interesse am und die Erwartungen an den Einsatz von KI zur Unterstützung der API-Sicherheit. Bei der Umsetzung müssen jedoch noch weitere Fortschritte erzielt werden. Es ist gut zu sehen, dass Bedenken in Bezug auf KI nicht bedeuten, dass Unternehmen KI zur Optimierung der API-Sicherheit ausschließen.

KI und Konsolidierung müssen Priorität haben bzw. behalten, um die Sicherheit von Webanwendungen und APIs zu verbessern. Angriffe auf Webanwendungen und APIs werden bereits immer ausgefeilter. Die Verteidigung der APIs muss damit Schritt halten. Diese Umfrage zeigt, dass es gut darum steht.

Case Study: Nine

Nine stärkt und optimiert Sicherheit mit Fastly's Managed Security Service

Nine, Australiens größtes Medienunternehmen in lokalem Besitz, führt Australiens bekannteste und beliebteste Marken in den Bereichen Nachrichten, Wirtschaft und Finanzen, Lifestyle, Unterhaltung und Sport. Nine ist Eigentümer des Fernsehsenders 9Network, wichtiger Publikationen wie dem Sydney Morning Herald, digitaler Angebote wie nine.com.au, der Abonnement-Videoplattform Stan, mehrerer Radiosender und anderer.

Die Herausforderung

Als Nine sich darauf vorbereitete, die Sicherheit seiner Webanwendungen auszubauen, erkannte das Plattformentwicklungsteam, dass es eine Konsolidierung auf einen einzigen Partner für die Verwaltung der Sicherheit seiner Webanwendungen erreichen musste. Der Partner würde proaktiv Bedrohungserkennung und -bekämpfung für Nine-Webanwendungen bereitstellen und bei Bedarf auch Sicherheitsexpertise für die Zusammenarbeit bieten. Durch den richtigen Managed Security Service würde auch der Aufwand für mehrere Serviceanbieter reduziert, und die Tools und das Management des Infrastructure-as-Code-Ansatzes von Nine würden optimiert. Mit einem verwalteten Dienst zur Überwachung und proaktiven Abwehr von Angriffen hätte das Technikteam von Nine mehr Zeit, sich mit Produkten und Dienstleistungen zu befassen, um die Marken des Unternehmens zu stärken.

> „Fastly Managed Security Service erweitert unsere Sicherheitskapazitäten – vom Bot-Schutz bis zur Bandbreitenbegrenzung bei neuen Bedrohungen. Und wir werden in der Lage sein, unseren Schutz im Laufe der Zeit weiter auszubauen."
>
> Andre Lackmann, Technology Director bei Nine

Die Lösung

Nine entschied sich für die Fastly Next-Gen WAF und den Managed Security Service aufgrund der Sicherheitsexpertise, der Skalierbarkeit, der technologischen Eignung und des Nutzens.

Sicherheitsexpertise

Anstatt ihre Techniker zu Web Application Firewall (WAF)-Experten ausbilden zu lassen, wusste man bei Nine, dass es vorteilhafter wäre, den Managed Security Service von Fastly zu nutzen und die Next-Gen WAF von den Experten von Fastly proaktiv verwalten zu lassen. „Nine begrüßte die Möglichkeit, Fastly die Möglichkeit zu geben, in unserem Namen Änderungen vorzunehmen", sagte Lee Webb, Senior Engineering Manager bei Nine.

„Meine Entwickler sind beeindruckt von den Sicherheitsexperten, die Fastly uns zur Seite gestellt hat, sie haben großen Respekt. Es hilft, Vertrauen aufzubauen, wenn man Leute hat, die genauso talentiert sind wie man selbst."

Das SOC von Nine hat die Berichte zum Threat Hunting, die Teil des Managed Security Service sind, als sehr nützlich empfunden. „Fastly lieferte Empfehlungen für Feinabstimmungen sowie umsetzbare Bedrohungsintelligenz und Empfehlungen mit konkreten Schritten, die wir zur Schadensbegrenzung nutzen konnten. Auf dieser Grundlage haben wir uns entschlossen, den Fastly Managed Security Service für alle unsere öffentlichen Websites zu implementieren", so Webb.

Durch die Einbindung aller öffentlich zugänglichen Websites von Nine in den Managed Security Service von Fastly konnte Nine die Komplexität und Redundanz in seiner Umgebung und die Anzahl der Tools reduzieren. „Das spart uns viel Zeit", bestätigt Webb.

Vertrauenswürdiger Partner

Nine arbeitete 2017 mit Fastly zusammen, um Legacy-Systeme auf einen Microservices-Ansatz umzustellen. Damals nahm das Unternehmen Fastly als Anbieter eines Content Delivery Network (CDN) in Anspruch. Im Laufe der Jahre hat sich Fastly als kompetent und umgänglich erweisen. Im Rahmen eines Betaprogramms hat das Fastly Managed Security Service-Team seine Fähigkeit unter Beweis gestellt, Webanwendungen proaktiv vor Cyber-Bedrohungen zu schützen und eine fachkundige Cybersecurity-Zusammenarbeit zu bieten.

Als Nine den Managed Security Service bei einigen der größten Sportereignisse wie dem Australian Open-Tennisturnier einsetzte, erwies sich das Customer Security Operations Center (CSOC) von Fastly, das im Rahmen des Managed Security Service rund um die Uhr Bedroohungsüberwachung und -reaktion bereitstellt, als proaktiver und serviceorientierter Partner. „Wir waren mit dem von Fastly gebotenen Sicherheitsservice sehr zufrieden.

Unsere Beziehung zu Fastly ist vertrauensvoll und bewährt“, so Webb. „Wir vertrauen darauf, dass Fastly den Herausforderungen gewachsen ist, denn das haben sie im Laufe unserer Zusammenarbeit bewiesen.“

Weniger Arbeitsbelastung

„Fastly ermöglichte es unseren Teams, sich nicht so sehr mit dem mühsamen Aspekt, der täglichen Überwachung, befassen zu müssen. Dadurch konnten wir uns auf die Umsetzung konzentrieren und darauf, wie unsere Dienste aus technologischer Sicht bereitgestellt werden können, und wir konnten unser Augenmerk auch stärker auf das Nutzererlebnis legen“, so Andre Lackmann.

Über Nine

Branche: Streaming-Medien, Digital Publishing
Standort: Asien-Pazifik
Kunde seit: 2017
Bevorzugte Features: Managed Security Services, NG WAF, CDN

Nine ist Australiens größtes Medienunternehmen in lokalem Besitz mit Aktivitäten in den Bereichen Fernsehen, Video-on-Demand, Print, Digital und Radio. Nine ist unter anderen Eigentümer von 9Network, wichtiger Zeitschriften wie The Sydney Morning Herald, The Age und Australian Financial Review, digitaler Angebote wie nine.com.au, 9Honey, Pedestrian Group und Drive, der Abonnement-Videoplattform Stan, Talk-Back-Radio und hält Mehrheitsbeteiligungen an Domain und Future Women.

www.nineforbrands.com.au

Ein weiterer Vorteil, den Nine festgestellt hat, ist die erhebliche Reduzierung von Spam-Warnungen, die an das Security Operations Center (SOC) gehen. Die Fastly Next-Gen WAF zeichnet sich nicht nur durch eine weitaus höhere Genauigkeit und praktisch keine Fehlalarme aus, sondern dank der Überwachung der WAF durch das CSOC von Fastly werden nur eskalierte Alarme weitergeleitet. Das Team schätzt die Verwendung von Slack als primären Benachrichtigungskanal mit Richtlinien, wann SMS und Anrufe gerechtfertigt sind.

Maßgeschneiderte Technologie

Die Edge-Cloud-Plattform von Fastly, einschließlich seines CDN, seiner Sicherheitsprodukte und seiner Managed Services, passt gut zum Infrastructure-as-Code-Ansatz von Nine bei der Softwarebereitstellung. Fastly fügt sich leicht ein, anstatt dass Nine einen anderen Ansatz eines anderen Anbieters übernehmen muss. „Es ist beeindruckend, wie gut sich die Technologie einfügt“, so Webb.
Die Entwickler von Nine kümmern sich um ihre Anwendungen bis hin zum Edge und können dies mit den Sicherheitstools von Fastly wie Next-Gen WAF tun, weil Fastly Nine die Kontrolle über ihren Technologiestack ermöglicht und gleichzeitig fortschrittliche Sicherheitsmaßnahmen nahtlos integriert. „Bei anderen Anbietern von Managed Security war das nicht möglich“, erklärt Webb.

Fokus auf die nächsten drei Olympischen Sommerspiele

Mit Blick auf die Zukunft, in der sich die Bedrohungslandschaft weiterentwickelt, schätzt Nine die Beruhigung, die der Managed Security Service von Fastly ihnen bietet. „Es gibt eine professionelle Sicherheitsunterstützung, die mit neu auftretenden Bedrohungen Schritt hält, sie kontinuierlich überwacht und uns hilft, darauf zu reagieren. Und das wird sehr wichtig, wenn Nine die Rechte für die Olympischen Sommerspiele erwirbt“, so Andre Lackmann, Technology Director bei Nine. „Großveranstaltungen sind uns nicht fremd, aber es gibt kein größeres Ereignis als die Olympischen Spiele. Aus technischer Sicht ist das ein gewaltiges Unterfangen, auch in Bezug auf die Sicherheit. Wir freuen uns daher auf die Zusammenarbeit mit Fastly, um unseren australischen Zuschauern und Lesern ein erstklassiges Nutzererlebnis zu bieten.“

Nine

Studiensteckbrief

Herausgeber	CSO, CIO und COMPUTERWOCHE
Exklusiver Studienpartner	Fastly
Grundgesamtheiten	C-Level-Führungskräfte – CISOs, CIOs, VP Security, IT-Sicherheitsführungskräfte oder IT-Führungskräfte innerhalb der Plattform oder DevSecOps-Teams (Entscheidungsträger) Sicherheitsexperten, Sicherheitsanalysten, Sicherheitsarchitekten (Influencer) aus den folgenden Regionen: DACH, Skandinavien, VK, Frankreich und Spanien
Teilnehmergenerierung	Persönliche E-Mail-Einladung über die exklusive Entscheiderdatenbank von CIO, CSO und COMPUTERWOCHE und – zur Erfüllung der Quotenvorgaben – über externe Online-Access-Panels
Gesamtstichprobe	235 abgeschlossene und qualifizierte Interviews
Untersuchungszeitraum	15. bis 23. November 2023
Methode	Online-Umfrage (CAWI)
Fragebogenentwicklung und Durchführung	Custom Research Team von CSO, CIO und COMPUTERWOCHE in Zusammenarbeit mit dem Studienpartner

Stichprobenstatistik

Funktionale Rolle	C-Level (CSO, CISO, CIO, CTO, VP Security, IT-Sicherheit)	30,2 %
	IT-Führungskraft, IT-Manager mit dedizierter Verantwortung für IT-Sicherheit	17,0 %
	IT-Sicherheitsführungskraft, IT-Sicherheitsmanager	20,4 %
	Director Cybersecurity	6,0 %
	DevSecOps-Team	5,1 %
	Sicherheitsexperte, Sicherheitsanalyst, Sicherheitsarchitekt	11,5 %
	Netzwerksleiter	6,8 %
	Compliance / Risikomanagement	1,7 %
	Sonstige	1,3 %
Jährliche Aufwendungen in IT-Systeme	Weniger als 5 Prozent des gesamten IT-Budgets	13,6 %
	5 bis weniger als 10 Prozent des gesamten IT-Budgets	35,7 %
	10 bis weniger als 20 Prozent des gesamten IT-Budgets	27,2 %
	20 bis 30 Prozent des gesamten IT-Budgets	13,6 %
	Mehr als 30 Prozent des gesamten IT-Budgets	4,3 %
	Weiß nicht / keine Antwort	5,5 %

Impressum

Exklusiver Studienpartner

Fastly
179 Great Portland St
London W1W 5PL, Vereinigtes Königreich
Telefon: +49 89 255527978
E-Mail: kontakt@fastly.com
Website: www.fastly.com

Gesamtstudienleitung

Matthias Teichmann
Director Research
Foundry Global Services
Telefon: +49 89 36086 131
matthias.teichmann@foundryco.com

Studienkonzept / Fragebogenentwicklung:
Matthias Teichmann (Foundry)

Endredaktion / CvD Studienberichtsband:
Matthias Teichmann

Analysen / Kommentierungen:
Oliver Schonschek, Bad Ems

Hosting / Koordination Feldarbeit:
Armin Rozsa (Foundry)

Layout:
Patrick Birnbreier, München

Umschlaggestaltung unter Verwendung einer Illustration von
© shutterstock.com / BadBrother

Kontakt:
Matthias Teichmann
matthias.teichmann@foundryco.com

Herausgeber:

Foundry
(formerly IDG Communications)

IDG Tech Media GmbH
Georg-Brauchle-Ring 23
80992 München, Deutschland
Telefon: +49 89 36086 0
Fax: +49 89 36086 118
E-Mail: info@idg.de

Vertretungsberechtigter:
Jonas Triebel, Geschäftsführer

Registergericht:
Amtsgericht München, HRB 99110

Umsatzsteueridentifikationsnummer:
DE 811 257 834

Weitere Informationen unter:
www.foundryco.com

Über Fastly

Die leistungsstarke und programmierbare Edge-Cloud-Plattform von Fastly unterstützt weltweit führende Marken bei der Bereitstellung bestmöglicher Online-Erlebnisse. Fastly bietet seinen Kund:innen Edge Computing, Content Delivery sowie Cybersecurity- und Observability-Produkte zur Verbesserung ihrer Website-Performance, Erhöhung der Sicherheit und Förderung von Innovationen auf globaler Ebene. Im Vergleich zu herkömmlichen Anbietern ist die moderne Netzwerkarchitektur von Fastly eine der schnellsten der Welt. Sie ermöglicht Entwickler:innen, sichere Websites und Anwendungen global bereitzustellen, bei gleichzeitig kurzen Markteinführungszeiten und einem Kosteneinsparungspotenzial, das branchenführend ist. Unternehmen auf der ganzen Welt vertrauen auf Fastly, wenn es darum geht, ihr Internet-Erlebnis zu verbessern, darunter Reddit, Wendy's, Stripe, Neiman Marcus, Universal Music Group, SeatGeek und Advance Publications.

fastly®

Erfahren Sie mehr über Fastly unter https://www.fastly.com/de und folgen Sie uns unter @fastly.

Sicherheit ist ein wesentlicher Bestandteil jedes Online-Geschäfts, und Kunden verlassen sich auf Fastly, wenn es darum geht, ihre geschäftskritischen Websites, Anwendungen und APIs schnell zu sichern. Der moderne Ansatz von Fastly für die Anwendungssicherheit bietet die Genauigkeit, Flexibilität und Benutzerfreundlichkeit, die unsere Kund:innen kennen und erwarten. Fastly bietet eine Reihe von Sicherheitslösungen für Unternehmen an, die sich mit dem Schutz von Websites, Anwendungen und APIs vor verschiedenen Bedrohungen wie DDoS-Angriffen, Angriffen auf der Anwendungsebene und missbräuchliches Verhalten durch automatisierte Software befassen. Diese Lösungen sind auf Echtzeit, Skalierbarkeit und Anpassbarkeit ausgelegt und bieten Unternehmen die Möglichkeit, ihre Sicherheit an ihre spezifischen Anforderungen anzupassen. Mit dem Fokus auf Leistung und Flexibilität ermöglicht Fastly Unternehmen, ihre digitalen Erfahrungen zu schützen.

Fastly bietet den proaktiven Schutz, den moderne Anwendungen benötigen, lässt sich in Ihre DevOps- und Sicherheits-Toolchains integrieren und gewährleistet eine beispiellose Transparenz. Unsere flexible Architektur kann Ihre Anwendungssicherheitsstrategie vorantreiben, indem sie Entwicklungs- und Sicherheitsteams Einblick gibt, wo und wie Ihre Webanwendungen und APIs angegriffen werden.