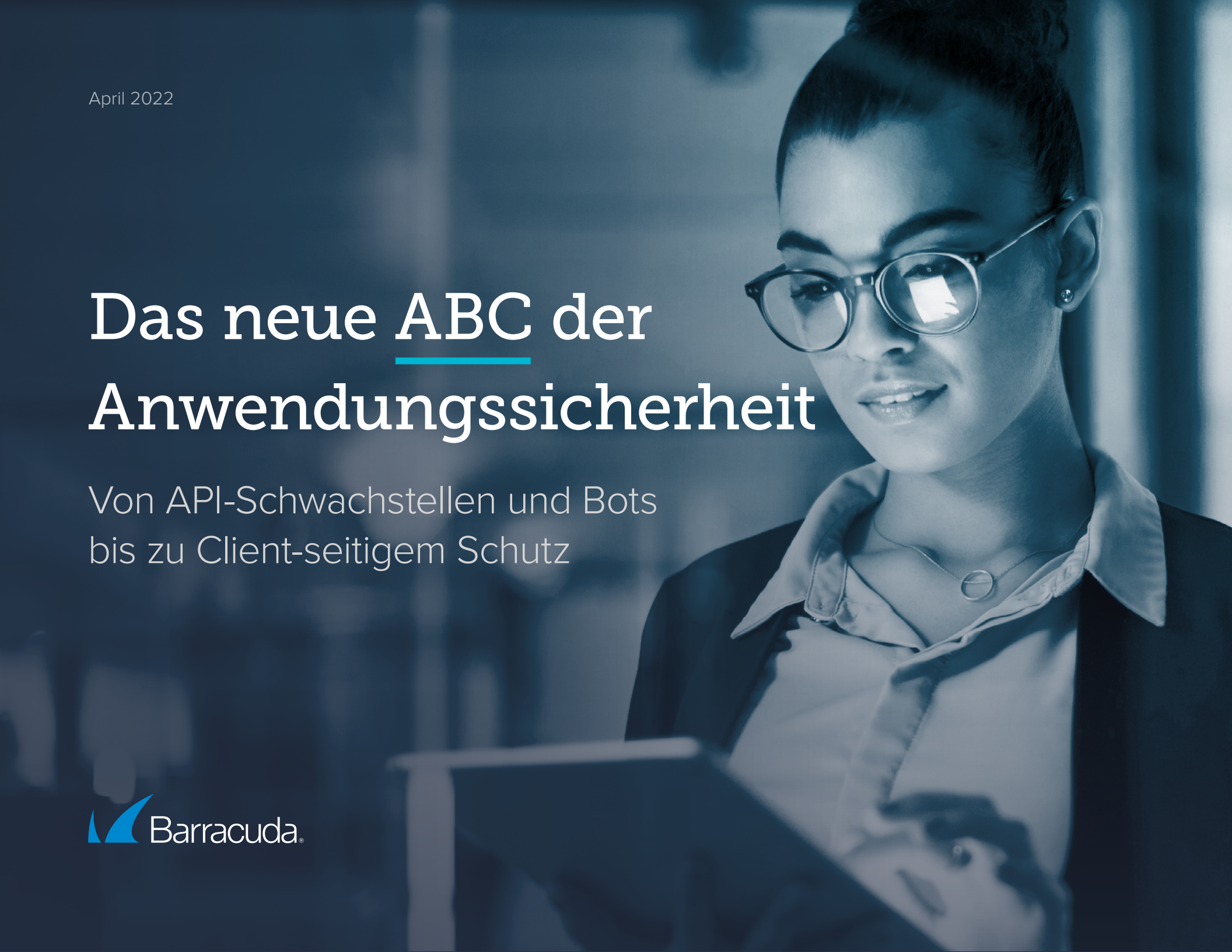
April 2022

Das neue ABC der Anwendungssicherheit

Von API-Schwachstellen und Bots bis zu Client-seitigem Schutz



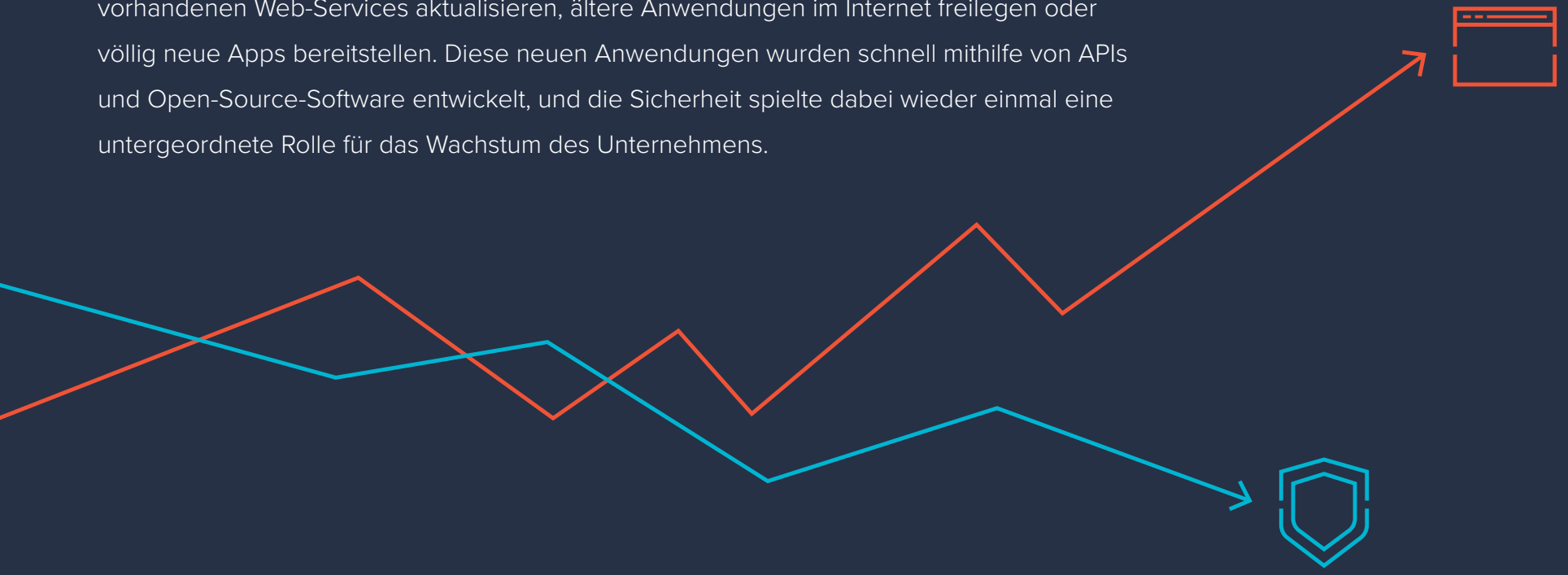
Barracuda

Inhalt

Barracuda

Einführung: Neuere, gefährlichere Angriffsvektoren

Anwendungen sind die Bausteine für die Abläufe digitaler Unternehmen und ihrer Interaktionen mit ihren Endbenutzern und Kunden. Der Umstieg auf externes Arbeiten im Jahr 2020 hat die Bedeutung von Web-Apps erhöht, und viele Unternehmen mussten möglichst schnell ihre vorhandenen Web-Services aktualisieren, ältere Anwendungen im Internet freilegen oder völlig neue Apps bereitstellen. Diese neuen Anwendungen wurden schnell mithilfe von APIs und Open-Source-Software entwickelt, und die Sicherheit spielte dabei wieder einmal eine untergeordnete Rolle für das Wachstum des Unternehmens.



Barracuda

Es gab schon immer eine Reihe an Herausforderungen für Unternehmen, was die Anwendungssicherheit angeht. Anwendungen sind ein Hauptangriffsvektor für Datenschutzverletzungen – wie seit einigen Jahren durch den Verizon Data Breach Investigation Report bestätigt wird – und einer der beiden Hauptgründe für Datenschutzverletzungen. Angefangen mit den traditionellen Angriffen auf Webanwendungen, wie SQL-Injection, Cross-Site-Scripting und Command-Injection, haben sich diese Angriffe auch auf APIs und mobile Anwendungen ausgeweitet.

In den letzten Jahren haben sich die Bedrohungen für Anwendungen vervielfacht, und es sind neue, gefährlichere Angriffsvektoren entstanden. Die am schnellsten wachsenden Angriffsvektoren sind nun API-Schwachstellen, automatisierte Bot-Angriffe und Client-seitige Angriffe. Tatsächlich nannten die für den Barracuda-Bericht Application Security – Ein Überblick befragten Personen Bot-Angriffe, Schwachstellen in Webanwendungen, Angriffe auf die Software-Lieferkette und mangelhafte API-Sicherheit als Hauptgrund für eine erfolgreiche Sicherheitsverletzung in ihrem Unternehmen.

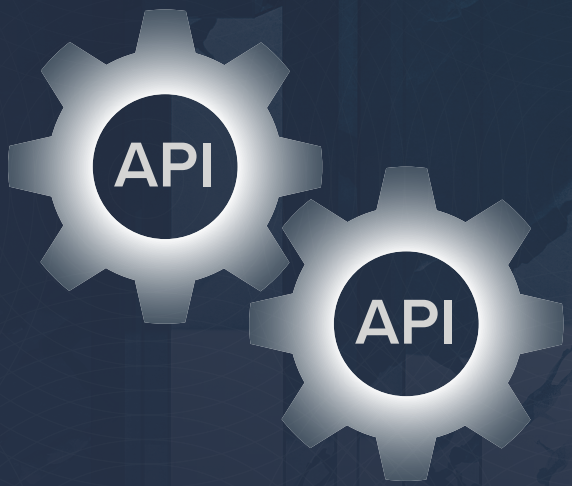
Die Zahl der Schwachstellen und Sicherheitsverletzungen, die auf APIs und Client-seitige Angriffe zurückzuführen sind, ist exponentiell gestiegen, und einige dieser Sicherheitsverletzungen wie jene bei T-Mobile und British Airways haben aus den falschen Gründen Schlagzeilen gemacht. Client-seitige Angriffe, auch als Supply-Chain-Angriffe bekannt, wurden erstmals 2018 entdeckt und als Magecart bezeichnet, da sie hauptsächlich auf Magento-basierte Online-Shops abzielten. Die Angreifer identifizierten zunächst JavaScript von Drittanbietern, das häufig auf Seiten mit Bezahlvorgängen verwendet wurde. Anschließend hackten sie diese Quelldateien und fügten ihren Code zum Abgreifen von Karten ein. Beim anschließenden Aufruf der Website durch einen Benutzer wurde das nun bösartige JavaScript geladen und zum Diebstahl der Anmeldedaten des Benutzers verwendet.

Bot-Angriffe haben sich auf andere Weise auf Unternehmen ausgewirkt. Ein großer Angriff ist beispielsweise der automatisierte Kauf von Gegenständen in limitierter Auflage für den Weiterverkauf. Bekannt als Scalping-Angriffe, führen diese zu Engpässen für tatsächliche Kunden, wie z. B. die Knappheit an PlayStation 5. Bots führen jetzt auch eine Vielzahl von Angriffen durch, von denen Account Takeover-Angriffe und DDoS-Angriffe die größten Schäden verursachen.

Dieses E-Book befasst sich eingehend mit diesen drei kritischen Angriffsvektoren – API-Schwachstellen, Bot-Angriffe und Client-seitige Angriffe – und zeigt auf, wie Unternehmen die Lücken in ihrer Anwendungssicherheit schließen und sich vor diesen sich entwickelnden Bedrohungen schützen können.

A steht für API-Sicherheit

Seit vielen Jahren werden APIs im Backend von Geschäftsanwendungen zur Maschine-zu-Maschine-Kommunikation eingesetzt. APIs sind heute allgegenwärtig und ermöglichen die meisten der Anwendungen, die wir im Alltag nutzen. Die meisten Mobil- und Webanwendungen, die wir bei der Arbeit und in der Freizeit nutzen, setzen APIs ein. Sie sind das Herzstück von Unternehmen, treiben moderne digitale Plattformen an und ermöglichen die digitale Transformation.



Barracuda

Unternehmen haben sich für die Entwicklung von „API First“-Applikationen entschieden, weil sie mit dieser Methode innovativ sein und schnell auf dem Markt sein können. APIs ermöglichen eine schnelle Bereitstellung, wenn sie mit agilen und DevOps-Praktiken verwendet werden, durch die Entwickler schnell neue Funktionen für Web- und Mobilanwendungen erstellen und veröffentlichen können. Mit zunehmender API-Nutzung werden sie zur Grundlage für wichtige Services für die Anwendungen, die sie ermöglichen, und der Zugriff auf kritische Daten hat sich wiederum exponentiell erhöht.

Die zunehmende Verbreitung von APIs und ihr direkter Zugang zu wichtigen Daten sind der Grund, warum sie zu einem bevorzugten Ziel für Angreifer wurden. APIs sind auf Automatisierung ausgelegt, und das macht das Auffinden und Ausnutzen unsicherer APIs für Angreifer sehr profitabel. Mit automatisierten Angriffen können Cyberkriminelle Daten schneller und einfacher ausfiltern als mit einer Web-Applikation. API-basierte Anwendungen kodieren auch ihre Geschäftslogik in der Anwendung selbst, im Gegensatz zu traditionellen Anwendungen, bei denen diese Logik im Backend-Server verborgen ist. Dadurch kann ein Angreifer den Anwendungsverkehr leicht ausspähen, um API-Endgeräte zu identifizieren und Angriffe gegen sie durchzuführen.

Die Tatsache, dass APIs ein wichtiges neues Ziel für Angreifer sind, wird durch den BugCrowd PriorityOne Bericht für 2021 bestätigt. Darin wird offengelegt, dass sich die Zahl der API-Schwachstellen in einem einzigen Jahr verdoppelt hat. Diese Schwachstellen werden in den kommenden Jahren noch schneller zunehmen und sich zu einem der wichtigsten Vektoren für Anwendungsangriffe entwickeln.

API-Sicherheitslücken haben

sich in einem

Jahr verdoppelt

Barracuda

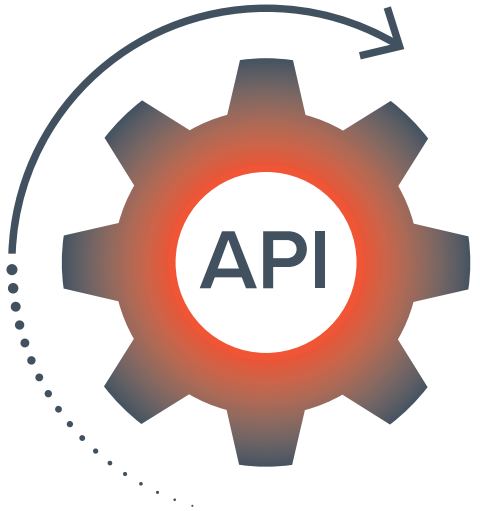
Beispiel: Experian-API exponierte Kreditauskünfte

Ein Rechercheur entdeckte kürzlich eine große API-Schwachstelle beim Online-Preisvergleich von Krediten für Studierende. Als er die Website eines Kreditgebers besuchte, bot dieser an, seine Kreditwürdigkeit anhand seines Namens, seiner Adresse und seines Geburtsdatums zu überprüfen. Als Rechercheur sah er sich den dahinter laufenden Code an und stellte fest, dass es sich um einen API-Aufruf von Experian handelte. Die verwendete API ermöglichte es Kreditgebern, automatisierte Abfragen zu senden und FICO-Kreditauskünfte von der Kreditauskunftei abzurufen.

Der Rechercheur stellte fest, dass auf die Experian-API direkt, ohne irgendeine Art von Anwendungssicherheit, zugegriffen werden konnte, und durch die einfache Eingabe von Nullen in das Feld für das Geburtsdatum konnte er die Kreditwürdigkeit eines jeden abrufen. Anschließend entwickelte er ein praktisches Tool zur Automatisierung der Suchvorgänge. Die API resultierte zusätzlich zu den Kreditauskünften auch vier „Risikofaktoren“, die den Grund für den Wert der Kreditauskunft erklären könnten.

Als er Experian davon in Kenntnis setzte, entfernte das Unternehmen einfach den API-Zugang für diesen einzelnen Endpunkt.

Die Gefahr dieser Exposition wird durch das von dem Rechercheur entwickelte Instrument deutlich. Er war Rechercheur und meldete das Problem an Experian, damit es behoben wird. Wenn dieser API-Endpunkt jedoch von einem böswilligen Akteur entdeckt worden wäre, hätte dieser ihn leicht dazu verwenden können, die Kreditwürdigkeit von Personen zu erfassen, deren Name und Adresse öffentlich bekannt sind, was möglicherweise erheblichen Schaden verursacht hätte. Es ist unbekannt, ob der API-Aufruf zu einem sogenannten „Hard Pull“ (negative Auswirkung auf die Bonität) oder einem „Soft Pull“ (bonitätsneutral) geführt hat und wie sich die Abfrage der Kreditauskunft auf die Bonität der Person ausgewirkt hätte.



Beispiel: Brute-Force-Angriffe auf private Meeting-Passwörter auf Zoom

Zoom-Meetings waren standardmäßig durch ein sechsstelliges numerisches Passwort geschützt. Das bedeutet, dass für jedes Meeting eines von 1 Million möglichen Passwörtern in Gebrauch war. Ein Rechercheur entdeckte, dass diese Passwörter anfällig für Brute-Force-Angriffe waren, was zu Zoom Bombing und ähnlichen Angriffen führte.

Als Zoom noch über ein numerisches Passwort verfügte, konnte ein Benutzer den Link zum Zoom-Meeting zum Öffnen einer Webseite verwenden, die zur Eingabe des Passworts aufforderte. Zu dem Zeitpunkt, an dem der Benutzer die erforderlichen Felder ausgefüllt und die Eingabetaste gedrückt hat, konnten die Backend-API-Interaktionen beobachtet werden, um die Schwachstelle zu erkennen.

Das Wichtigste, was wir an diesem Prozess feststellten, war, dass keine Ratenbegrenzung aktiviert war. Das bedeutet, dass der Rechercheur in der Lage war, kontinuierlich Passwörter auszuprobieren. Nach 43.164 Versuchen, die etwa 29 Minuten dauerten, konnte er das richtige Passwort herausfinden – das entspricht einer Rate von etwa 25 Passwörtern pro Sekunde.

Würden mehrere parallele Rechner für einen Angriff verwendet, könnte das Passwort sehr schnell geknackt werden.

Dieser Hack hatte massive Auswirkungen. Angesichts der Anzahl hochrangiger Regierungsbehörden und ähnlicher Organisationen, die Zoom nutzen, hätten böswillige Akteure aufgrund dieser Problematik in Meetings eindringen, sie belauschen und schwere Schäden anrichten können. Der Rechercheur übermittelte diese Informationen an Zoom, das mehrere Änderungen zur Behebung des Problems implementierte.

Neben der fehlenden Ratenbegrenzung wurde hier noch ein weiteres Problem entdeckt – das Fehlen einer ordnungsgemäßen Protokollierung und Überwachung, mit der das Zoom-Team relativ leicht von solchen Versuchen hätte alarmiert werden können.

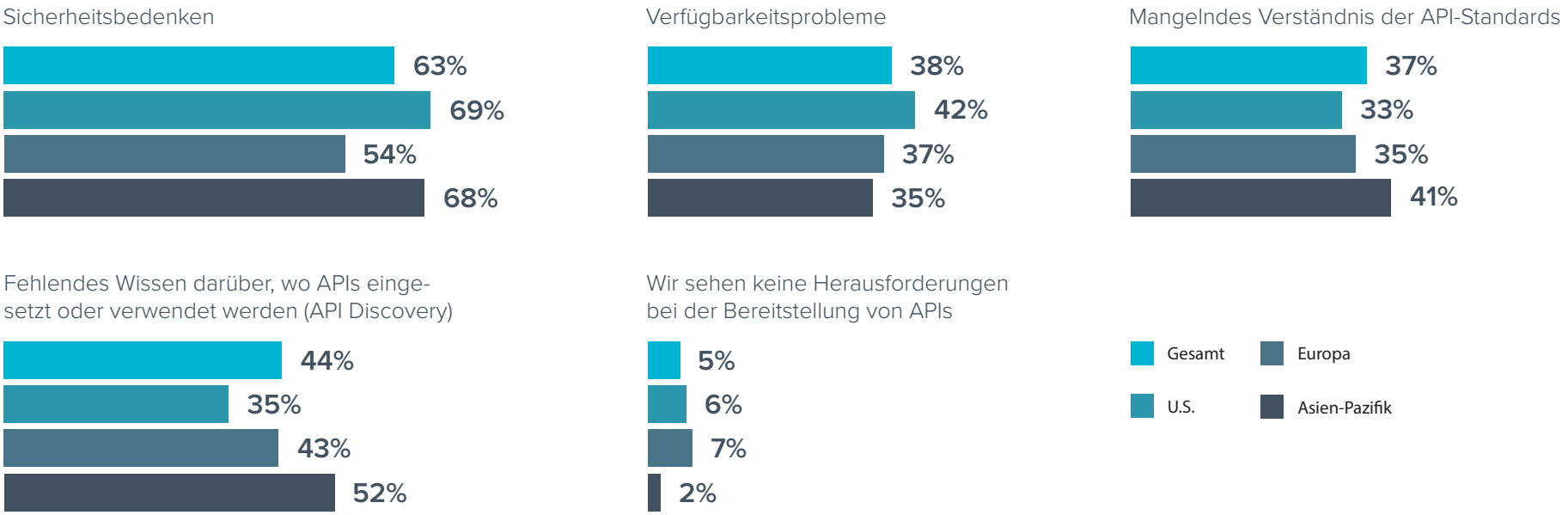
Barracuda

Was Fachleute für Anwendungssicherheit sagen

Angesichts des Ausmaßes, den ein API-Sicherheitsverstoß haben kann, ist es kein Wunder, dass die API-Sicherheit für Fachleute oberste Priorität hat. In der jüngsten Umfrage von Barracuda unter Fachleuten für Anwendungssicherheit befragten wir sie zu den größten Herausforderungen bei der Bereitstellung von APIs – und die Security war die größte Problematik. Dies wird auch durch die von Open Web Application Security (OWASP) Top 10 der API-Sicherheit veröffentlichte Liste mit den einzigartigen Schwachstellen und Sicherheitsrisiken von APIs bestätigt.

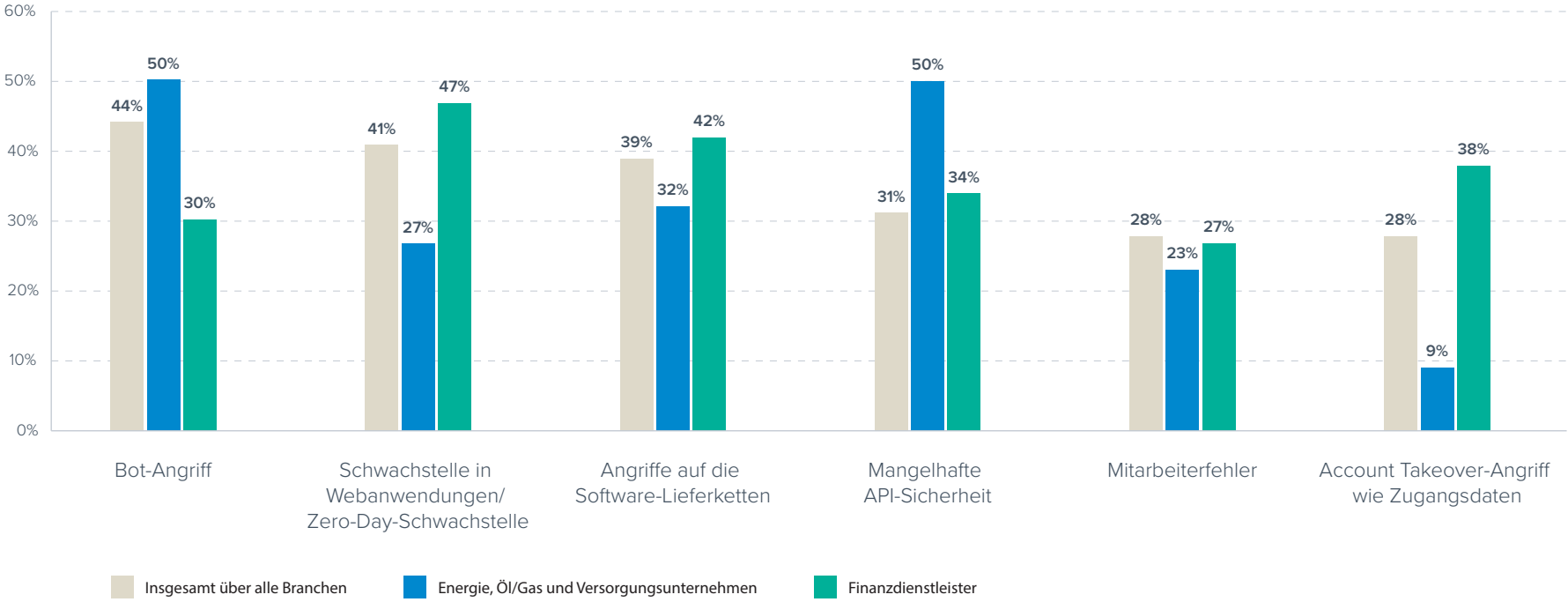
Was sind die größten Herausforderungen für Ihr Unternehmen bei der Bereitstellung von APIs?

(n=728)



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?

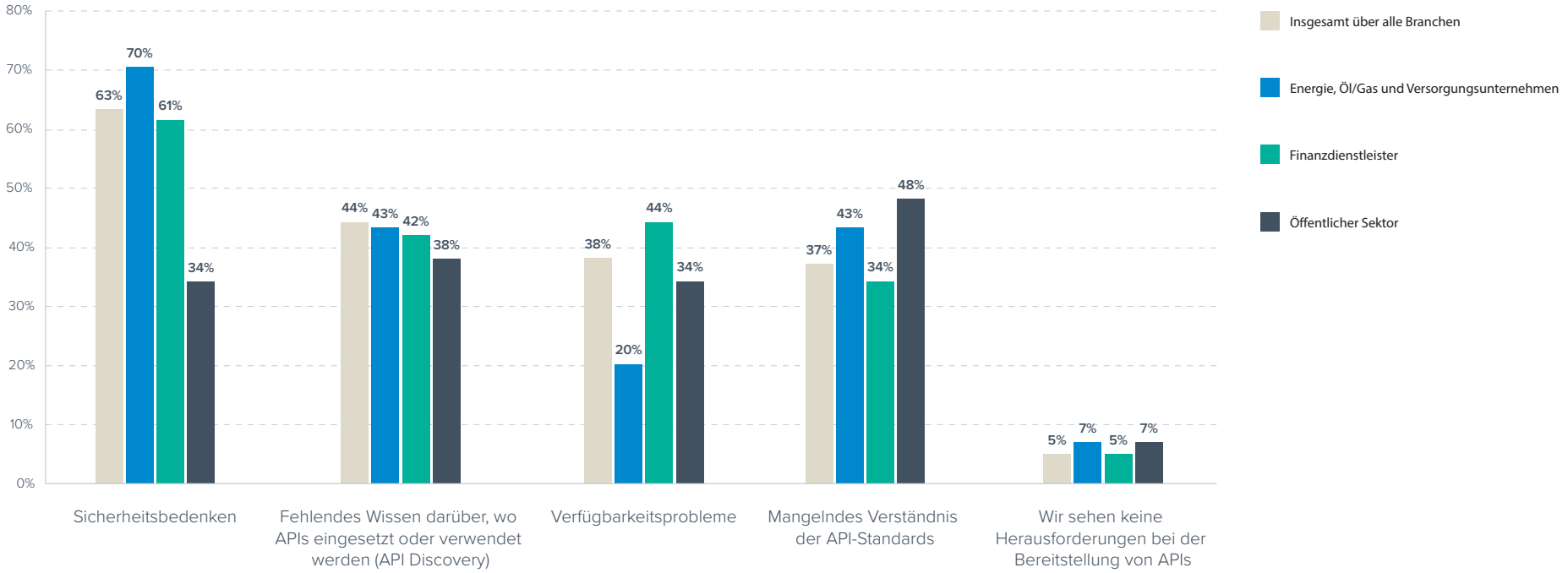
(n=541)



Den Umfrageergebnissen zufolge ist die Energie-, Öl-, Gas- und Versorgungsbranche am ehesten von einer API-Sicherheitslücke betroffen. Während die Branche vor allem wegen gezielter Ransomware- und IoT-Angriffe in den Schlagzeilen ist, sind ihre APIs – von denen viele öffentlich zugänglich sind – ebenfalls einer immensen Angriffsgefahr ausgesetzt. Die Befragten aus dem Finanzdienstleistungssektor, einer Branche, in der APIs der Lebensnerv automatisierter Transaktionen sind, nannten API-Verletzungen ebenfalls als Hauptgrund für Sicherheitsverletzungen.

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

(n=728)

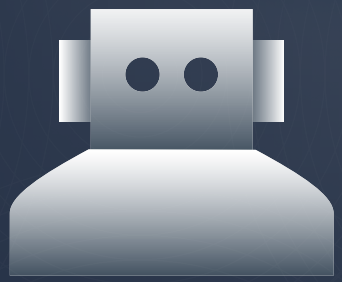


Der öffentliche Sektor ist den Antworten zufolge der unwahrscheinlichste jener, die sich mit Herausforderungen bei der API-Einführung auseinandersetzen. Interessanterweise ist sein größtes Problem das „mangelnde Verständnis von API-Standards“, und die API-Sicherheit steht an dritter Stelle, im Gegensatz zu den anderen Sektoren, die die API-Sicherheit fast durchgängig als größtes Problem betrachten. Im Vergleich dazu sind die Bereiche Energie, Öl, Gas und Versorgungsunternehmen sowie das verarbeitende Gewerbe am meisten um die API-Sicherheit besorgt.

Es ist nicht überraschend, dass die Befragten von Finanzdienstleistern in den verschiedenen Sektoren die größten Sorgen hinsichtlich Ausfallzeiten hatten. Die Befragten aus der Energie-, Öl-, Gas- und Versorgungsbranche waren am wenigsten über die Einhaltung von Standards besorgt, was in gewisser Weise besorgniserregend ist, da die Einhaltung von Standards bei der Erstellung von APIs eine bessere Sicherheit ermöglicht.

B steht für Bot-Schutz

In den letzten Jahren hat der automatisierte Bot-Traffic stark zugenommen. Sie wurden einst hauptsächlich von Suchmaschinen eingesetzt, doch nun haben Bots zahlreiche Aufgaben – gute wie schlechte. Die gutartigen Bots sind Crawler von Suchmaschinen, Social-Media-Netzwerken, Aggregatoren, Monitoring-Bots etc. Diese Bots befolgen die Regeln der Website-Inhaber, die in der Datei robots.txt festgelegt werden, veröffentlichen Methoden zur Validierung ihrer Identität und arbeiten so, dass die von ihnen besuchten Websites und Apps nicht überlastet werden.

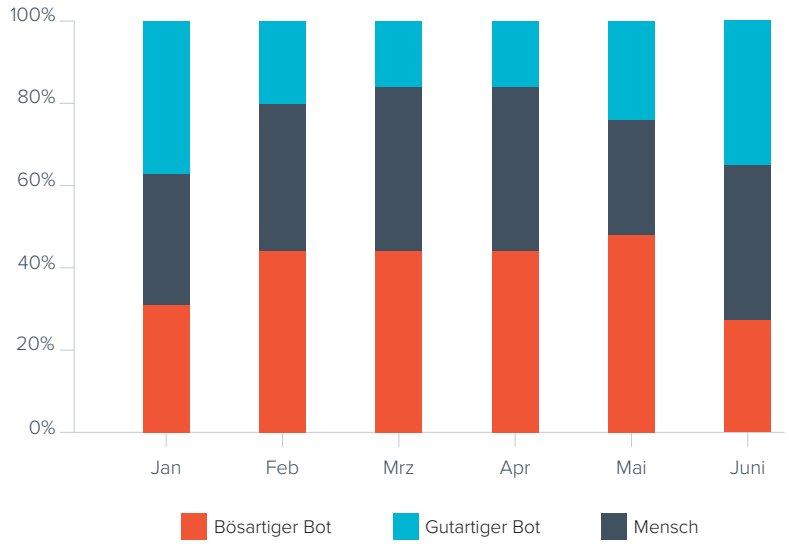


Barracuda

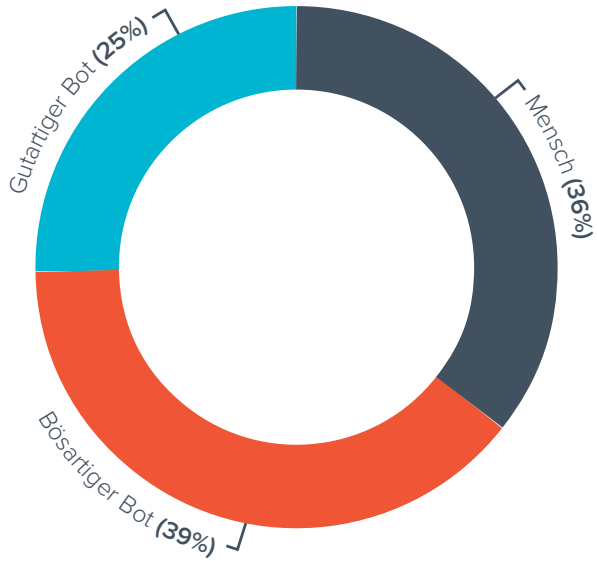
Bösartige Bots führen verschiedene schädliche Aktivitäten aus. Diese reichen von einfachen Scrapern, die Daten aus einer Anwendung abschöpfen wollen (und leicht zu blockieren sind) bis zu fortgeschrittenen hartnäckigen Bots, die sich fast wie Menschen verhalten und alles tun, um eine Erkennung zu vermeiden. Diese Bots führen Angriffe wie Web- und Preis-Scraping, Bestandshortung, Account Takeover-Angriffe, DDoS-Angriffe (Distributed Denial of Service) und viele mehr aus. Bösartige Bots erzeugen einen großen Teil des heutigen Website-Traffics, und es ist wichtig für Unternehmen, diese zu erkennen und zu blockieren.

Der automatisierte Traffic macht fast zwei Drittel des Datenverkehrs im Internet aus. Das ergaben Messungen durch Barracuda-Technologie in den ersten sechs Monaten des Jahres 2021. Knapp 25 % dieses Traffics werden von gutartigen Bots erzeugt – wie Suchmaschinen-Crawler, Bots von Social-Media-Netzwerken und Monitoring-Bots.

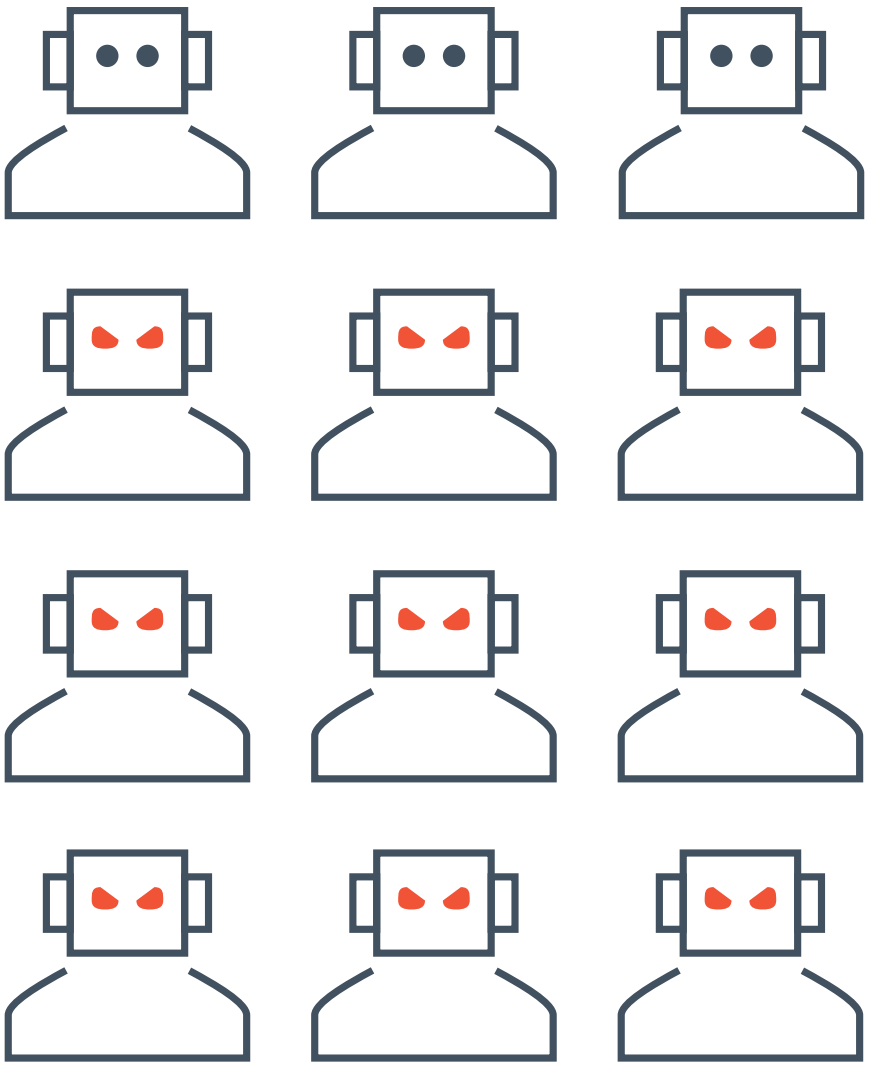
Verteilung nach Monat



Verkehrsverteilung: Bots vs. Menschen (Januar - Juni 2021)



Heutzutage sind Bots äußerst raffiniert und können in ihrem Verhalten fast menschlich sein, um die meisten Schutzmaßnahmen zu umgehen. Die standardmäßigen Abwehrmaßnahmen, vor allem Google reCAPTCHA, stellen für sie kein Problem dar. Die bildbasierten CATPCHAs sind in Wahrheit für Bots sogar einfacher zu lösen als für Menschen. Es gibt ein ganzes Ökosystem, das auf Bots aufbaut: Von den Menschen, die diese intelligenten Bots aufbauen, über Dienste, die „vertrauenswürdige“ Google-Konten („high-reputation“) zur Umgehung von CAPTCHA anbieten, und Dienste, die private IP-Adressen (auch Resis genannt) zur Umgehung von IP-Reputationsblöcken anbieten, bis hin zu Treuhand-Diensten, die den Missbrauch von Bot-Käufern verhindern. Da immer mehr Menschen auf Bots zurückgreifen, um schnelles Geld zu verdienen, wie z. B. beim Wiederverkauf der PlayStation 5 im Dezember 2020, werden Bots zum Mainstream und damit zu einem großen Problem.



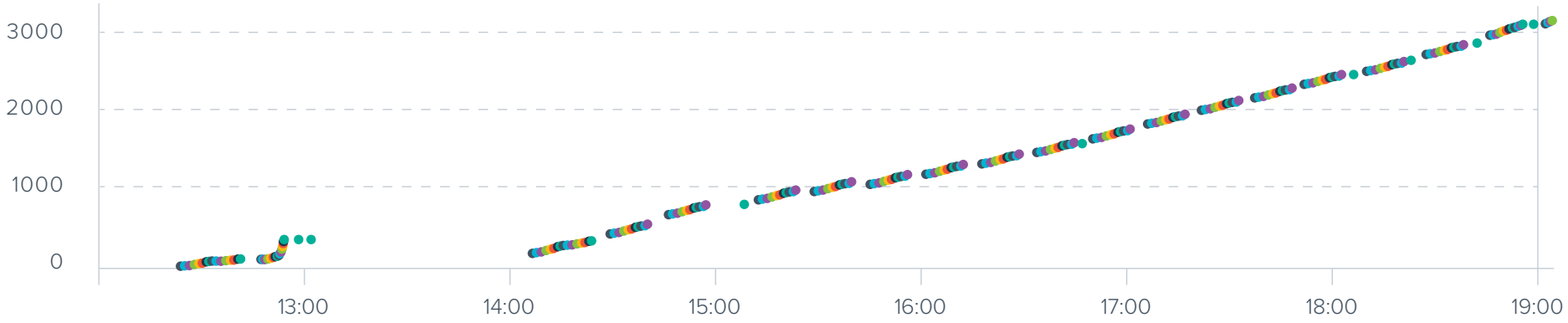
Barracuda

Beispiel: Preis-Scraping bei einem E-Commerce-Shop in Osteuropa

Barracuda entdeckte und verhinderte einen Preis-Scraping-Versuch bei einem E-Commerce-Shop mit Sitz in Osteuropa. Der Shop hatte eine Rabattaktion für Apple-Produkte laufen, und es gab einige verdächtige Muster beim Traffic-Verhalten. Der verdächtige Traffic ging von Standardbrowser-Clients aus und kam über mehrere lokale private IP-Adressen. Diese lokalen IP-Adressen stammten jedoch von VPS-Hostinganbietern, und jeder Client griff nur auf einen Standardsatz von Seiten zu.

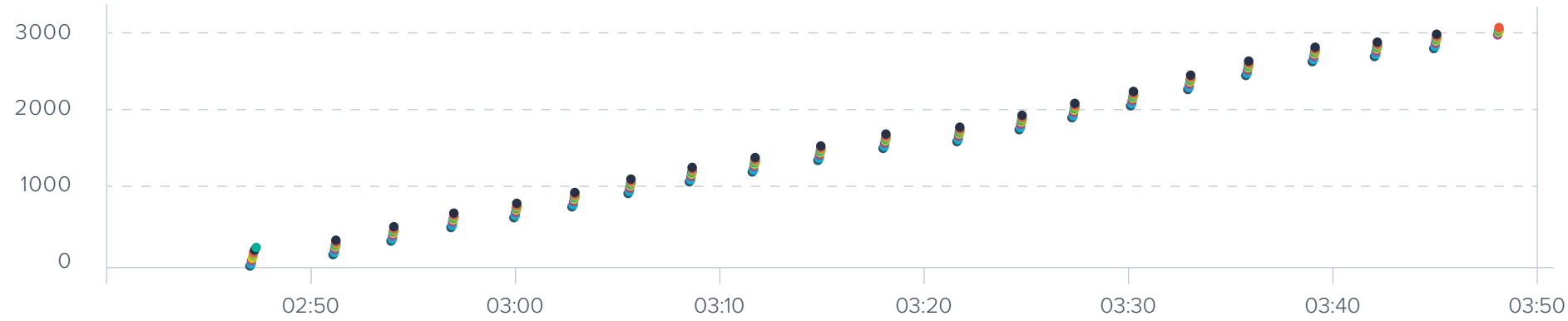
Die Angreifer wurden mit Hilfe dieser Korrelation erwischt – und der Versuch des Price-Scraping wurde gestoppt.

Sich wiederholendes Muster eines Preis-Scraping-Bots



Die Bots griffen mehrmals pro Stunde auf denselben Satz Produkt-URLs zu, nachdem der erste Ansturm blockiert worden war.

Bot ändert Muster, um der Entdeckung zu entgehen

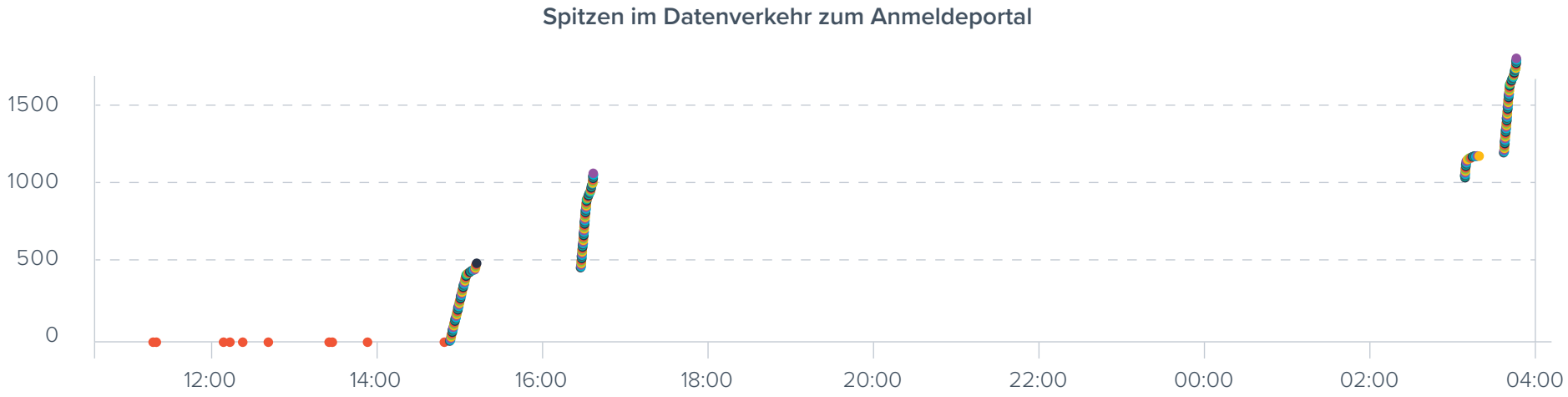


Bots versuchen, mit einem anderen Browsing-Muster mehrmals pro Stunde auf eine kleinere Menge von Produktseiten zuzugreifen.

Barracuda

Beispiel: Versuch, das Anmeldeportal eines indischen Fertigungsunternehmens zu überlasten

Das Anmeldeportal eines indischen Fertigungsunternehmens verzeichnete ungewöhnlich viel Traffic. Der Traffic kam hauptsächlich aus mobilen Netzwerken, was ungewöhnlich, aber bei dieser Website nicht unerwartet war. Bei näherer Analyse erkannte das System jedoch, dass der eingehende Traffic wahrscheinlich von einem Desktop-Browser mit Hotspot-Verbindung kam, der vorgab, ein Mobilgerät zu sein. Die mehreren verschiedenen Clients, die versuchten, diese Anmeldeseite zu überwältigen, wurden erfolgreich blockiert, und die Reaktionszeit der Seite ging wieder auf den Normalwert zurück.



Die ersten Punkte waren ein Bot, der vorgab, ein Mensch zu sein, und seine Zugriffe ausdehnte. Danach sind Cluster zu sehen, und jeder Punkt stellt einen anderen Client dar, der versucht, auf die Anmeldeseite zuzugreifen.

Barracuda

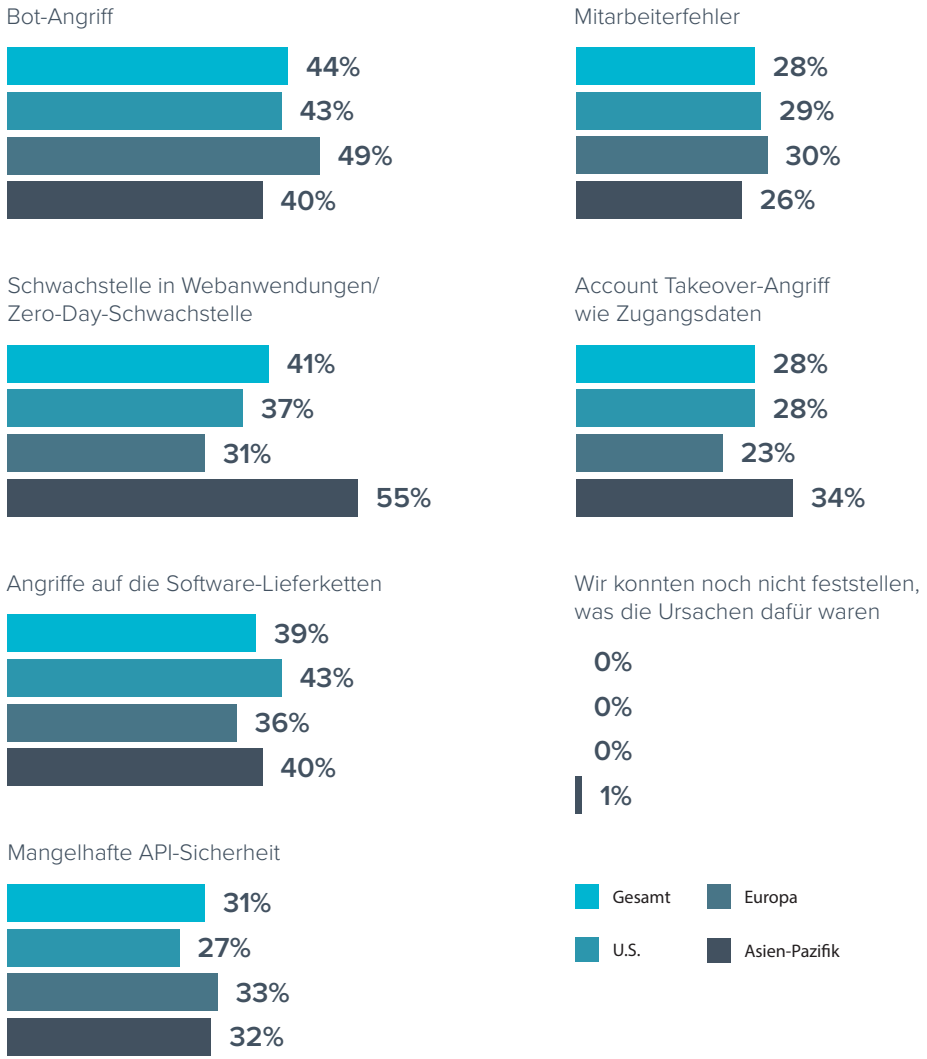
Was Fachleute für Anwendungssicherheit sagen

Bot-Angriffe haben in den letzten Jahren rasant zugenommen, was zu erheblichen Kompromittierungen geführt hat. Vor zwei Jahren waren die größten Bedrohungen durch Bots Account Takeover oder Credential Stuffing, und die Angriffe wurden häufig veröffentlicht, ebenso wie öffentliche Offenlegungen von „Credential Dumps“ von Websites wie LinkedIn.

Laut der aktuellen Umfrage von Barracuda unter Fachleuten für Anwendungssicherheit waren Bot-basierte Angriffe in den letzten 12 Monaten die wahrscheinlichste Ursache für erfolgreiche Sicherheitsverletzungen aufgrund von Anwendungsschwachstellen.

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?

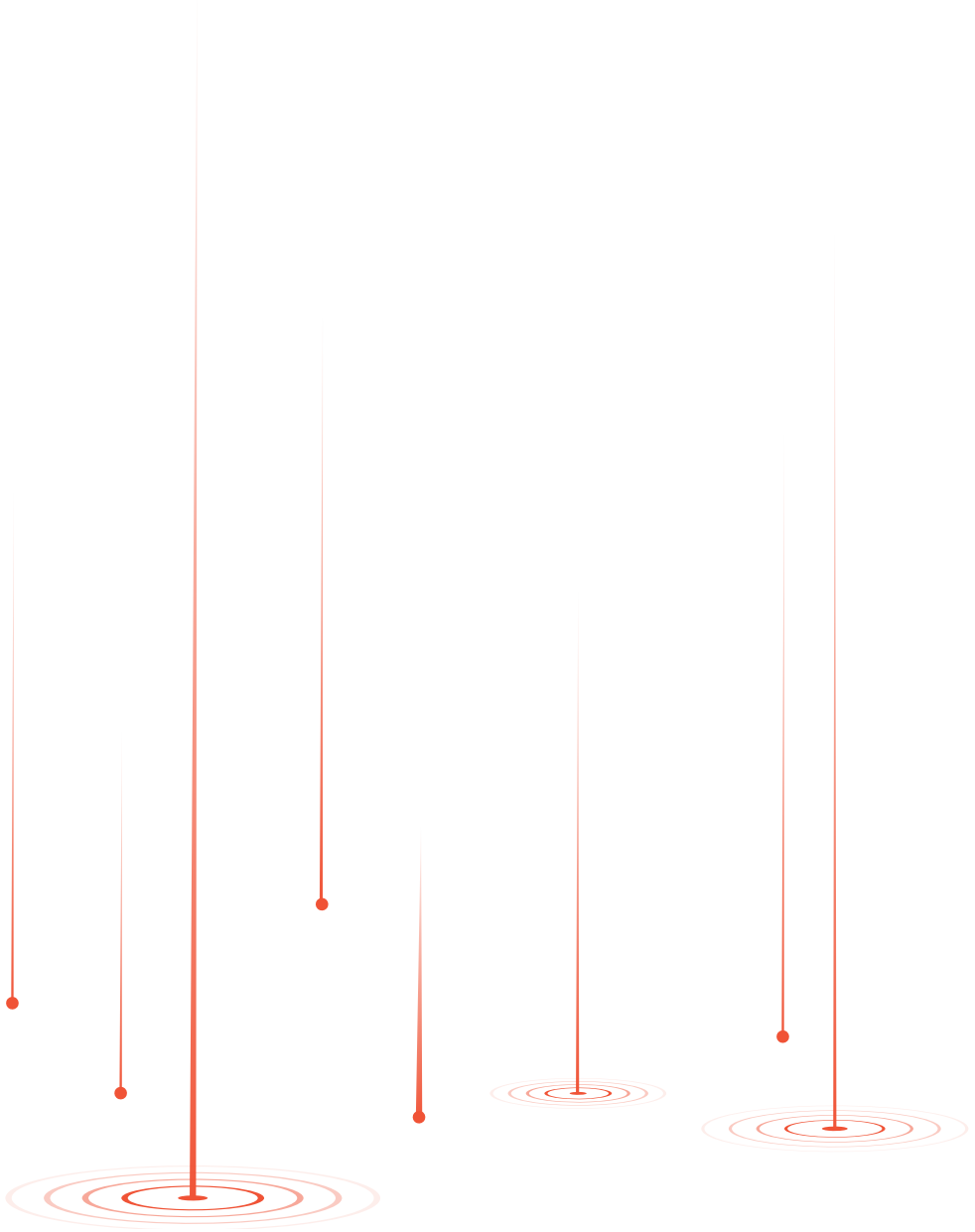
(n=541)



Das breite Spektrum an Bot-Angriffen, die auf Anwendungen abzielen, stellt ein großes Problem für die Abwehr dar.

Bei dieser Vielfalt an Angriffsmöglichkeiten ist es nicht verwunderlich, dass viele Unternehmen Schwierigkeiten haben, ihre Anwendungen vor Bots zu schützen. Während Bot-Spam zwar eher ein lästiger Angriff ist, wird er allerdings oft als Deckmantel benutzt, um etwas Bösartiges zu verbergen. Daher muss er bekämpft werden, und darf nicht ignoriert werden. Je nach Häufigkeit und Authentizität kann Bot-Spam schwierig abzuwehren sein und sich schnell von einer harmlosen Belästigung zu einem betrieblichen Problem entwickeln.

Bots mit Fokus auf Browser- und App-Spoofing stellen ebenfalls ein großes Problem dar. Diese Spoofs reichen von einfach bis komplex, einem einfachen 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.

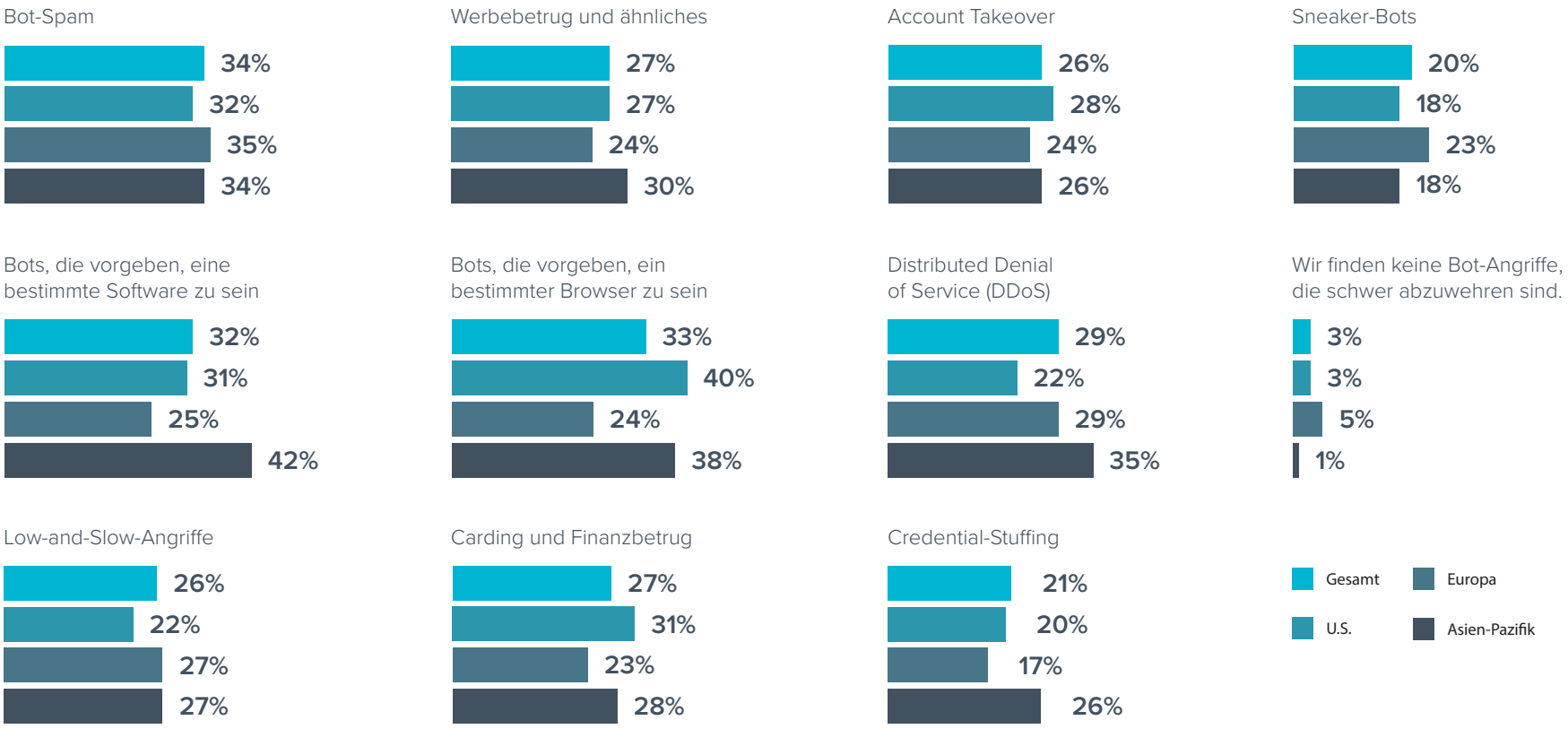


Barracuda

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.

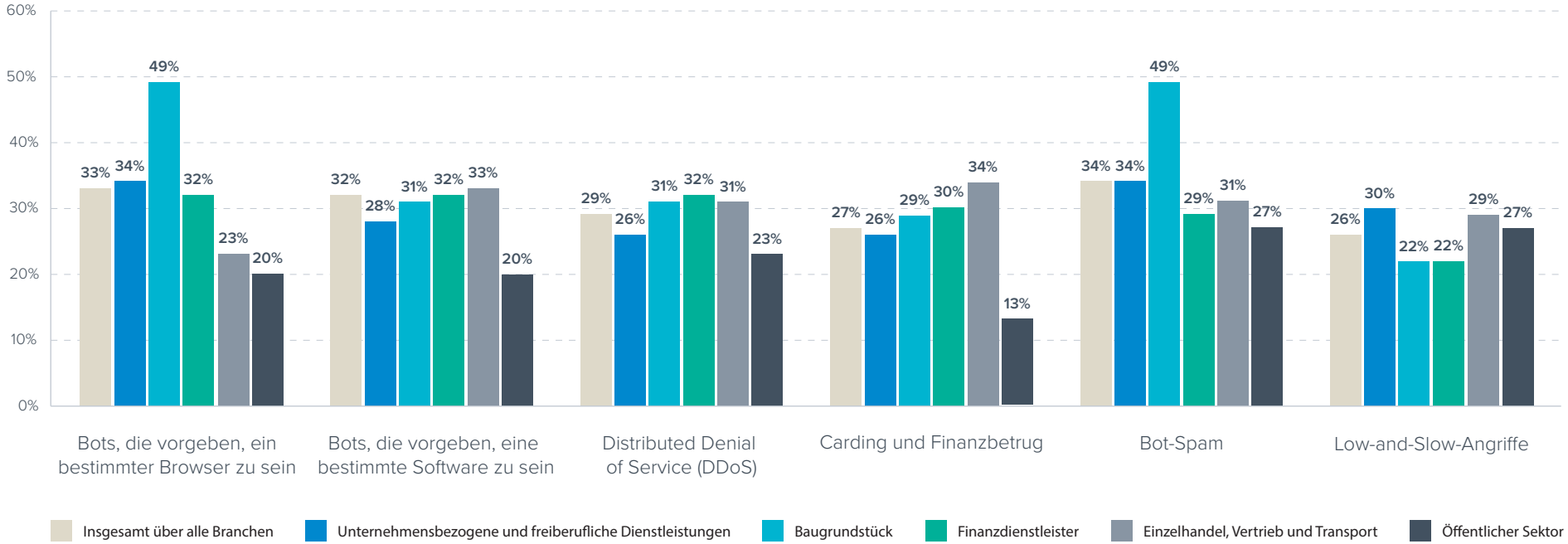
Bei welchen Arten von Bot-Angriffen, die auf Anwendungen abzielen, hat Ihr Unternehmen Schwierigkeiten bei der entsprechenden Verteidigung?

(n=750)



Gegen welche der folgenden Arten von Bot-Angriffen, die auf die Anwendungen Ihres Unternehmens abzielen, haben Sie Schwierigkeiten, sich zu verteidigen?

(n=750)



Für die Befragten aus der Finanzdienstleistungsbranche waren drei Arten von Bot-Angriffen die größte Herausforderung bei der Abwehr: DDoS, Bots, die sich für eine bestimmte Software ausgeben, und Bots, die sich für einen bestimmten Browser ausgeben. Diese Art von Spoofing wird zu einem Problem für Finanzanwendungen, und Angreifer verwenden gecrackte Versionen, um bösartige Aktionen gegen diese Unternehmen auszuführen. DDoS bedeutet erhebliche finanzielle Einbußen, weil diese Systeme einfach nicht verfügbar sind. Interessant ist auch, dass der Karten- und Finanzbetrug an zweiter Stelle der Liste steht, denn man würde erwarten, dass diese die größte Bedrohung darstellen. Dies zeigt, dass die Verbreitung von Apps oder browserbasiertem Zugang für Finanzunternehmen enorm ist und weiter zunimmt.

Barracuda.

Im Allgemeinen sind Bots, die sich für eine bestimmte Software oder einen bestimmten Browser ausgeben, eine der fünf größten Herausforderungen für die meisten Sektoren. Die zweite interessante Reaktion kam aus dem Bau- und Immobiliensektor; der öffentliche Sektor hingegen ist ziemlich besorgt über Bot-Spam. Dies deutet darauf hin, dass Immobilienwebsites bei ihren Angeboten viel Spam sehen könnten. Spam im öffentlichen Sektor ist auch ein großes Problem. Vor einigen Jahren war beispielsweise die Anzahl an „Spam"-Einträgen in den Netto-Neutralitätsdiskussionen der FCC ein Problem.

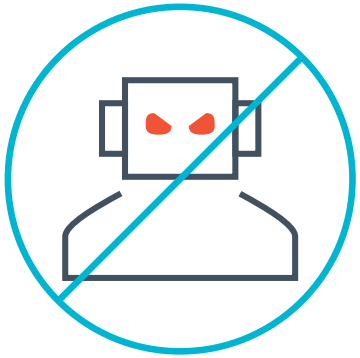
Im öffentlichen Sektor, im Einzelhandel, in Unternehmen und professionellen Dienstleistungen stellen Low-and-Slow-Bots die größten Bedenken dar. In Organisationen des öffentlichen Sektors werden häufig viele Dateien heruntergeladen, die nicht geschützt sind und regelmäßig Ziel von Angreifern werden, die versuchen, DDoS-Angriffe durchzuführen. Einzelhandelsunternehmen haben auch viel durch Slow-and-Low-Bots zu verlieren, die verschiedene Angriffe wie Account Takeover, Preis-Scraping, Scalping und vieles mehr versuchen.

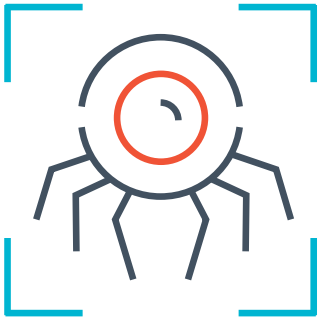
Das Verhindern, Erkennen und Identifizieren von Bots ist eine entscheidende Funktionalität für Anbieter, die Unternehmen im Kampf gegen Bot-basierte Angriffe unterstützen wollen.

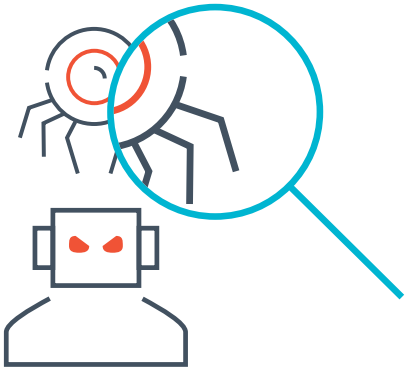
Barracuda

Das Verhindern, Erkennen und Identifizieren von Bots ist eine entscheidende Funktionalität für Anbieter, die Unternehmen im Kampf gegen 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.





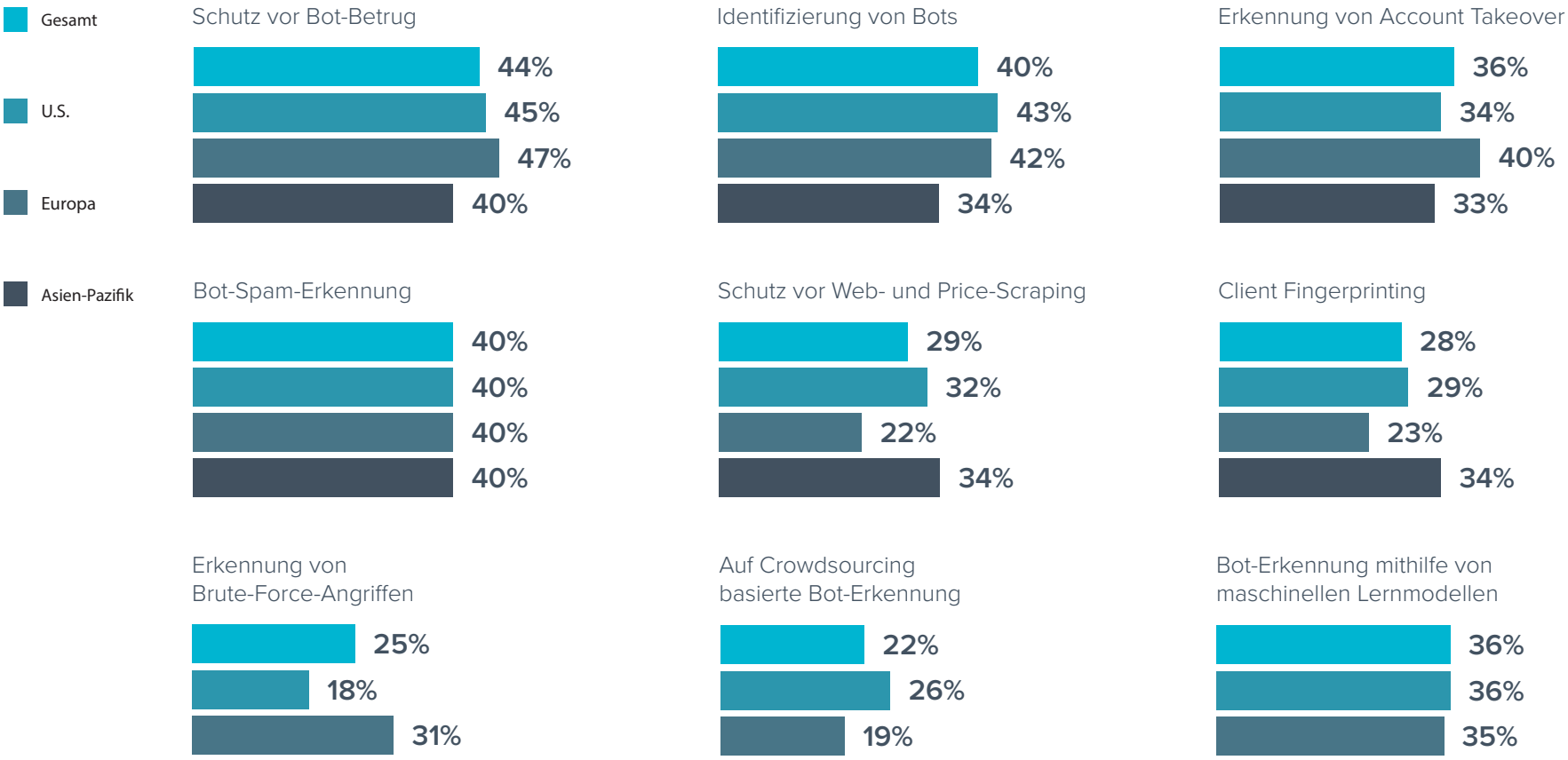


Barracuda

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.

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

(n=750)



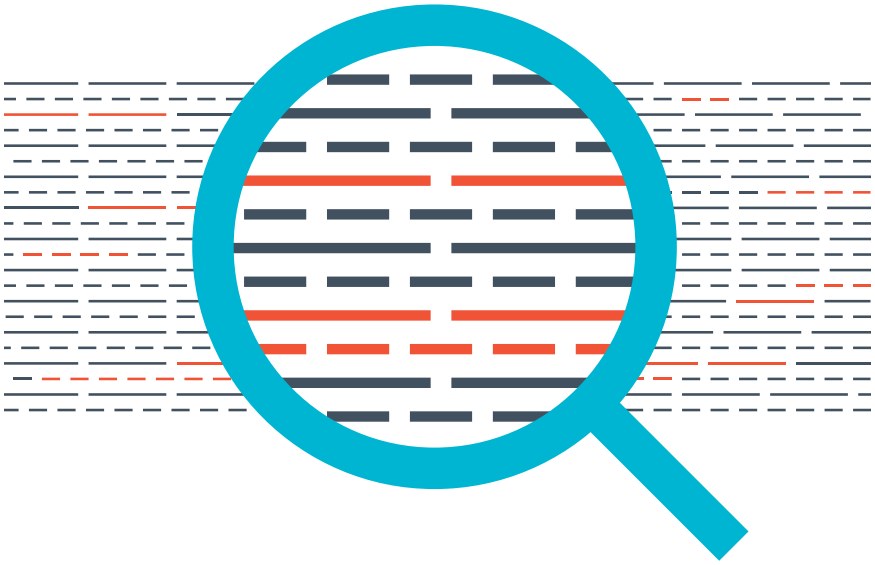
C steht für Client-seitigen Schutz

Im Laufe der Jahre ist eine Vielzahl neuer, webspezifischer Schwachstellen aufgetaucht, wie Clickjacking und Cross-Site-Scripting (XSS), von denen viele auf der Client-Seite auftreten. Und leider sind Injektionsschwachstellen, die vor mehr als einem Jahrzehnt auf der Client-Seite auftraten, immer noch aktuell.

Client-seitige Angriffe, auch bekannt als Supply-Chain-Angriffe oder Magecart-Angriffe (benannt nach der ursprünglich auf die Magento-Shopping-Anwendung gerichtete Angriffe), sind schwer zu erkennen und zu blockieren.

Barracuda

Seit den Anfängen des Internets in den späten 1980er Jahren haben sich Apps kontinuierlich weiterentwickelt, um unseren unerschütterlichen Appetit auf alles, was das Internet anbelangt, zu befriedigen. Diese Veränderung hat nicht nur auf der Serverseite stattgefunden, sondern auch auf der Client-Seite (also Browser). Ebenso wie dynamische Inhalte statische Inhalte ersetzten, ersetzten einseitige Anwendungen das einfache JavaScript-basierte Rendering durch ein Erlebnis, das besser für das Scrollen auf Smartphones oder Tablets geeignet ist. Da ein immer größerer Teil der Anwendungslogik auf die Client-Seite verlagert wird, haben Angreifer ihre Aufmerksamkeit ebenfalls auf die Client-Seite gerichtet. Ein Großteil dieser Client-seitigen Logik wird entweder mit Open Source oder mit anderen Drittanbieter-Codes implementiert – und dabei bleibt die Sicherheit auf der Strecke.



Warum also verwenden Entwickler den Code von Drittanbietern? Nun, einfach gesagt, wäre das moderne Web ohne dies nicht möglich. Moderne Webseiten bestehen aus Dutzenden oder sogar Hunderten von externen Skripten von Dritt- oder Viertanbietern. Mit Tools wie webpagetest.org kann man die überraschende Anzahl von Drittanbieter-Skripten auf einer bestimmten Webseite sehen. Das ist ein akzeptierter Ansatz in der Webentwicklung, denn die Alternative ist undenkbar: Tausende von Codezeilen neu zu erfinden. Das Problem ist eine Frage des Vertrauens: Ein Skript, das heute gut ist, kann morgen schon gehackt sein. Angreifer haben es auf die Quellen abgesehen, die diesen Code von Drittanbietern hosten, weil ihr Hack jede Anwendung, die diesen Code verwendet, in ein Opfer verwandelt.

Da es der Code von Drittanbietern ist, der böswillig verändert wird, bemerken die meisten Anwendungsbesitzer erst viel später, dass die Skripte kompromittiert sind. Die Skripte selbst werden aus anderen Quellen wie CDNs und Code-Depots geladen und in der Regel nicht direkt von der Website an den Browser übermittelt. Das bedeutet, dass es mit den derzeitigen Tools und Verfahren schwierig ist, sie zu erkennen und ihnen Einhalt zu gebieten.

Beispiel: Angriff auf die Lieferkette von British Airways

Im Jahr 2018 führte eine kompromittierte Lieferkette dazu, dass die Daten von 380.000 bis 500.000 Kunden von British Airways kompromittiert wurden. Der Verstoß führte zum Verlust von persönlichen Daten und Zahlungsinformationen der Betroffenen.

Der Verstoß war zu diesem Zeitpunkt einer der bekanntesten Magecart-Angriffe. Magecart war eine Gruppe, die zum ersten Mal im Jahr 2016 beim Abschöpfen von Kartendaten im Internet auffiel. Sie schleusten Skripte ein, die gezielt Daten aus Online-Zahlungsformularen stahlen und die gestohlenen Daten dann entweder selbst verwendeten oder an andere Hacker verkauften.

Im Fall von British Airways änderte die Magecart-Gruppe ein spezielles JavaScript namens Modernizr, das in ihren Web- und Mobilanwendungen verwendet wird. In dieses Skript haben sie eine kleine Funktion eingebettet, die am Ende des Skripts ausgeführt wird. Als diese Funktion ausgeführt wurde, sammelte sie die in das Zahlungsformular eingegebenen Daten und schickte sie an eine von der kriminellen Gruppe betriebene Website. Das führte zu einer massiven Datenexfiltration, und British Airways wurde zu einer Geldstrafe in Höhe von 20 Millionen Pfund verurteilt, die damals höchste Geldstrafe im Vereinigten Königreich (die ursprüngliche Summe von 183,39 Millionen Pfund wurde aufgrund der wirtschaftlichen Auswirkungen der Pandemie auf die Flug- und Reisebranche reduziert).

Von der Datenschutzverletzung **betroffene Kunden**

380-500K

British Airways **mit Geldstrafe belegt**

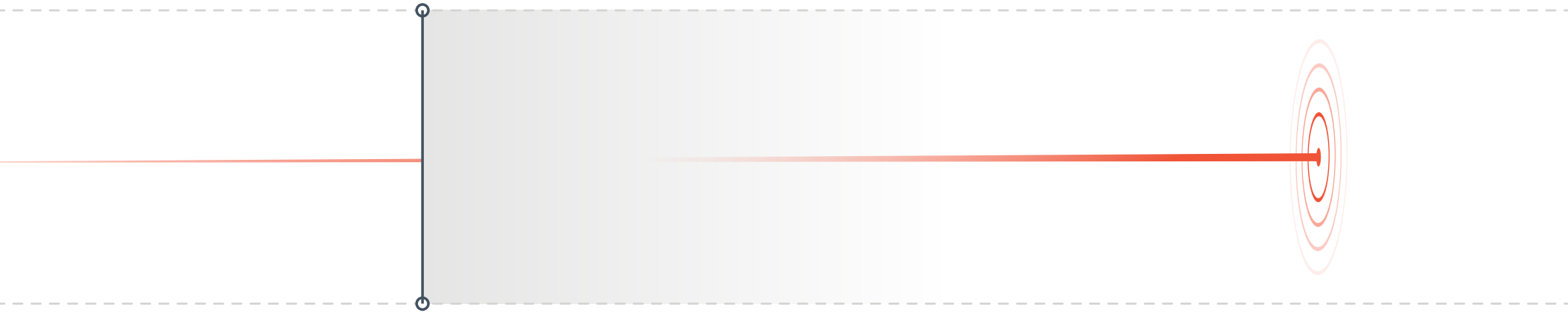
20M Pfund

Barracuda

Beispiel: Visa warnt vor Online-Skimmer

Im September 2020 gab Visa eine Warnung über einen neuen Online-Skimmer namens Baka heraus, der Client-seitige Skimming-Angriffe ausführte. Der Skimmer hatte einige interessante Mechanismen, um die Erkennung zu verhindern. Der Skimmer wurde zum Zeitpunkt der Ausführung dynamisch in den Speicher des Client-Computers geladen. Somit wurde er von Standard-Scans oder Seitenprüfungen nicht erkannt. Er war so konzipiert, dass er nur vom Speicher aus ausgeführt wird und keine Spuren im Speicher des Browsers gefunden werden konnten. Die Erfinder dieses Skimmers hatten sich sehr bemüht sicherzustellen, dass er vollständig verschlüsselt und schwer zu erkennen war, wenn er auf einer Website oder in einer Anwendung ausgeführt wurde.

Zum Zeitpunkt der Meldung war der Skimmer bereits bei vielen Online-Shops aktiv im Einsatz; offensichtlich war er von erfahrenen Entwicklern konzipiert worden, die ihn so lange wie möglich unentdeckt lassen wollten.



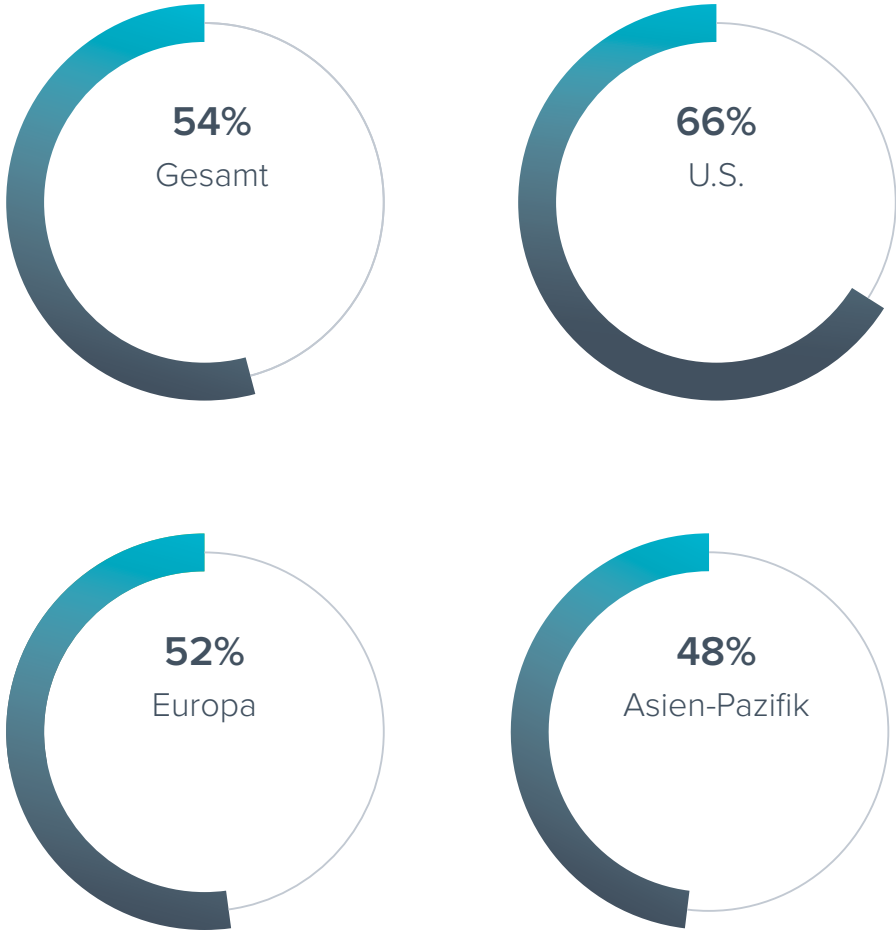
Was Fachleute für Anwendungssicherheit sagen

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

Das Streben nach Effizienz bei der Anwendungsentwicklung zeigt sich einmal mehr bei den Antworten in der jüngsten Barracuda-Umfrage unter Fachleuten für Anwendungssicherheit, wobei mehr als die Hälfte der Unternehmen vorgefertigte Skripte von Drittanbietern für Webanwendungen verwenden. Die Sicherheit sollte bei der Verwendung von Drittanbieter-Code ein großes Anliegen sein. Das gilt insbesondere dann, wenn der Code direkt von der Quellplattform, wie z. B. GitHub, an einen Browser übermittelt wird. Wenn der Code manipuliert wurde, könnte ein Angriff über die Software-Lieferkette, wie z. B. Magecart, unmittelbar bevorstehen. Unternehmen sollten sich vor diesem Ansatz der Anwendungsentwicklung hüten.

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

(n=750)

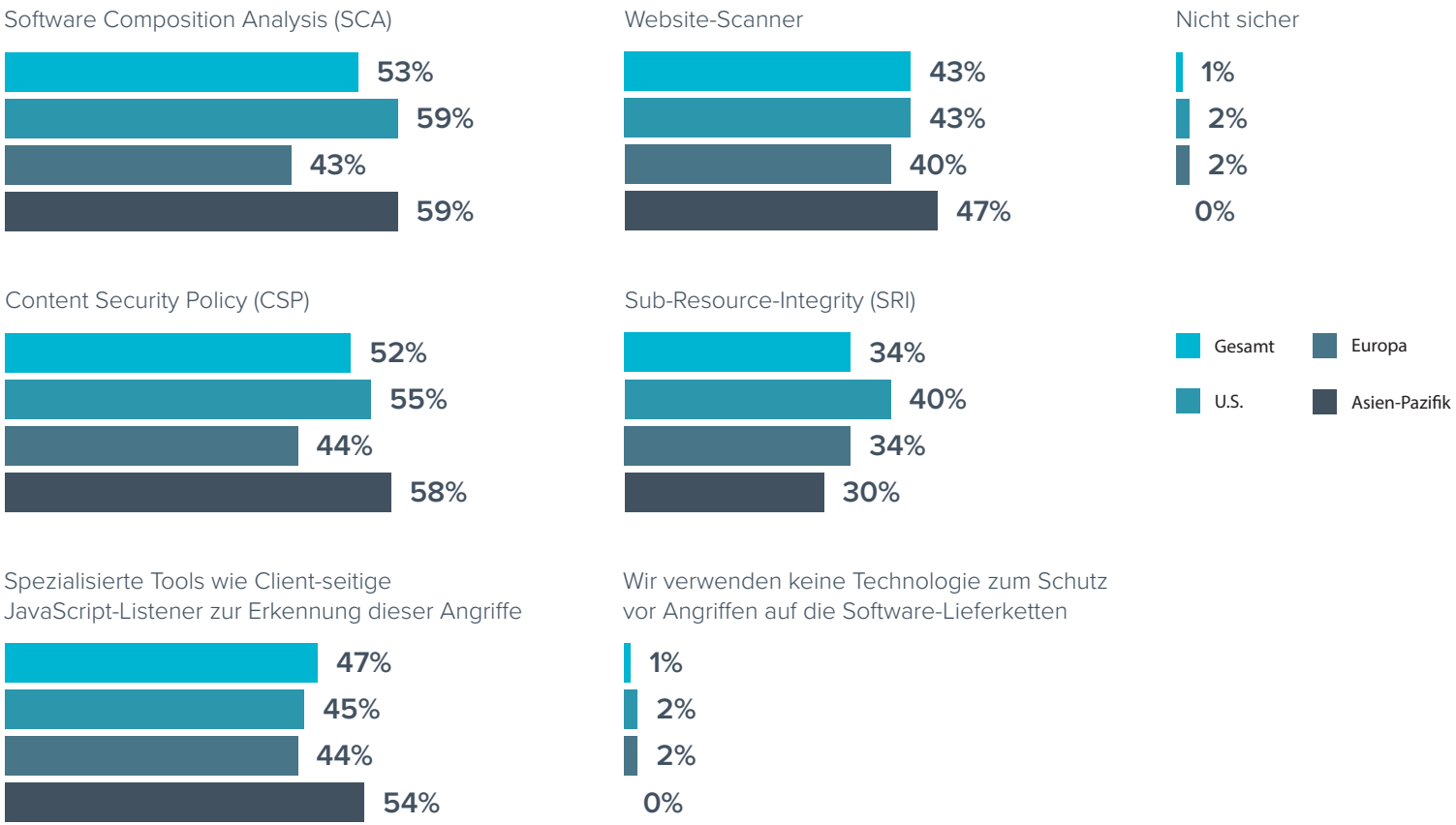


Für die Abwehr von Angriffen auf die Lieferkette gibt es relativ standardisierte Schutzmaßnahmen. Mehr als in anderen Regionen nutzen Befragte aus dem asiatisch-pazifischen Raum spezialisierte Tools zur Erkennung von Angriffen, einschließlich Client-seitiger JS-Listener. Solche Listener haben eine bessere 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?

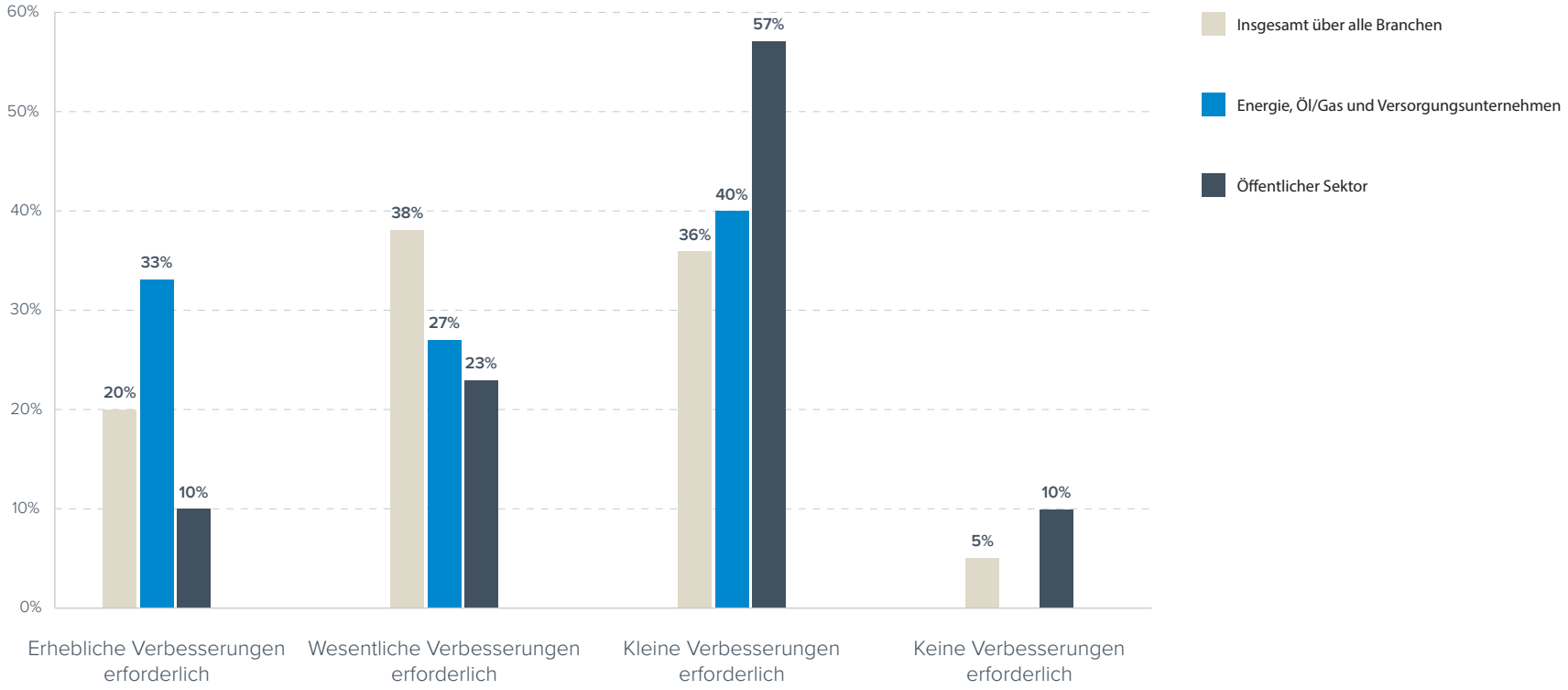
(n=750)



Barracuda

Welche Verbesserungen sind Ihrer Meinung nach in Ihrem Unternehmen erforderlich, wenn es um die Abwehr von Angriffen auf die Software-Lieferkette geht?

(n=728)



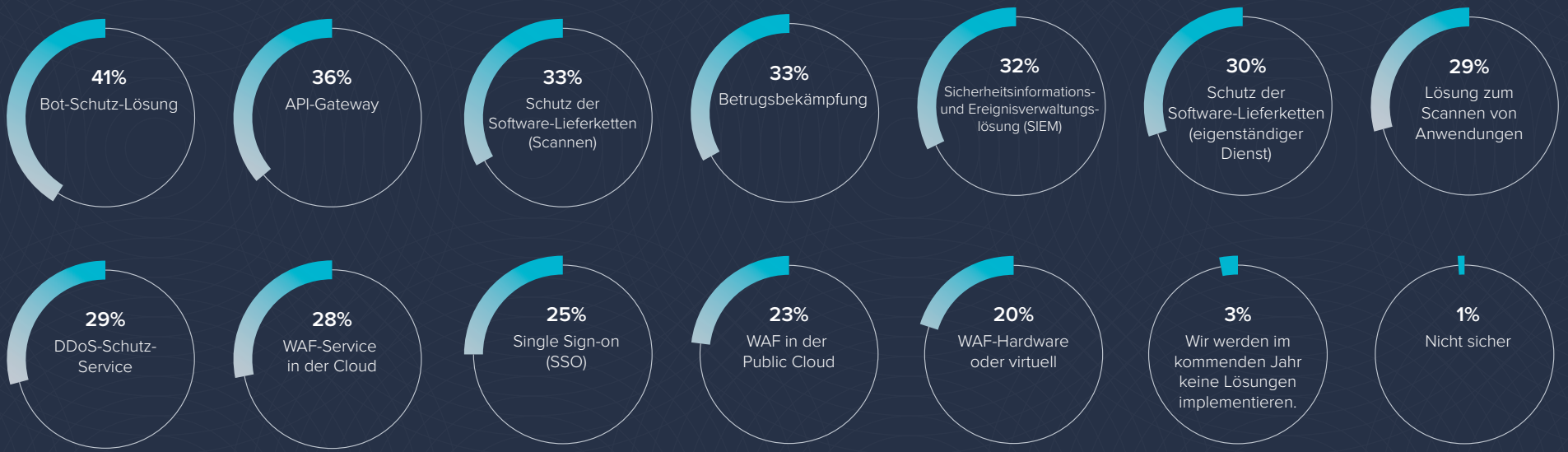
Die meisten Unternehmen sind sich hinsichtlich der für ihre Website-Supply-Chains erforderlichen Verbesserungen uneins. Die Befragten des öffentlichen Sektors gaben am ehesten an, dass für ihren Schutz kleine Verbesserungen oder Verbesserungen erforderlich sind. Lediglich der Energie-, Öl-, Gas- und Versorgungssektor gab an, dass erhebliche Verbesserungen erforderlich sind. Dies liegt wohl daran, dass es diesen Angriffsvektor erst seit relativ kurzer Zeit gibt und die Auswirkungen noch nicht vollständig bekannt sind. Je mehr dieser Angriffe ans Tageslicht kommen, desto mehr wird der Angriffsvektor an Bedeutung gewinnen.

Schlussfolgerung: Vorbereitung auf die neuen ABCs der Anwendungssicherheit

Unternehmen werden mehr denn je über ihre Web- und API-Anwendungen angegriffen. Mit der zunehmenden Verbreitung neuerer Technologien suchen Angreifer nach Möglichkeiten, deren Sicherheitsmaßnahmen zu umgehen und in die Systeme einzudringen. APIs, Bot-Angriffe und Client-seitige Angriffe sind die neuesten Methoden, mit denen sie aus Spaß und Profitgründen in Anwendungen eindringen.

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

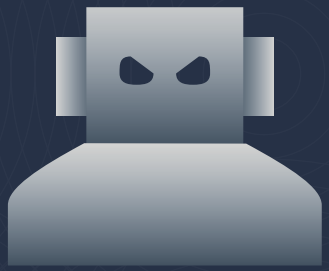
(n=750)



Barracuda

Unsere Recherchen haben ergeben, dass Unternehmen sich dessen bewusst sind, da viele von ihnen im kommenden Jahr neue Lösungen wie Bot-Schutz (41 %), API-Gateway (36 %) und Software-Supply-Chain-Schutz (Scanning) (33 %) einsetzen wollen.

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 fähig ist, Kunden vor all diesen Angriffsvektoren zu schützen. Ein plattformbasierter Ansatz für die Anwendungssicherheit bietet einen leistungsstarken Schutz sowohl gegen herkömmliche als auch gegen neue Bedrohungen und gleichzeitig eine einfache Bedienung und Verwaltung.



Barracuda

Über Barracuda

Wir von Barracuda wollen die Welt sicherer machen. Wir glauben, 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 Lösungen, die mit unseren Kunden wachsen und sich anpassen. 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 de.barracuda.com.