Mai 2021

MARKTBERICHT

Application Security 2021 - Ein Überblick

Bösartige Bots, defekte APIs und Angriffe auf die Lieferkette gefährden Unternehmensdaten. »

Barracuda
Your journey, secured.

Inhalt

Einleitung

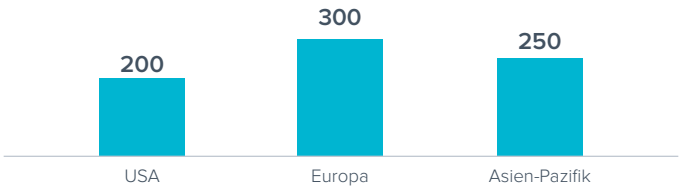
Application Security 2021 - Ein Überblick

Unternehmen stehen vor einer Reihe von Herausforderungen, wenn es um die Anwendungssicherheit geht. Im Laufe der Jahre haben Webanwendungen als Top-Angriffsvektor für Sicherheitsverletzungen stetig zugenommen. Der Wechsel in Richtung Remote-Arbeit im Jahr 2020 hat diese Verschiebung noch verstärkt. Vor diesem Hintergrund mussten viele Unternehmen interne Anwendungen dem Internet aussetzen, und eine beträchtliche Anzahl musste Anwendungen schnell in die Cloud verlagern.

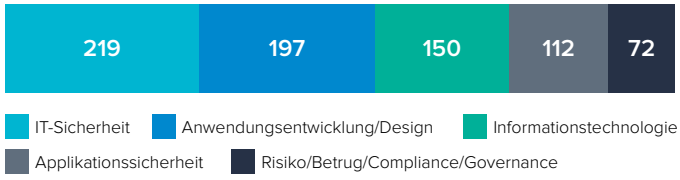
Im Rahmen dieser Umfrage haben wir Unternehmen gefragt, wie oft sie im vergangenen Jahr als direkte Folge einer Sicherheitslücke in einer ihrer Anwendungen angegriffen wurden. Der weltweite Durchschnitt lag bei zwei Sicherheitsverletzungen in den letzten 12 Monaten.

Die Befragten gaben an, dass die überwiegende Mehrheit dieser Angriffe auf Schwachstellen in Web-Applikationen zurückzuführen ist. Bot-Angriffe, Probleme mit der API-Sicherheit und Angriffe auf die Software-Lieferketten gehören zu den wichtigsten Faktoren, die zu diesen Sicherheitsverletzungen beitragen. Die Umfrageteilnehmer gaben bereitwillig zu, dass in allen drei Bereichen erhebliche Verbesserungen erforderlich sind. Und obwohl es einige interessante regionale und subregionale Unterschiede gab, waren die Trends weltweit sehr ähnlich.

Umfrageteilnehmer nach Region



Umfrageteilnehmer nach Job-Funktion



Methodik

Barracuda beauftragte das unabhängige Marktforschungsunternehmen Vanson Bourne mit der Durchführung einer globalen Umfrage unter **750 Entscheidungsträgern für Anwendungssicherheit**, die für die Anwendungsentwicklung und -sicherheit ihrer Organisation verantwortlich sind. Die Umfrageteilnehmer aus den **USA, Europa und dem asiatisch-pazifischen Raum** repräsentierten Organisationen mit 500 oder mehr Mitarbeitern weltweit. Da die IT-Zuständigkeiten und Cybersecurity-Bedrohungen je nach Region unterschiedlich sind, wurden Teilnehmer aus einer Vielzahl von Job-Funktionen und Branchen befragt, um ein Verständnis der Anwendungssicherheitsrisiken aus verschiedenen Perspektiven zu erhalten. Durchgeführt wurde die Umfrage im März und April 2021.

Die größten globalen Herausforderungen

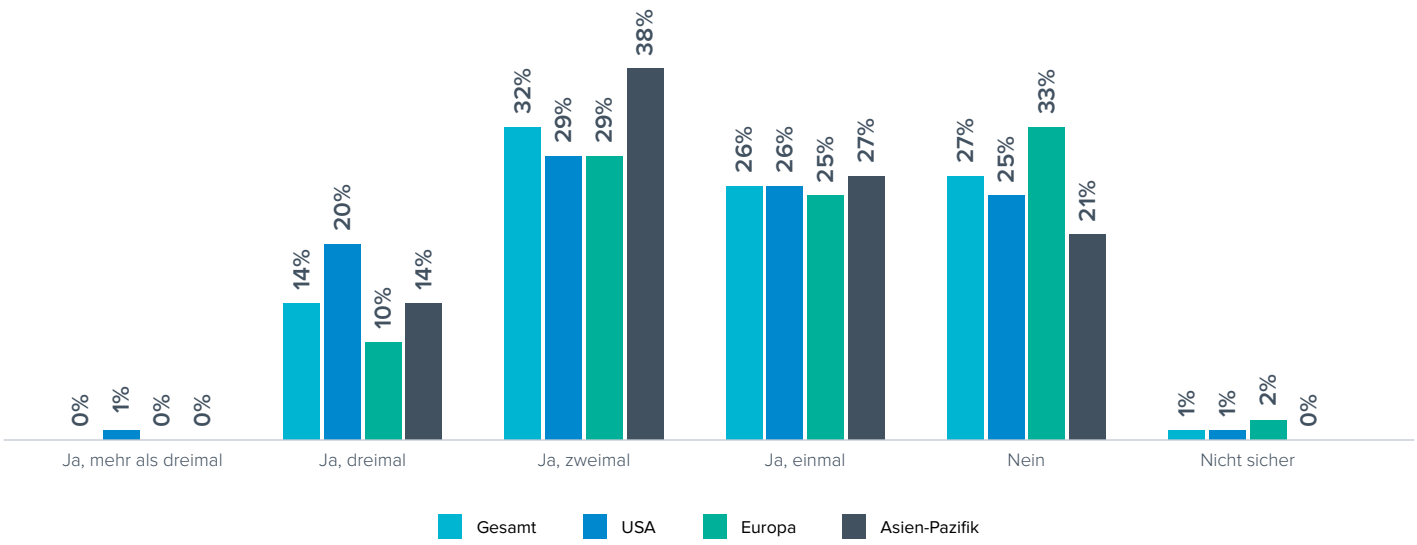
ERGEBNIS #1

Im Durchschnitt wurden die befragten Unternehmen in den letzten 12 Monaten zwei Mal als direkte Folge einer Anwendungsschwachstelle erfolgreich angegriffen.

72% der Befragten gaben an, dass ihr Unternehmen mindestens eine Sicherheitsverletzung aufgrund einer Anwendungsschwachstelle erlitten hat. Damit wird deutlich, wie aggressiv und allgegenwärtig anwendungsbasierte Cyberangriffe geworden sind. Dies ist wahrscheinlich auf die große Bandbreite an Sicherheitsbedrohungen zurückzuführen, die versuchen, Unternehmen zu schaden, sowie auf die internen Schwierigkeiten, mit denen viele Unternehmen konfrontiert sind.

Hat Ihr Unternehmen in den letzten 12 Monaten eine Sicherheitsverletzung als direkte Folge einer Schwachstelle in einer Ihrer Anwendungen erlitten?

(n=750)



Die größten globalen Herausforderungen

ERGEBNIS #2

Das Spektrum der Herausforderungen im Bereich der Anwendungssicherheit, mit denen Unternehmen konfrontiert sind, geht über die Schwierigkeiten bei der Absicherung mehrererAngriffsvektoren hinaus.

Es liegt auf der Hand, dass Unternehmen durch spezifische Sicherheitsbedrohungen wie Bot-Angriffe, Angriffe auf die Software-Lieferketten und die Sicherung ihrer APIs beunruhigt sind. Dies sind jedoch nicht die einzigen Herausforderungen. Auch Anforderungen an die Effizienz stellen ein Problem dar. Beleg hierfür sind die 35% der Befragten, die angeben, dass das Hinzufügen von Sicherheitsfunktionen die Entwicklungszeit von Anwendungen erheblich verlangsamt.

Die fünf größten Herausforderungen aus weltweiter Sicht sind Bots, Angriffe auf die Lieferkette, Schwachstellenerkennung, API-Sicherheit und Sicherheitsvorkehrungen, welche die App-Entwicklung verlangsamen.

Es gibt einige interessante regionale Unterschiede. In den USA schafft es die Erkennung von Schwachstellen nicht unter die Top 5. Stattdessen ist die Implementierung von Sicherheit in die kontinuierliche Integration und kontinuierliche Entwicklung (CI/CD) eine der größten Herausforderungen.

In Europa hingegen ist man weniger besorgt, dass Angriffe auf die Lieferkette und die App-Sicherheit die Entwicklung bremsen. Die Beseitigung von Bedrohungen wird hier als größere Herausforderung angesehen.

Im asiatisch-pazifischen Raum sind Sicherheitsmaßnahmen, die die App-Entwicklung verlangsamen, ein viel größeres Problem als in anderen Regionen.

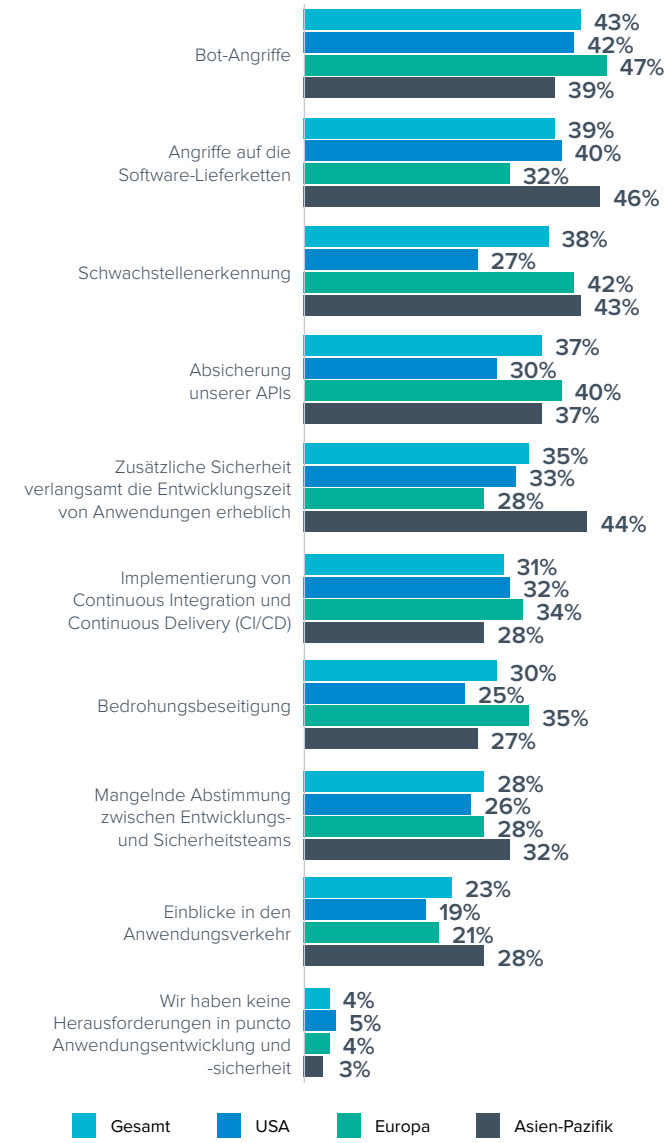
Die Schwachstellenerkennung ist eine Herausforderung, für die es viele relativ ausgereifte Lösungen gibt. Dabei ist die Herausforderung, Sicherheit in der Entwicklungsphase zu implementieren, insbesondere in DevOps-Umgebungen, an sich schon ein komplexes Thema.

In diesem Bericht konzentrieren wir uns auf die neueren Herausforderungen:

- Bots
- Angriffe auf Lieferketten
- API-Sicherheit

Welche dieser Herausforderungen bestehen in Ihrem Unternehmen in Bezug auf Anwendungsentwicklung und-sicherheit?

(n=750)



Die größten globalen Herausforderungen

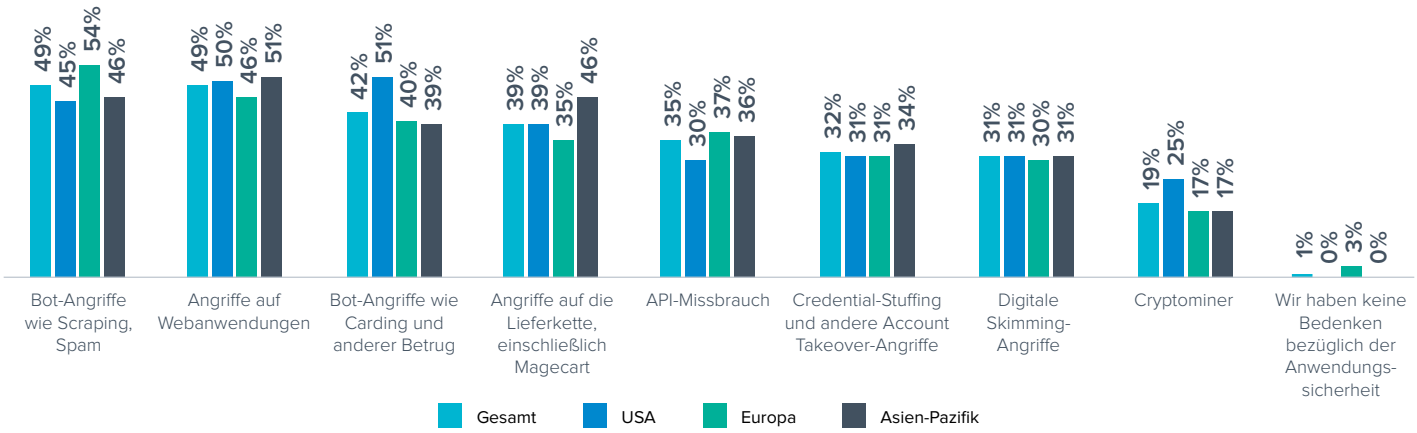
ERGEBNIS #3

Eine breite Palette von Risiken für die Anwendungssicherheit gibt Anlass zur Sorge. Verschiedene Variationen von Bot-basierten Angriffen stellen jedoch eine besonders große Sorge dar.

Es ist kein Geheimnis, dass Bots in den letzten Jahren zu einem wachsenden Problem für Unternehmen geworden sind. Dies wird durch die Tatsache unterstrichen, dass Bot-basierte Angriffe zwei der drei von Entscheidungsträgern am häufigsten genannten Risiken für die Anwendungssicherheit ausmachen. Dicht dahinter folgen API-Angriffe und Angriffe auf die Lieferkette. Unternehmen dürfen die Bedeutung der Anwendungssicherheit nicht aus den Augen verlieren. Denn über eines dieser Risiken könnte leicht eine Schwachstelle ausgenutzt werden. Eine Erholung von den Folgen könnte sich dabei als durchaus schwierig erweisen. Dies wird durch die Anzahl der Befragten deutlich, die Schwachstellen in Webanwendungen/Zero-Day-Angriffe als eines der Top-Risiken identifizieren.

Über welche AppSec-Risiken machen Sie sich in Ihrem Unternehmen am meisten Sorgen?

(n=750)



Bot-Angriffe

ERGEBNIS #4

Die Bandbreite der Bot-Angriffe, die Anwendungen ausnutzen können, stellt ein echtes Problem dar.

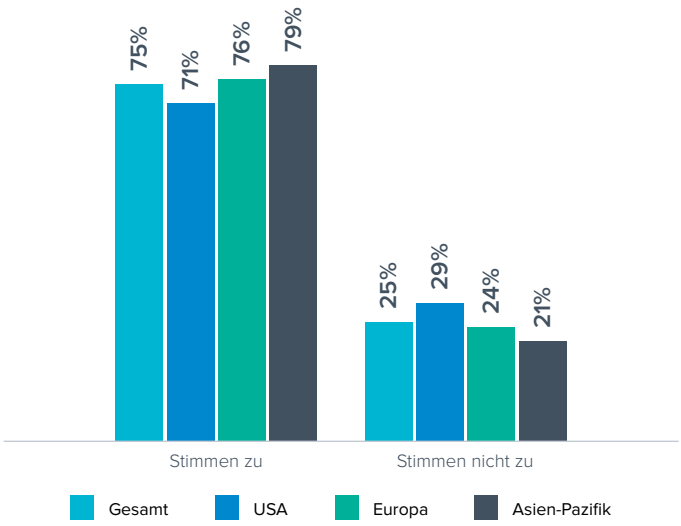
Drei Viertel der Entscheidungsträger bestätigen, dass die Bandbreite der Bot-Attacken beim Schutz von Anwendungen echte Schwierigkeiten in ihren Unternehmen verursacht. Es scheint, als könnten Organisationen einfach nicht mithalten. Mit einer ganzen Bot-Ökonomie, komplett mit Bot-Marktplätzen und Brokern, die sicherstellen, dass Bot-Benutzer selbst nicht betrogen werden, wird dieses Problem in den kommenden Jahren nur weiter wachsen. Automatisierte Angriffe decken eine so große Vielfalt an Vektoren und Intelligenz auf der Tooling-Seite ab, dass dies weltweit zu einem massiven Problem geworden ist.

Unternehmen werden externe Hilfe von Experten für Anwendungs- und Bot-Sicherheit benötigen, um sich effektiv gegen Bots zu wehren, die es auf ihre Anwendungen abgesehen haben. Ohne angemessene Abwehrmaßnahmen wird es unweigerlich zu Sicherheitsverletzungen oder – in einigen Fällen – zu erneuten Sicherheitsverletzungen kommen.

In unseren Daten stimmten die Befragten aus Unternehmen, in denen mehr als einmal ein Angriff stattfand, dieser Aussage am ehesten zu. Dies deutet wiederum darauf hin, dass Bots wahrscheinlich eine Ursache für viele dieser Verstöße waren.

Das vielfältige Spektrum an Bot-Angriffen, die unsere Anwendungen ausnutzen könnten, macht eine Verteidigung zunehmend schwieriger.

(n=750)



Bot-Angriffe

ERGEBNIS #5

Bot-basierte Angriffe sind die wahrscheinlichste Ursache für Sicherheitsverletzungen aufgrund von Anwendungsschwachstellen in den letzten 12 Monaten.

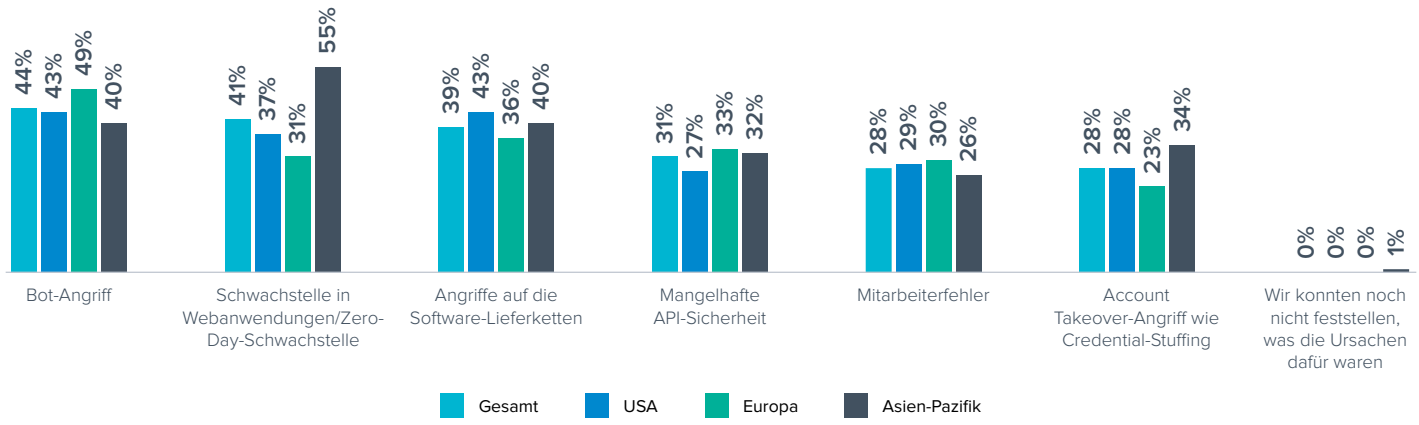
Die Besorgnis um Bots ist durchaus begründet, da sie im letzten Jahr besonders erfolgreich bei Angriffen auf Anwendungen waren. Aber das ist sicherlich nicht der einzige Vektor, der dazu beigetragen hat.

Im Durchschnitt gaben die Befragten an, dass es zwei Faktoren gab, die zu der letzten Sicherheitsverletzung in ihrem Unternehmen beigetragen haben, was auf das Ausmaß der Herausforderung hinweist.

Die Situation wird noch besorgniserregender, wenn man bedenkt, dass mehr als ein Viertel (28%) angibt, dass Mitarbeiterfehler bei der jüngsten Sicherheitsverletzung eine Rolle spielten. Unternehmen können so viele Sicherheitstools einsetzen, wie sie für richtig halten. Wenn jedoch ein Mitarbeiter einen Fehler macht und so Tür und Tor öffnet, dann wird ein Bot-basierter Angriff, ein Angriff auf die Software-Lieferketten oder ein anderer Angriff diese Schwachstelle schnell ausnutzen.

Welcher der folgenden Punkte trug in den letzten 12 Monaten zu einem Sicherheitsverstoß bei, bei dem eine Schwachstelle in einer der Anwendungen Ihres Unternehmens ausgenutzt wurde?

(n=541)



Bot-Angriffe

ERGEBNIS #6

Das breite Spektrum an Bot-Angriffen, die auf Anwendungen abzielen, erschweren es dem Verteidiger, diese abzuwehren.

Bei so viel Vielfalt in diesem Angriffsvektor ist es nicht verwunderlich, dass viele Unternehmen Schwierigkeiten haben, ihre Anwendungen gegen Bots zu schützen. Bot-Spam ist zwar eher eine lästige Attacke, wird aber oft als Deckmantel für bösartigere Angriffe verwendet und muss daher sehr ernst genommen werden. Je nach Häufigkeit und Authentizität kann Bot-Spam sehr schwierig abzuwehren sein und sich schnell von einem harmlosen Ärgernis zu einem betrieblichen Problem entwickeln.

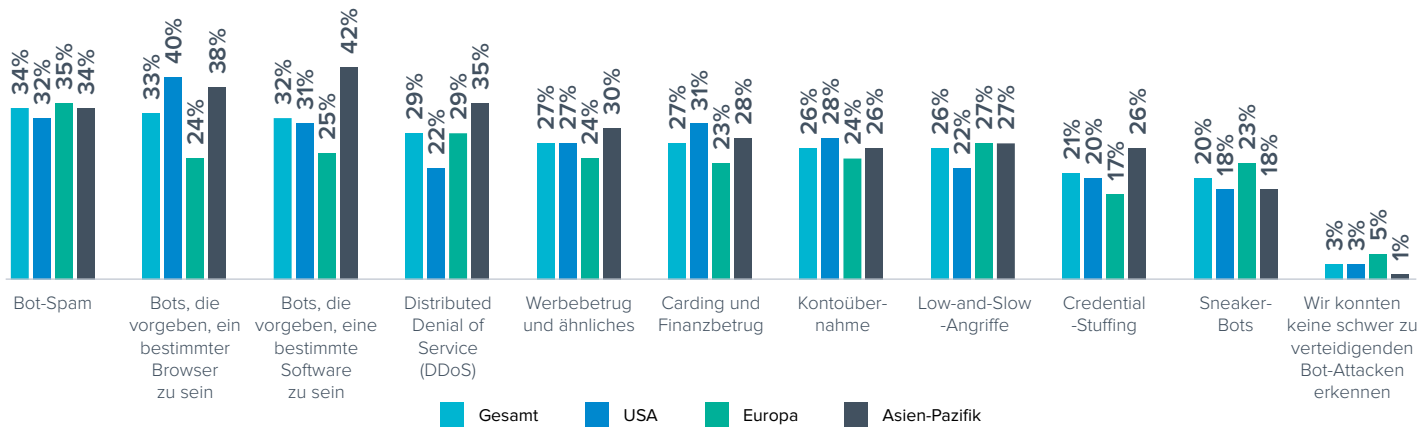
Bots mit Fokus auf Browser- und App-Spoofing stellen ebenfalls ein großes Problem dar. Diese Spoofs reichen von einfachen zu komplexen Varianten – ein Benutzer, der versucht, seinen echten Browser zu verbergen, bis hin zu Bots, die kompromittierte Versionen von Apps in Klickfarmen für Werbebetrug oder andere bösartige Zwecke ausführen.

Jeder dieser Bots, der in Verbindung mit einem anderen verwendet wird, erhöht die Chancen auf Erfolg. Multi-Vektor-Bot-Angriffe nach dem Schema „Low-and-Slow“ sind der Kern des Problems und trugen höchstwahrscheinlich zu erfolgreichen Sicherheitsverletzungen im vergangenen Jahr bei.

Es gibt einige interessante regionale Unterschiede. Asien-Pazifik ist die Region, in der DDoS-Angriffe die meiste Besorgnis hervorrufen, weit über den anderen Regionen und dem weltweiten Durchschnitt. Browser-Spoofing stand in den USA an erster Stelle, während Software-Spoofing im asiatisch-pazifischen Raum am häufigsten vorkam. In Europa sind Sneaker-Bots ein Thema.

Bei welchen Arten von Bot-Angriffen, die auf Anwendungen abzielen, hat Ihr Unternehmen Schwierigkeiten bei der entsprechenden Verteidigung?

(n=750)



Bot-Angriffe

ERGEBNIS #7

Das Verhindern, Erkennen und Identifizieren von Bots wird ein entscheidende Faktor für Anbieter sein, die Unternehmen in der Verteidigung von Bot-basierte Angriffe unterstützen wollen.

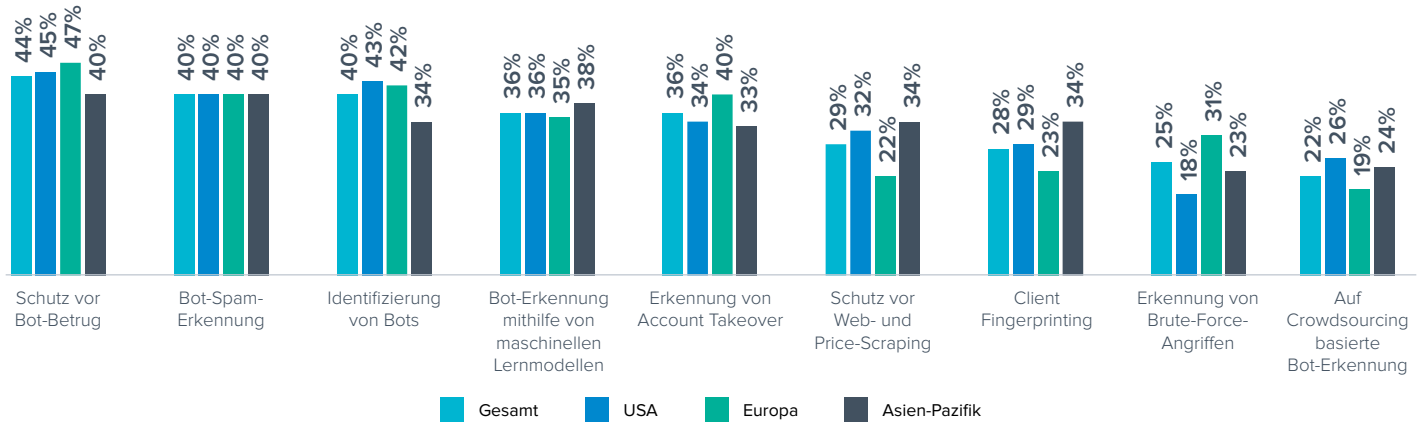
Es ist egal, ob Unternehmen mit Spam-Bots, betrügerischen Bots oder Bots im Bereich Software- und Browser-Spoofing zu kämpfen haben. Wenn es um die Abwehr dieses Angriffsvektors geht, sind bei allen Verbesserungen dringend nötig. Schließlich haben Bots im vergangenen Jahr am häufigsten zu erfolgreichen Angriffen auf Anwendungen beigetragen. Laut den Befragten gibt es drei eindeutige Bereiche, die bei der Wahl einer Sicherheitslösung zur Abwehr von Bots besonders wünschenswert sind: Betrugsprävention, Spam-Erkennung und Bot-Identifikation.

Diese Arten von Funktionen wären für die Abwehr der meisten Angriffstypen entscheidend. Allerdings wird jeder Anbieter, der diese Eigenschaften in einer einzigen Lösung bereitstellen kann, die bestehenden Bot-Schutz-Funktionen der meisten Unternehmen über die Maßen verbessern.

Bei diesen beiden zentralen Ergebnisse werden in Europa die Erkennung von Account Takeover und die Brute-Force-Erkennung durchweg als wichtigere Funktionen angesehen als in den USA und der Region Asien-Pazifik. Dies ist wahrscheinlich auf den Schutz der Privatsphäre und die Kosten eines Verstoßes gegen die DSGVO zurückzuführen. Die Tatsache, dass diese Angriffe von Low-and-Slow-Bots durchgeführt werden, erschwert zudem die Abwehr dieser Angriffe.

Welche Funktionen wären für Ihr Unternehmen bei der Auswahl einer Sicherheitslösung zum Schutz von Anwendungen vor Bot-Angriffen am wichtigsten?

(n=750)



API-Sicherheit

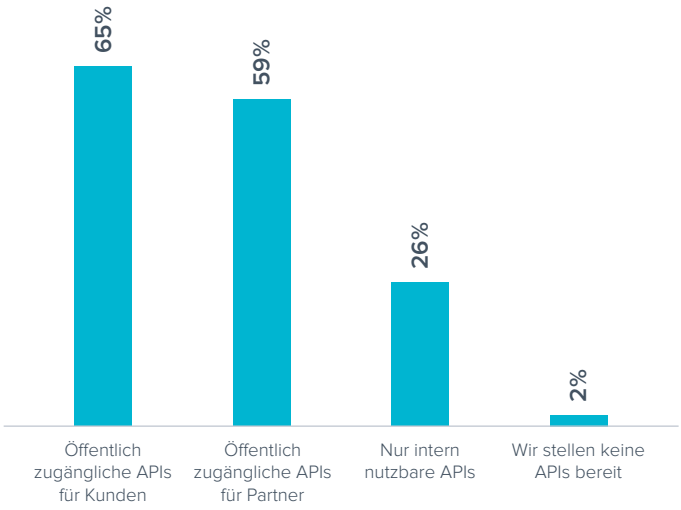
ERGEBNIS #8

Öffentlich zugängliche APIs sind alltäglich, sodass es zwingend erforderlich ist, sie richtig abzusichern.

Ein recht großer Prozentsatz der befragten Unternehmen setzt öffentlich zugängliche APIs für ihre Kunden (B2C) und Partner (B2B) ein, was dafür spricht, dass die meisten Unternehmen auf API-First-Entwicklung umstellen. APIs beschleunigen die Entwicklung neuer Versionen von Anwendungen erheblich und erweitern die Nutzbarkeit dieser Anwendungen, schaffen aber auch eine große neue Angriffsfläche für Cyberkriminelle. Eine mangelhafte API-Sicherheit ist nach wie vor eine der Hauptursachen für erhebliche Datenschutzverletzungen in den letzten zwei Jahren. Daher müssen Unternehmen sicherstellen, dass sie beim Schutz von APIs alle Bereiche abdecken.

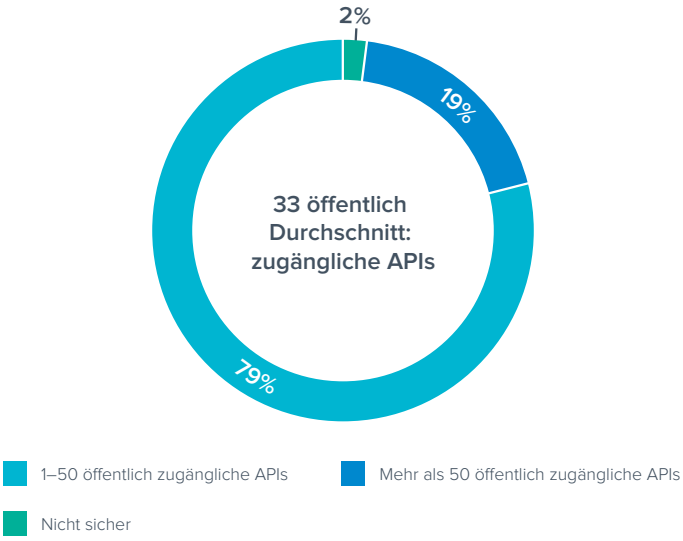
Welche Arten von APIs setzt Ihr Unternehmen ein?

(n=750)



Wie viele öffentlich zugängliche APIs setzt Ihr Unternehmen ein?

(n=642)



API-Sicherheit

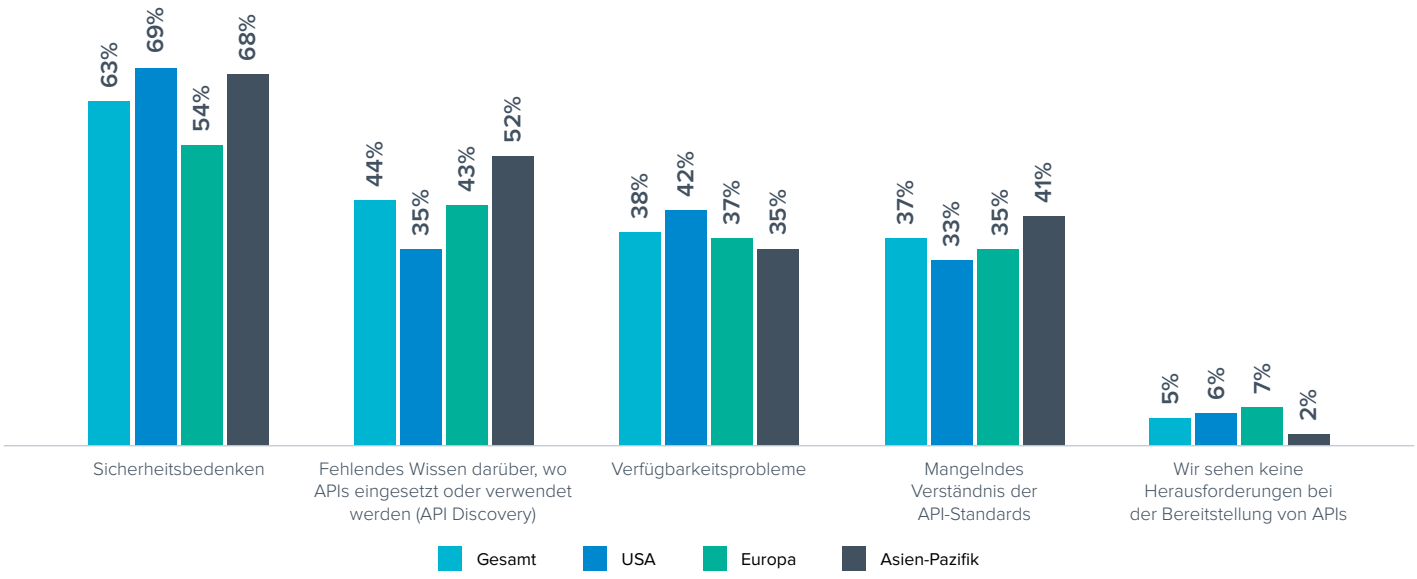
ERGEBNIS #9

Wenn es um APIs geht, stehen Sicherheitsbedenken an erster Stelle.

Es sollte nicht überraschen, dass bei Entscheidungsträgern in allen Regionen Sicherheitsbedenken, mit denen ihre Unternehmen bei der Bereitstellung von APIs zu kämpfen haben, ganz oben auf der Liste der Herausforderungen stehen. Eine API-basierte Anwendung ist wesentlich gefährdeter als eine herkömmliche webbasierte Anwendung, da sie mit direktem Zugriff auf alle sensiblen Daten der Anwendung bereitgestellt wird. Zweifellos tragen die genannten Wissenslücken in Bezug auf den Einsatz und die Verwendung von APIs sowie API-Standards zu diesen Bedenken bei.

Was sind die größten Herausforderungen für Ihr Unternehmen bei der Bereitstellung von APIs?

(n=728)

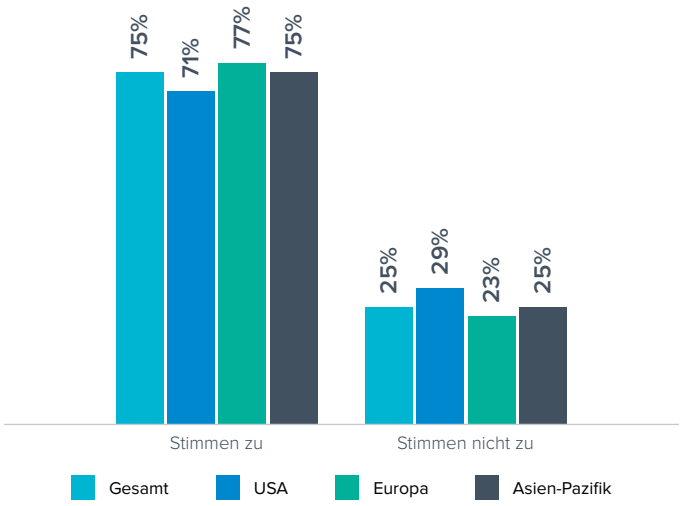


Unternehmen haben sich aufgrund der gebotenen Vorteile auf APIs gestürzt. Die Sicherheit hat damit jedoch nicht ganz Schritt gehalten. Dies bietet Angreifern mehr Möglichkeiten, Schwachstellen auszunutzen. Einige Gründe dafür sind ein mangelndes Verständnis der API-Sicherheit, Konfigurations-/ Mitarbeiterfehler sowie der Irrglaube, dass der Endanwender nicht weiß, dass im Hintergrund eine API läuft. Zudem sieht man in vielen, vielen Fällen, dass Anwendungsteams Test-APIs öffentlich und mit direktem Zugriff auf Produktionsdaten bereitstellen – ohne jegliche Sicherheit.

Wir haben die Umfrageteilnehmer auch gefragt, ob die Verwendung von APIs eine Sicherheitsherausforderung für ihre Organisation darstellt. 75% stimmten dem zu. Die meisten verstehen die Risiken von APIs ganz genau und das ist ein gutes Zeichen für die Zukunft der API-Sicherheit.

Die Verwendung von APIs hat für meine Organisation Sicherheitsprobleme mit sich gebracht

(n=728)



API-Sicherheit

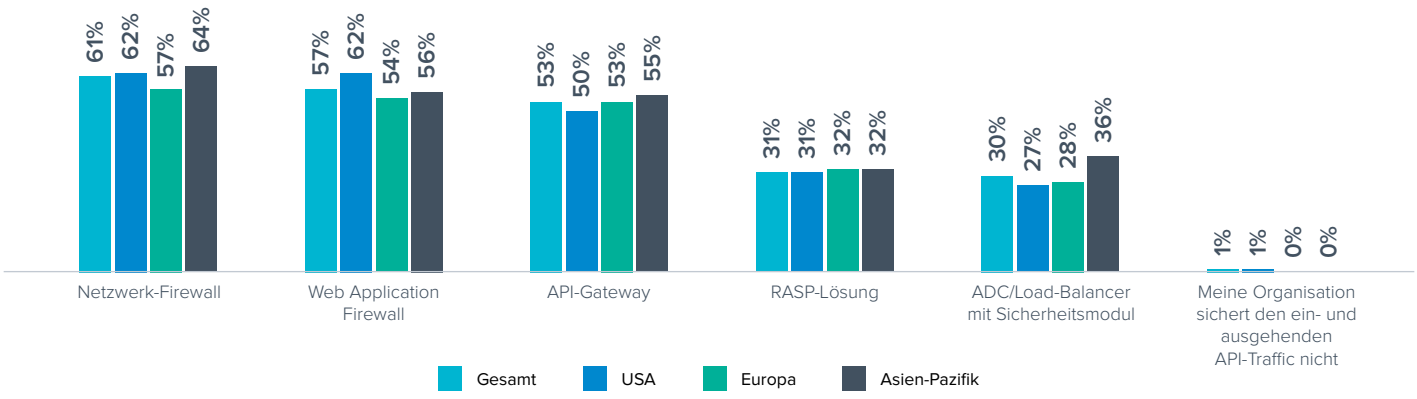
ERGEBNIS #10

Unternehmen haben eine Reihe von Lösungen zur Sicherung ihrer APIs eingeführt – sowohl für den eingehenden als auch für den ausgehenden und den Inter-API-Traffic. Die Mehrheit ist jedoch der Meinung, dass erhebliche Verbesserungen erforderlich sind.

Im Durchschnitt verwenden Unternehmen mehr als ein Tool, um ihren API-Datenverkehr zu sichern. Dies hat jedoch eindeutig nicht dazu beigetragen, die Bedenken bezüglich der API-Sicherheit zu zerstreuen. Zudem zeigt es, dass die aktuellen Lösungen für die Sicherung aller Arten von Datenverkehr entweder nicht auf dem gewünschten Niveau funktionieren oder nicht gut miteinander integriert sind, um APIs aus allen Richtungen zu sichern. Die API-Sicherheit ist immer noch ein Bereich, der sich in der Wachstumsphase befindet. Viele der Lösungen, die zum Schutz von APIs eingesetzt werden, bieten möglicherweise nicht genug Sicherheit. So können zum Beispiel Netzwerk-Firewalls nicht mehr als signaturbasierte Sicherheit, IP-basierte Ratenbegrenzung oder IP-basierte Zugriffskontrollen für APIs durchsetzen. Sie können keine positive Sicherheit für die API erzwingen oder eine API-Spezifikation importieren, um automatisch Kontrollen zu konfigurieren. API-Gateways erbringen sehr gute Leistungen im Bereich der API- und Traffic-Verwaltung, bieten aber unter Umständen keine vollständige API-Sicherheit in ihrem Funktionspaket. Es ist interessant zu beobachten, wie Unternehmen ihre mehrschichtigen Schutzmaßnahmen für APIs weiterentwickeln. Fazit ist jedoch, dass es noch viel Raum für Verbesserungen gibt.

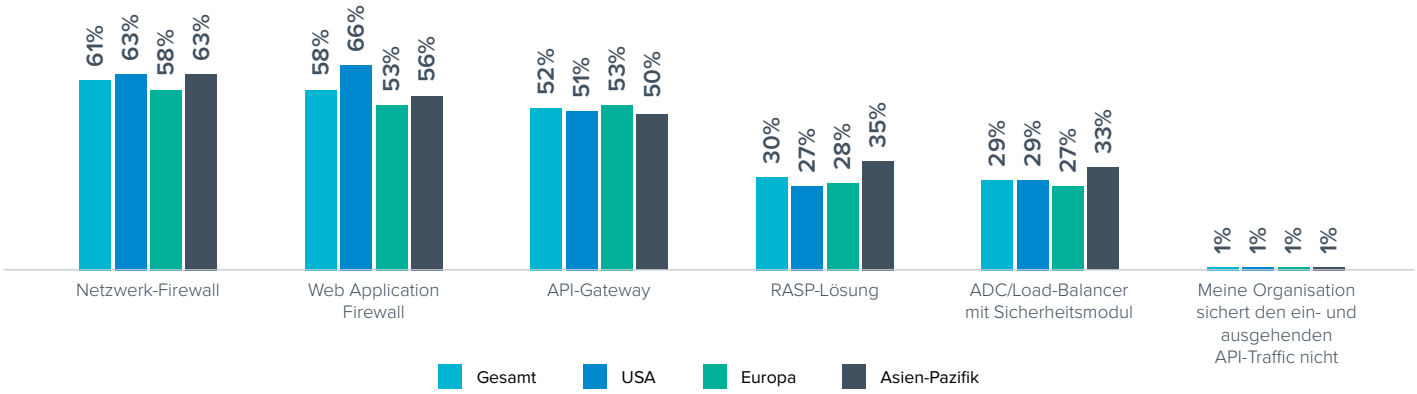
Welche Lösungen verwendet Ihr Unternehmen zur Sicherung des ein- und ausgehenden API-Traffics?

(n=728)



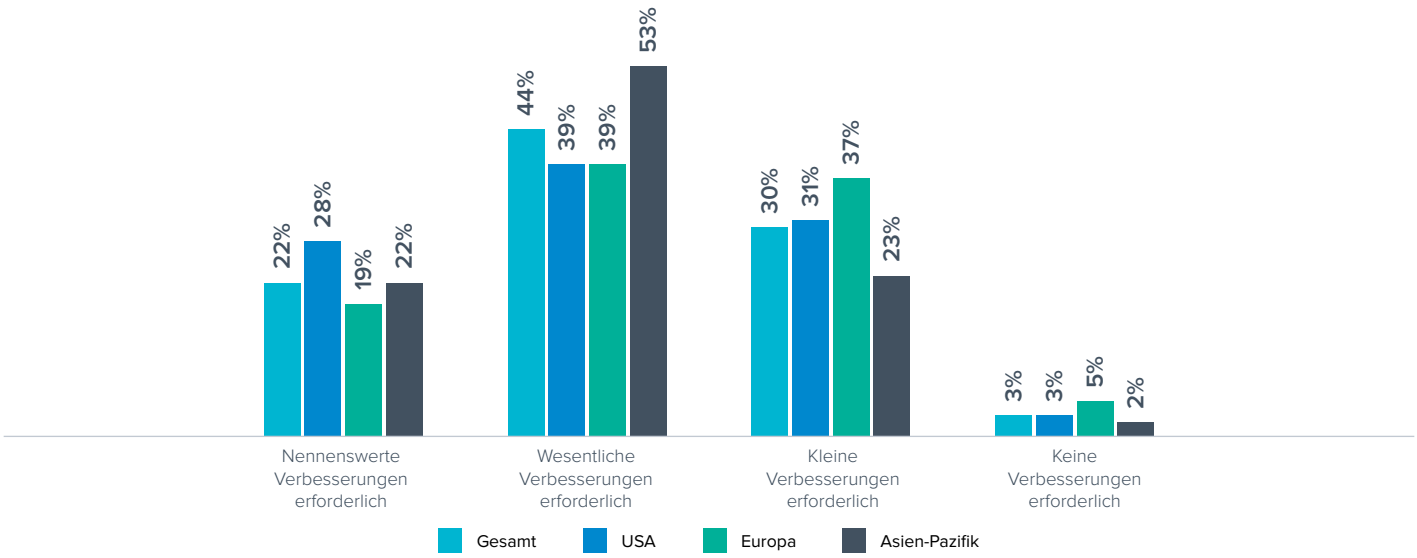
Welche Lösungen nutzt Ihr Unternehmen zur Absicherung des ein- und ausgehenden API-Traffics (Anwendung-Anwendung und API-API)?

(n=728)



Welchen Verbesserungsbedarf sehen Sie in Ihrer Organisation, wenn es um API-Sicherheit geht?

(n=728)



Angriffe auf die Software-Lieferketten

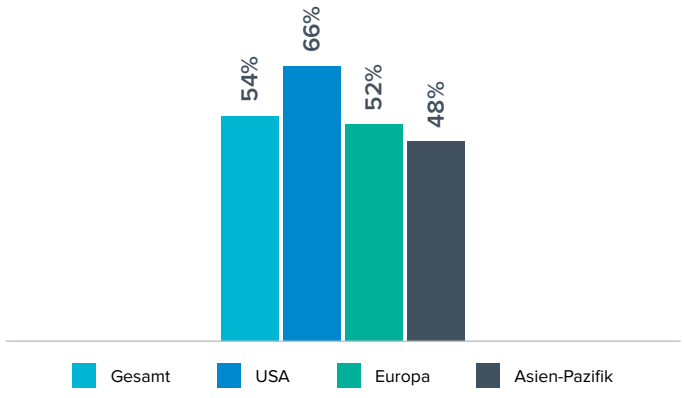
ERGEBNIS #11

Die Verwendung von Skripten von Drittanbietern für Web-Anwendungen ist ziemlich weit verbreitet. Dabei verwenden Unternehmen unterschiedliche Methoden, um Skripte an einen Browser auszuspielen.

Das Streben nach Effizienz bei der Anwendungsentwicklung ist erneut offensichtlich, da mehr als die Hälfte der Unternehmen im Durchschnitt vorgefertigte Skripte von Drittanbietern für Webanwendungen verwenden. Die Sicherheit sollte bei der Verwendung von Drittanbieter-Code ein großes Anliegen sein. Dies gilt insbesondere dann, wenn der Code direkt von der Quellplattform, wie z. B. GitHub, an einen Browser geliefert wird. Wenn der Code manipuliert wurde, könnte ein Angriff auf die Software-Lieferketten, wie z. B. Magecart, unmittelbar bevorstehen. Unternehmen sollten bei diesem Ansatz zur Anwendungsentwicklung vorsichtig sein.

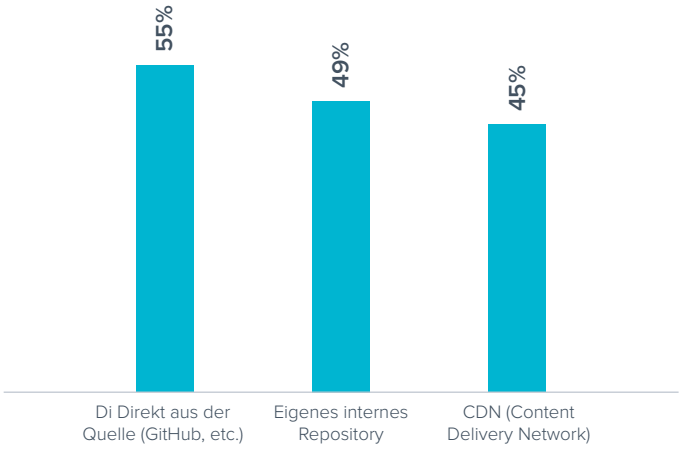
Wie viel Prozent der Webanwendungen Ihres Unternehmens verwenden schätzungsweise Skripte von Drittanbietern?

(n=750)



Auf welche Weise spielen die Websites Ihres Unternehmens clientseitige Skripte an Browser aus?

(n=750)



Angriffe auf die Software-Lieferketten

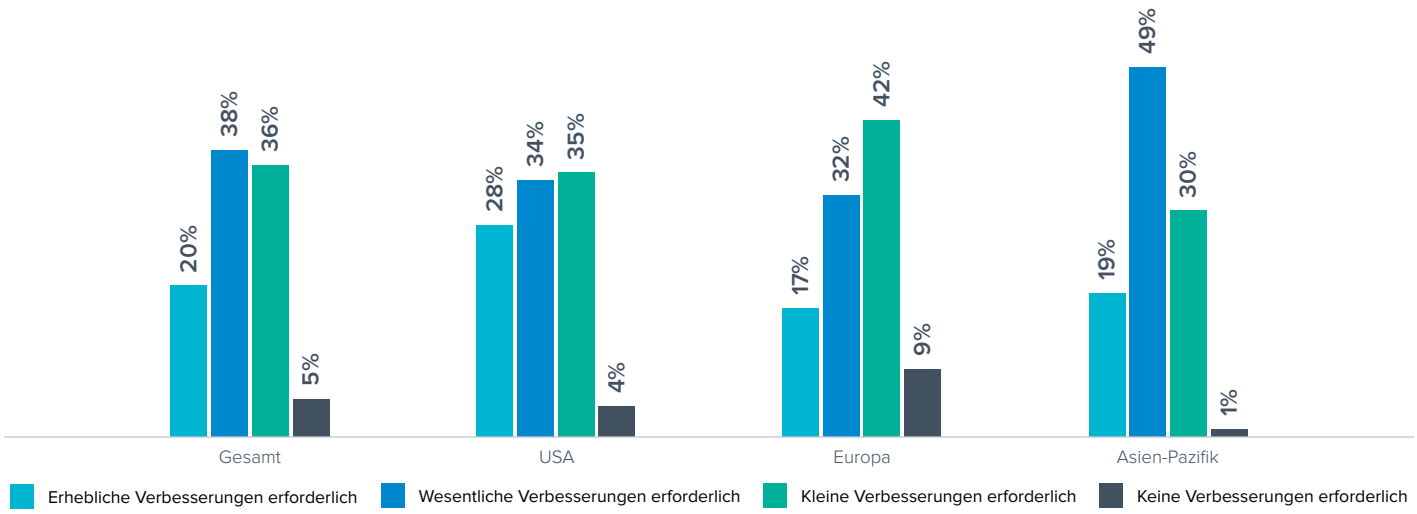
ERGEBNIS #12

Unabhängig von den Technologien, die zum Schutz vor Angriffen auf die Software-Lieferketten eingesetzt werden, sind sich die Befragten durchaus bewusst, dass ihr Unternehmen in diesem Bereich Verbesserungen vornehmen muss.

Angriffe auf die Software-Lieferketten sind immer ausgereifter geworden. Einige Skripte sind sogar in der Lage, die Ausführung von bösartigem Code zu vermeiden, wenn sie erkennen, dass ein Web-Schwachstellen-Scanner ausgeführt wird. Das macht eine wirksame Abwehr extrem schwierig. Dies fügt der sich ständig weiterentwickelnden Bedrohungslandschaft eine weitere Ebene der Komplexität hinzu. Obwohl Unternehmen eine Reihe von Technologien einsetzen, um sich zu schützen, scheint es, dass dieser Angriffsvektor, ähnlich wie Bot-Angriffe, immer einen Schritt voraus ist. Und mit Blick auf die jüngsten öffentlichkeitswirksamen Sicherheitsverletzungen ist den meisten Regionen klar, dass in Bezug auf Angriffe auf die Software-Lieferketten erhebliche Verbesserungen erforderlich sind.

Welcher Verbesserungsbedarf besteht in Ihrem Unternehmen, wenn es um die Abwehr von Angriffen auf die Software-Lieferketten geht?

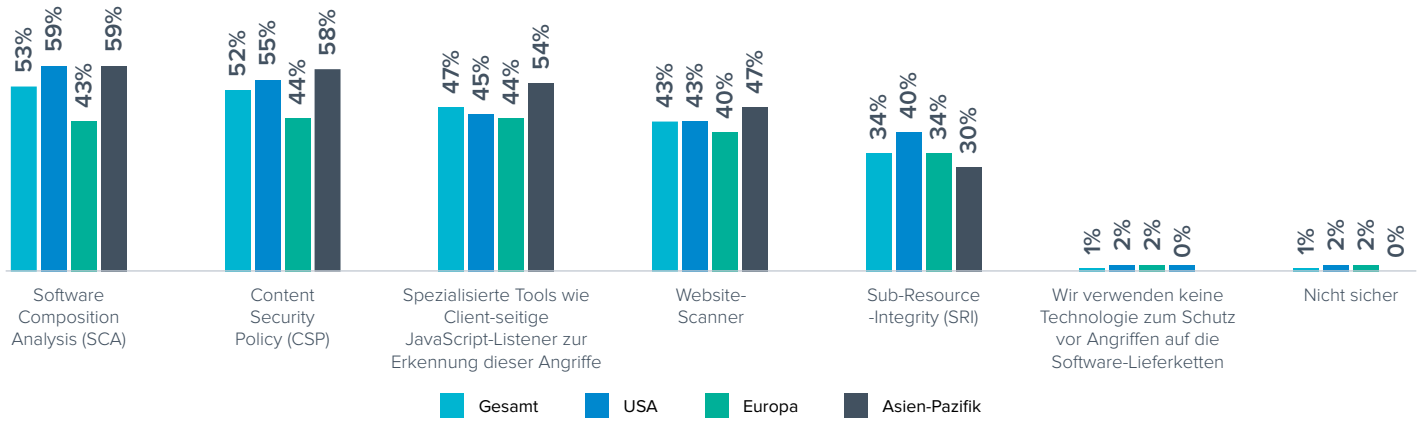
(n=750)



Für die Abwehr von Angriffen auf die Lieferkette gibt es relativ standardisierte Schutzmaßnahmen. Mehr als in anderen Regionen nutzen Befragte aus dem asiatisch-pazifischen Raum spezialisierte Tools zur Erkennung von Angriffen, einschließlich Client-seitiger JS-Listener. Solche Listener haben eine bessere Chance, die fortgeschritteneren Angreifer zu erkennen als Website-Scanner. Website-Scanner sind die viertbeliebteste Technologie auf dieser Liste, aber sie lassen sich leicht umgehen, wie der von Visa entdeckte Baka-Skimmer beweist. Die Einrichtung und Wartung der Sub-Resource-Integrity (SRI) gestaltet sich schwierig, was ein Grund für ihre geringe Popularität sein könnte.

Welche Technologien setzt Ihr Unternehmen zum Schutz vor Angriffen auf die Software-Lieferketten ein?

(n=750)



Fazit

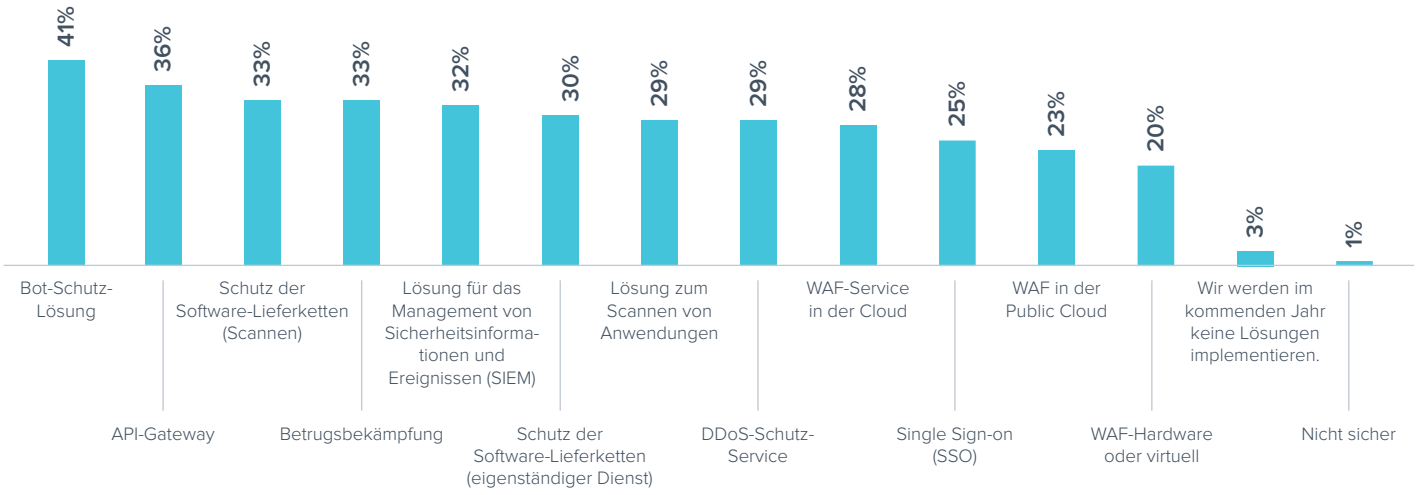
Bei einem so hohen Anteil von Unternehmen, die in den letzten 12 Monaten mehrfach über ihre Webanwendungen angegriffen wurden, ist es klar, dass mehr getan werden muss, um sich gegen diese Bedrohungen zu schützen. Dies gilt insbesondere angesichts neuerer Bedrohungen wie Bot-Angriffe, API-Angriffe und Angriffe auf die Lieferkette.

Unternehmen scheinen sich dessen durchaus bewusst zu sein, denn viele planen für das kommende Jahr den Einsatz neuer Lösungen wie Bot-Schutz (41%), API-Gateways (36%) und Schutzmaßnahmen für die Software-Lieferketten (Scanning) (33%).

Es ist ein gutes Zeichen, dass sich Unternehmen bemühen, diese Lücken zu schließen. Je mehr Lösungen sie jedoch hinzufügen, desto komplexer wird die Anwendungssicherheit. Um effektiven Schutz zu bieten, muss eine Anwendungssicherheitslösung eine Plattform sein, die Kunden vor all diesen Angriffsvektoren schützen kann. Ein plattformbasierter Ansatz für die Anwendungssicherheit kann einen leistungsstarken Schutz sowohl gegen herkömmliche als auch gegen neue Bedrohungen bieten und gleichzeitig eine einfache Bedienung und Verwaltung gewährleisten.

Welche der folgenden Lösungen wird Ihr Unternehmen im nächsten Jahr einsetzen?

(n=750)



Über Barracuda

Wir von Barracuda wollen die Welt sicherer machen.

Wir sind der Überzeugung, dass jedes Unternehmen Zugang zu Cloud-fähigen Sicherheitslösungen auf höchstem Niveau verdient, die einfach zu kaufen, zu implementieren und zu verwenden sind. Wir schützen E-Mails, Netzwerke, Daten und Anwendungen mit innovativen und anpassungsfähigen Lösungen, die mit den Unternehmen unserer Kunden wachsen.

Mehr als 200.000 Unternehmen weltweit vertrauen auf den Schutz durch Barracuda – auf eine Art und Weise, von der sie vielleicht nicht einmal wissen, dass sie gefährdet sind. Somit können sie sich darauf konzentrieren, ihr Geschäft auf die nächste Stufe zu bringen.

Weitere Informationen finden Sie unter barracuda.com.

Barracuda
Your journey, secured.