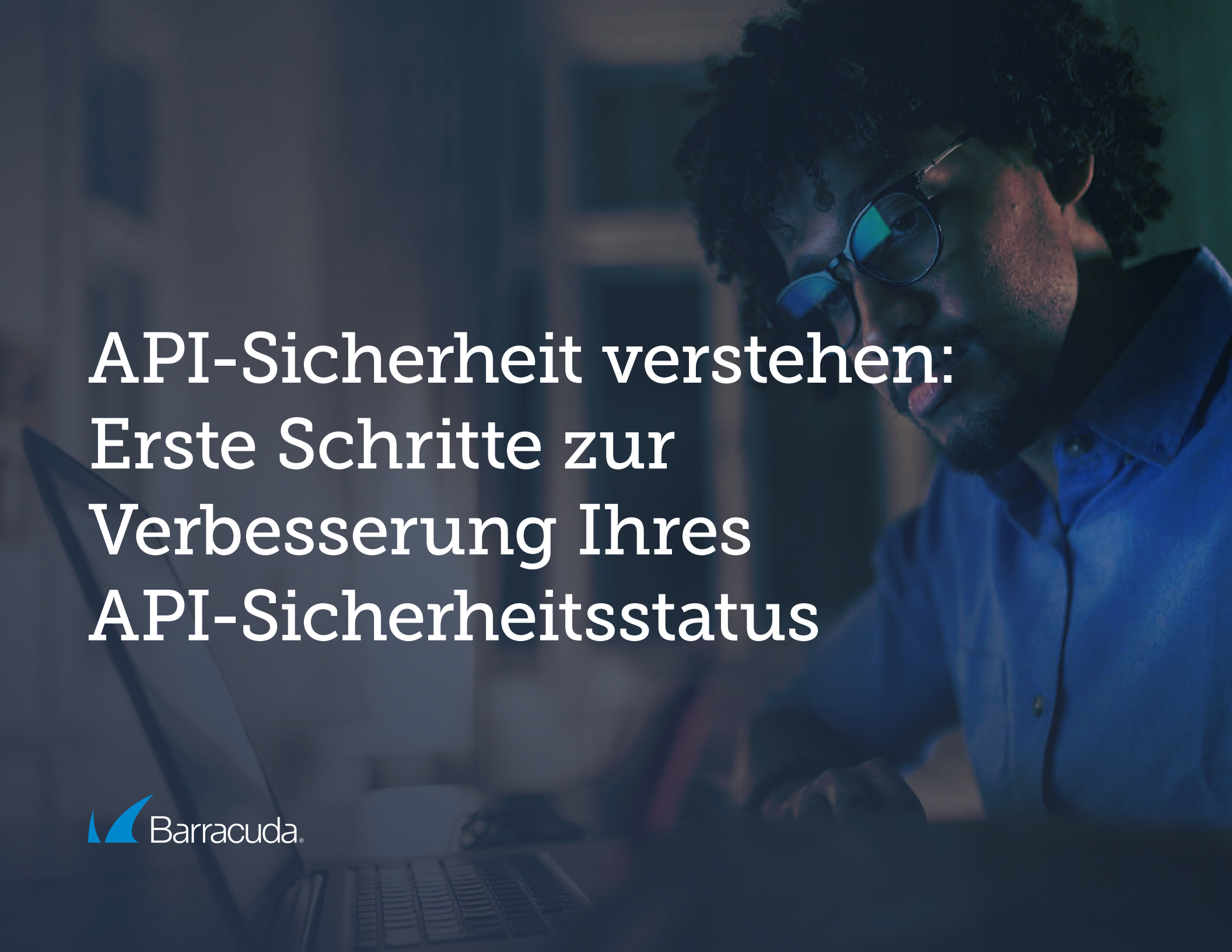


API-Sicherheit verstehen: Erste Schritte zur Verbesserung Ihres API-Sicherheitsstatus

Barracuda

API-Sicherheit im Wandel

API-Sicherheit hat sich von einem „nice-to-have“ zu einem wesentlichen Bestandteil jedes sinnvollen Sicherheitskonzepts entwickelt. Durch die Umstellung auf Cloud Computing ist die API-Sicherheit in den Fokus der Chief Information Security Officers gerückt. COVID-19 und die breitere Akzeptanz des Arbeitens im Home Office haben den Wandel weiter beschleunigt, da all diese Systeme auf der verstärkten Nutzung von APIs basieren.

APIs spielen in fast allen Geschäftssystemen eine zunehmend zentrale Rolle und Gartner schätzt, dass die Hälfte aller Business-to-Business-Transaktionen mittlerweile über eine API abgewickelt wird.Das erklärt, warum bei Umfragen, die CISOs nach dem größten Verbesserungspotential im Sicherheitsbereich fragen, die API-Sicherheit an erster Stelle steht.

Die API-Nutzung hängt von der Unternehmensgröße ab — 80% der Firmen mit weniger als 50 Mitarbeitern nutzen weniger als 50 APIs. Doch größere Unternehmen verwenden eine höhere Anzahl an internen und externen APIs — wobei das größte über 250 APIs nutzt.

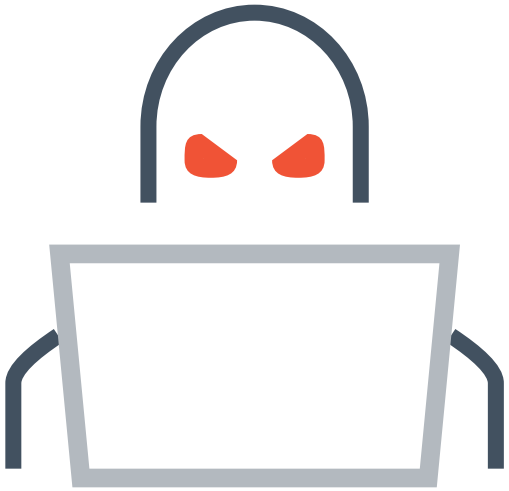
Barracuda

API-Angriffe und ihre Folgen

Dieses rasche Wachstum der API-Nutzung geht mit einem ebenso schnell wachsenden Sicherheitsrisiko einher. Die Forschungsgruppe Gartner geht davon aus, dass API-Angriffe sich noch im Jahr 2023 zum häufigsten Angriffsvektor entwickeln werden. Bis 2025 wird die Hälfte aller Datenschutzverletzungen vermutlich mit einem API-Angriff eingeleitet.

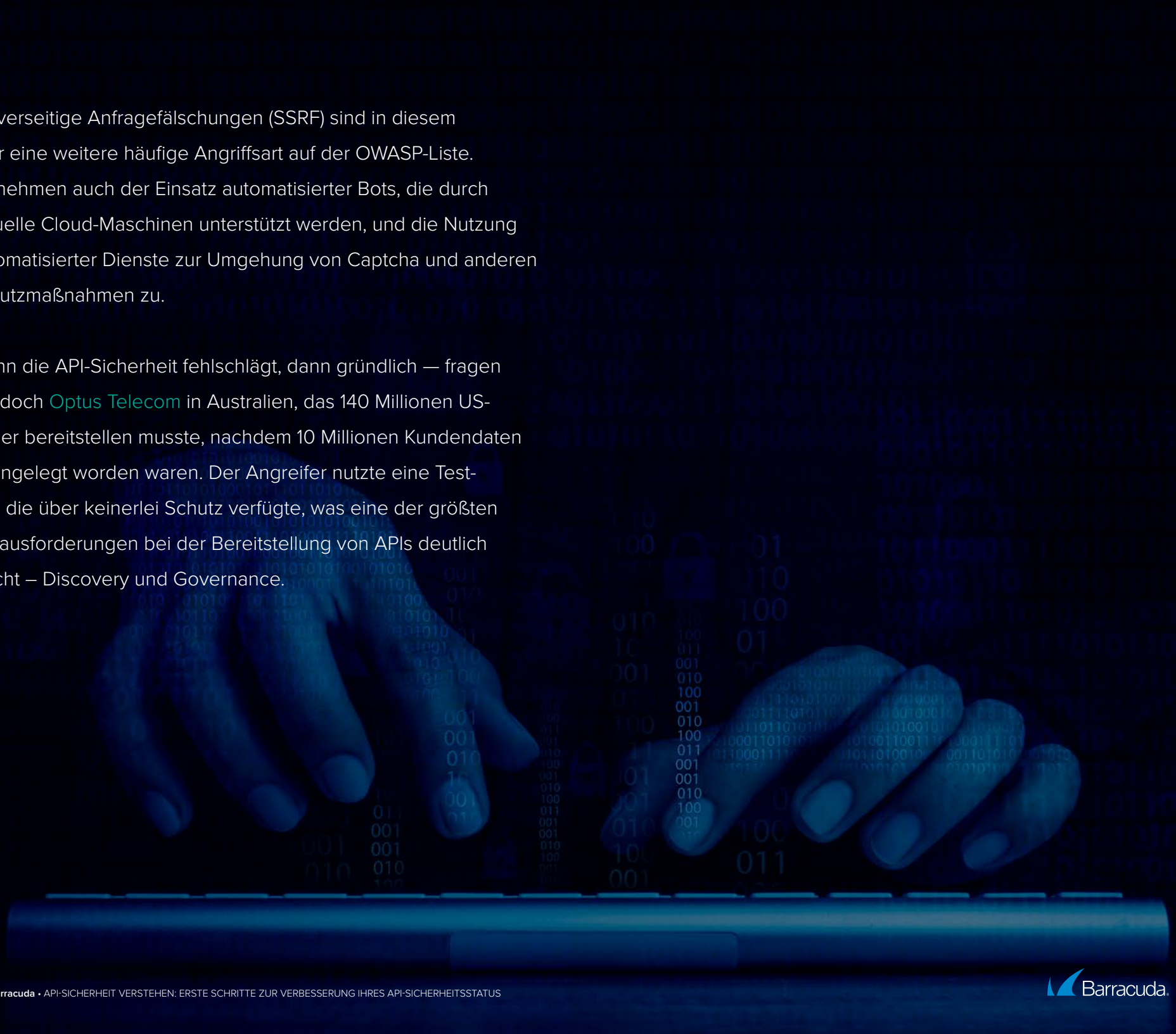
Das erklärt, warum das Open Web Application Security Project (OWASP) neben seiner allseits bekannten Liste für Web Application Security jetzt auch eine Top 10-Liste für API-Sicherheit herausgibt. Seit der ersten API-Liste im Jahr 2019 hat sich die Art der Sicherheitslücken sowie deren Verbreitung stark verändert.

Doch aufgrund des raschen Wandels bei der API-Sicherheit, sind auch die vom OWASP identifizierten Hauptrisiken heute andere als damals.Ein zentrales Thema auf der diesjährigen Liste sind die Authentifizierung und Autorisierung.Bei der fehlerhaften Autorisierung auf Objektebene handelt es sich um eine Möglichkeit, die Identität eines Objekts zu manipulieren, um einem Angreifer unerlaubten Zugriff auf die Systeme zu gewähren. APIs können mit Tausenden von Objekten interagieren, was sie zu einem der häufigsten Angriffsvektoren macht.Erfolgreiche Angriffe können zu Datenverlust oder sogar zu einer vollständigen Kontenübernahme führen.



Serverseitige Anfragefälschungen (SSRF) sind in diesem Jahr eine weitere häufige Angriffsart auf der OWASP-Liste. So nehmen auch der Einsatz automatisierter Bots, die durch virtuelle Cloud-Maschinen unterstützt werden, und die Nutzung automatisierter Dienste zur Umgehung von Captcha und anderen Schutzmaßnahmen zu.

Wenn die API-Sicherheit fehlschlägt, dann gründlich — fragen Sie doch Optus Telecom in Australien, das 140 Millionen US-Doller bereitstellen musste, nachdem 10 Millionen Kundendaten offengelegt worden waren. Der Angreifer nutzte eine Test-API, die über keinerlei Schutz verfügte, was eine der größten Herausforderungen bei der Bereitstellung von APIs deutlich macht – Discovery und Governance.



Die ersten Schritte zu mehr API-Sicherheit

Zuerst ist Transparenz gefragt.Wie bei allen Aspekten der Cybersicherheit bzw. jeder Art von Sicherheit, besteht der erste Schritt darin, sich einen möglichst klaren Überblick über Ihre Systeme zu verschaffen. Dadurch erhalten Sie einen besseren Einblick in Ihre potenziellen Schwachstellen.

Einfach gesagt, fehlt den Sicherheitsteams das Wissen darüber, welche APIs ihr Unternehmen nutzt und worauf diese APIs zugreifen.In einer Welt der Schatten-IT, in der Abteilungen ihre eigenen Cloud-Umgebungen, die sie mal kürzer und mal länger nutzen, aufbauen, kann es schwierig sein, überhaupt eine vollständige Prüfung durchzuführen.

Auch wenn Sie Ihre eigenen APIs äußerst sorgfältig prüfen, können Schatten-APIs weiterhin ein Risiko darstellen — das sind Schnittstellen, die ohne das Wissen der Sicherheitsteams und wahrscheinlich ohne die Einhaltung bewährter Governance- und Sicherheitspraktiken erstellt wurden.Diese waren möglicherweise nur für den internen Gebrauch durch Entwickler oder zur Durchführung schneller Testläufe gedacht und wurden nicht für den öffentlichen Zugriff konzipiert oder abgesichert.

Ein weiteres Risiko stellen Zombie-APIs dar — dabei handelt es sich um APIs, die nicht mehr in Verwendung sind und die man wahrscheinlich einfach vergessen hat.Irgendwann einmal waren Sie für die Infrastruktur eines Unternehmens wichtig, wurden jedoch nicht entfernt, als sie an Bedeutung verloren.Selbst Unternehmen mit ziemlich ausgereiften API-Sicherheitspraktiken verfügen nicht immer über Richtlinien zur Entfernung von APIs, die nicht mehr regelmäßig verwendet werden.

Der erste Schritt ist deshalb der Schutz Ihrer eigenen internen APIs.Externe APIs und APIs von Drittanbietern werden von der überwiegenden Mehrheit der Unternehmen genutzt und können mit eigenen Risiken verbunden sein — so hat beispielsweise selbst WordPress APIs standardmäßig aktiviert.

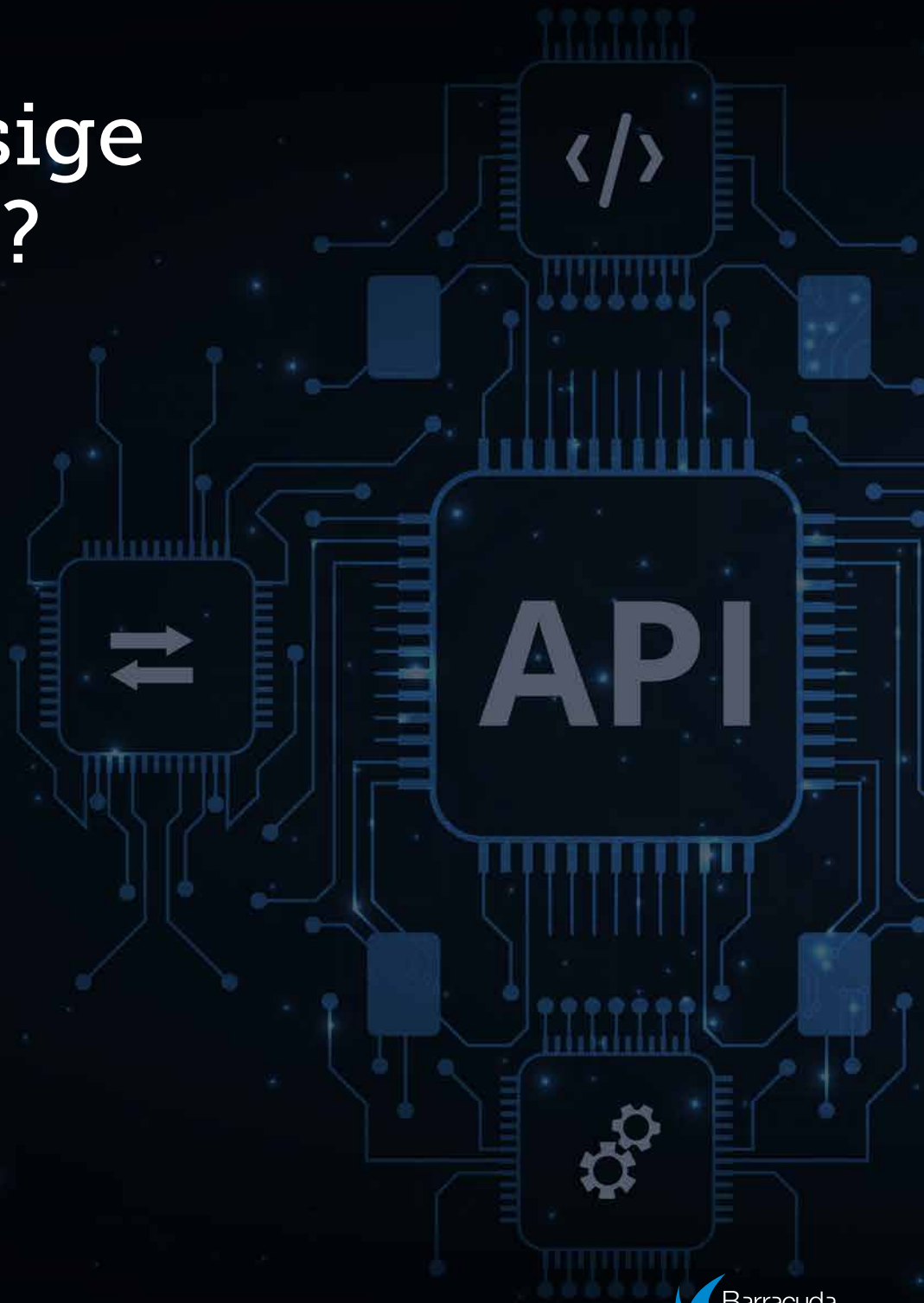
Jedes Drittsystem birgt die gleichen Risiken, wenn es um undokumentierte Zombie- und Schatten-APIs geht.

Sogar in Firmen, die bei der API-Sicherheit die Nase vorne haben, mühen sich IT-Mitarbeiter noch immer mit unausgereiften API-Sicherheitstools ab, die keinen umfassenden Einblick in die Abläufe zulassen.Das heißt, dass API-Sicherheit noch immer eine manuelle und zeitaufwändige Aufgabe ist.Selbst mit den besten Tools ist es aufgrund des Tempos, mit dem die Anzahl der APIs wächst, für Sicherheitsteams und Anbieter schwierig, Schritt zu halten.

Wie sieht zuverlässige API-Sicherheit aus?

Die Entwicklung von API-First-Software schreitet rasch voran und ist eine logische Weiterentwicklung in der zunehmend vernetzten Welt von heute.Die modulare Software-Entwicklung — bei der die Software in logische Teile zerlegt und dann zusammengefügt wird — stützt sich in hohem Maße auf APIs.Und in der heutigen Welt, in der es sich bei all diesen Modulen um Microservices handelt, die, um zu funktionieren, sowohl intra- als auch intermodulare APIs nutzen, ist das Erkennen und Absichern der APIs von entscheidender Bedeutung.Daran wird sich so schnell auch nichts ändern, weshalb sich die Sicherheitsteams dieser Herausforderung stellen müssen.

Das mag entmutigend klingen, aber es geht hier nicht darum, das Rad neu zu erfinden — wir können aus anderen Bereichen der Cybersecurity lernen.



Wer heute nicht plant, hat morgen schon verloren

Der erste Schritt zur API-Sicherheit besteht nicht im Erwerb eines Produkts, sondern in der Schaffung der Grundlagen.

Das bedeutet, dass Sie wissen müssen, auf welche APIs Ihr Unternehmen im Tagesgeschäft angewiesen ist. Gehen Sie die Protokolle durch, wenn Sie welche haben oder setzen Sie Systeme ein, die Ihnen diese wichtigen Daten liefern.

Danach gilt es Prozesse und Abläufe einzurichten. Die Mitarbeiter müssen die Risiken kennen und wissen, wie sie sich verhalten sollen.

Hier kommt die Governance ins Spiel — die Umsetzung dieser Prozesse und Abläufe.

Erst, wenn diese Grundlagen vorhanden sind, ist es sinnvoll mit Anbietern in Kontakt zu treten.Am besten überlegen Sie sich schon vorher, welches System das geeignetste für Ihr Unternehmen sein könnte.Möchten Sie einen einfachen Service oder wollen Sie Ihre eigene Lösung intern oder in der Cloud hosten?

Sobald Sie intern die Grundlagen geschaffen haben, kommt eine größere Herausforderung auf Sie zu: sicherzugehen, dass Ihre Zulieferer dasselbe tun.Achten Sie darauf, die richtigen Fragen zu stellen und APIs von Drittanbietern die geringstmöglichen Privilegien zu gewähren.

Die Bereitstellung erstklassiger API-Sicherheit kann zu einem echten Geschäftsvorteil werden.Wenn Ihre Kunden sehen, dass Sie API-Sicherheit ernst nehmen, bekommen vielleicht Sie den Zuschlag und nicht der Konkurrent, der weniger Sorgfalt walten lässt.

Mehr dazu

Barracuda Application Protection ist eine Plattform, die umfassenden Schutz für Web-Applikationen und APIs bietet (WAAP). Sie ist einfach bereitzustellen und skalierbar, um Anwendungen jeder Größe schützen zu können.

Ihre auf maschinellem Lernen basierenden API - Schutzfunktionen können alle JSON und GraphQL APIs erkennen, einschließlich der unbekannten Schatten- oder Zombie-APIs. Barracuda Application Protection ist als Appliance, virtuelle Maschine, SaaS-Service oder Container verfügbar und schützt Ihre Web-Applikationen und APIs überall.

Visit the Website.

Testen Sie Application Protection kostenlos.

Konfigurieren Sie Ihre Application Protection -Lösung

Über Barracuda

Barracuda ist bestrebt, die Welt zu einem sichereren Ort zu machen und überzeugt davon, dass jedes Unternehmen Zugang zu Cloud-fähigen Sicherheitslösungen auf höchstem Niveau verdient, die einfach zu erwerben, zu implementieren und zu nutzen sind. Wir schützen E-Mails, Netzwerke, Daten und Anwendungen mit innovativen Lösungen, die im Zuge der Customer Journey wachsen. Mehr als 200.000 Unternehmen weltweit vertrauen auf Barracuda und darauf, dass wir sie auch vor Risiken schützen, die ihnen möglicherweise gar nicht bewusst sind. Daher können sich diese Unternehmen ganz auf ihr Wachstum konzentrieren. Weitere Informationen finden Sie auf barracuda.com de.barracuda.com.