EINE WAF WÄHLEN, DIE FÜR SIE PASST

EIN PRAKTISCHER LEITFADEN

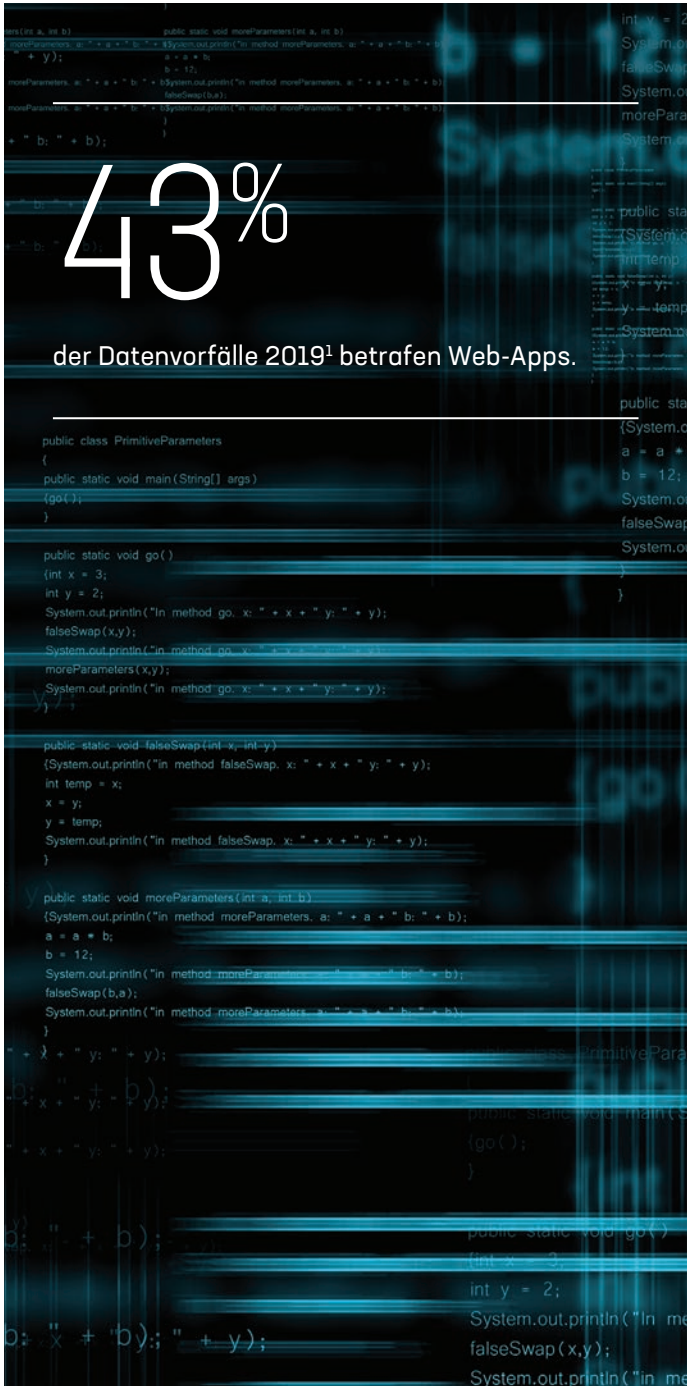
ZUR EINFÜHRUNG

Obwohl die Branche nach Kräften bemüht ist, sichere Praktiken in der Anwendungsentwicklung zu etablieren, hat die fortschreitende Dezentralisierung der Infrastruktur dazu geführt, dass die App-Implementierungen komplexer geworden sind – und entsprechend schwieriger zu schützen.

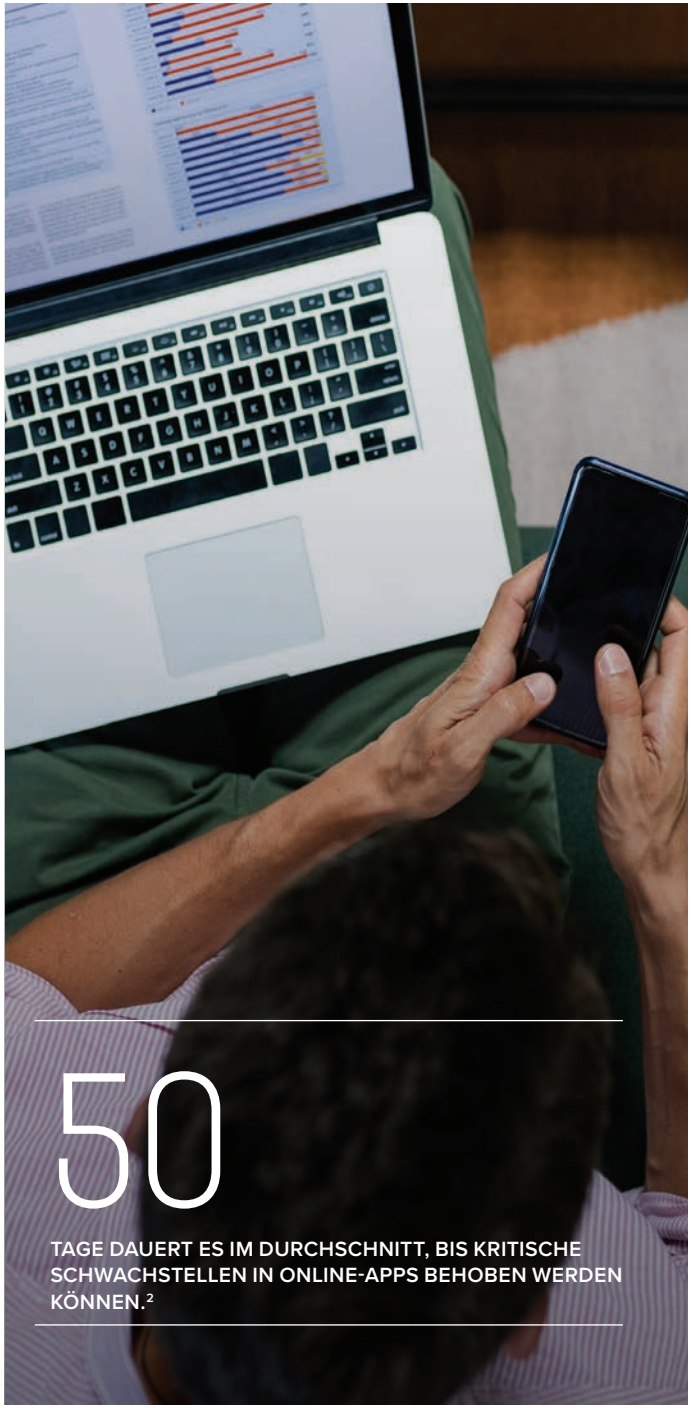
Der Data Breach Investigations Report 2020 von Verizon zeigt, dass 2019 nahezu die Hälfte aller Sicherheitsvorfälle Web-Anwendungen betraf. Dies sollte nicht überraschen – die heutigen dezentralisierten Multi-Cloud-Umgebungen, dazu Inhalte und Integrationen von Drittanbietern und neue Architekturen wie serverlose Umgebungen und Container ergeben komplizierte Implementierungen, was die Apps per se Risiken aussetzt.

Die gute Nachricht ist, dass es Tools gibt, die Ihnen helfen, Ihre Anwendungen gegen Sicherheitsverletzungen zu schützen, indem sie Schwachstellen eingrenzen und Angriffe stoppen. Zu diesen Tools gehören speziell Web Application Firewalls (WAFs). Eine WAF bietet sozusagenvirtuelle Patches für Schwachstellen in Code und Software, prüft aber auch den ein- und ausgehenden Anwendungsverkehr, erkennt und blockiert Scanner, Angreifer und Bots; die App-Performance für legitime Anwender bleibt dabei voll erhalten und wird sogar beschleunigt. Eine WAF kann auch für die Sicherheit Ihrer APIs sorgen, die die Grundlage moderner Anwendungen sind und daher ein beliebtes Ziel von Angreifern (und zwar mit viel Erfolg).

Unabhängig von der Anwendungsarchitektur und der Angriffsfläche können Sie eine WAF in unterschiedlichen Formen einsetzen, um Ihr Unternehmen vor Angriffen zu schützen. Zu diesen Formen gehören physische oder virtuelle Appliances, ob im Eigenbetrieb, als Cloud-Bereitstellung, als Container-Implementierung oder ausgelagert als spezieller Managed Service.



[1] https://enterprise.verizon.com/resources/reports/dbir/



50

TAGE DAUERT ES IM DURCHSCHNITT, BIS KRITISCHE SCHWACHSTELLEN IN ONLINE-APPS BEHOBEN WERDEN KÖNNEN.[2]

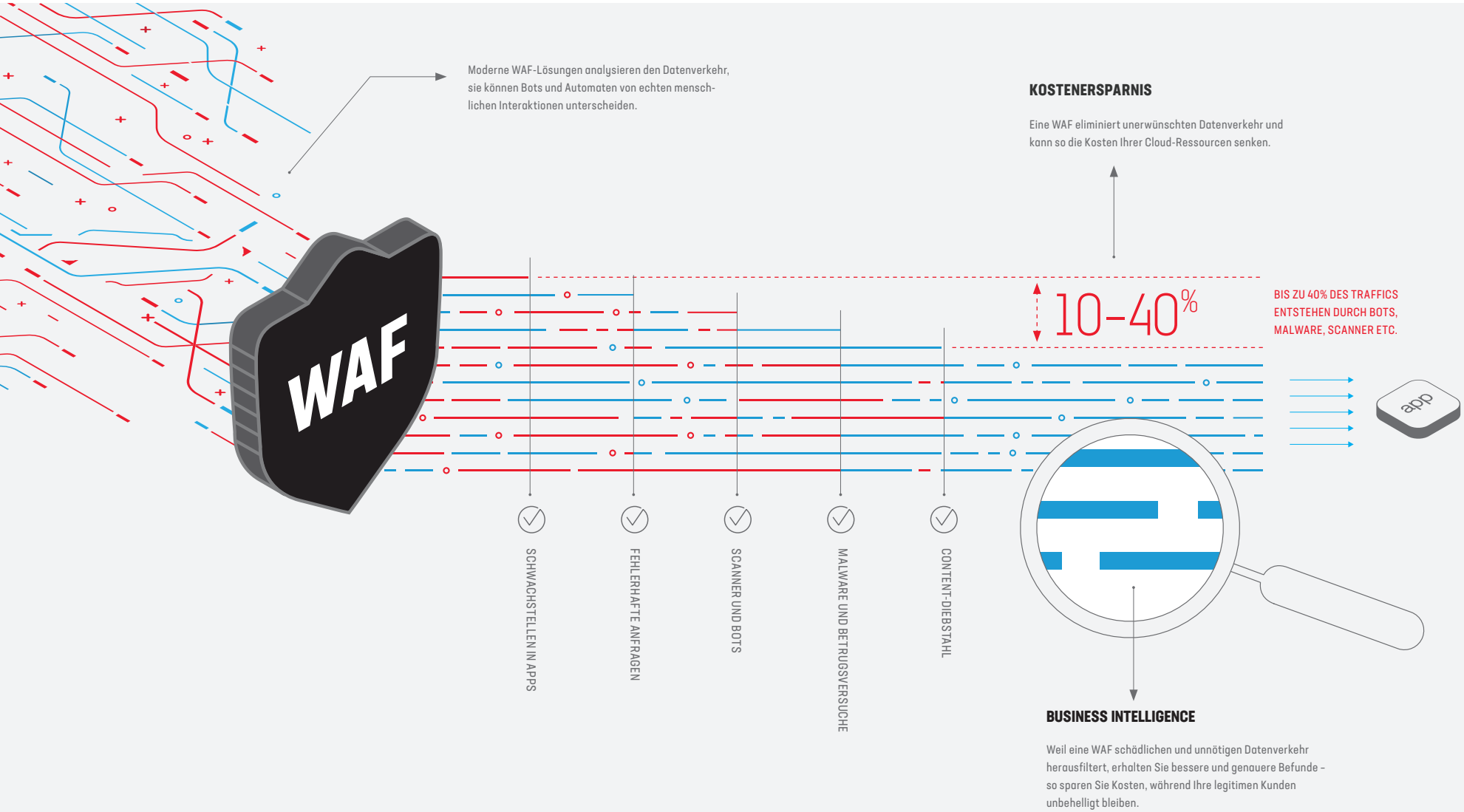
BRAUCHEN SIE EINE WAF? ES KOMMT DARAUF AN, WAS SIE HABEN.

- Haben Sie im Web öffentlich zugängliche Assets oder Mobilanwendungen?
- Haben Sie schützenswerte Assets im Web oder eine mobile Anwendung?
- Haben Sie mit Bots und ungebetenem automatisierten Traffic zu kämpfen?
- Haben Sie Compliance-Verpflichtungen?
- Haben Sie Software-Stacks, die Sie nur mühsam aktualisieren können?
- Haben Sie Ihre APIs gesichert? Oder noch nicht?
- Haben Sie ältere Web-Anwendungen in Betrieb?
- Haben Sie die dauernde Furcht vor Zero-Day-Angriffen satt?
- Haben Sie Lust, Ihre Time-to-Market durch Integration einer sauberen CI/CD-Pipeline deutlich zu verkürzen?

Wenn Sie eine dieser Fragen mit Ja beantwortet haben und überlegen, wie Sie Ihre Anwendungen, Ihre Daten und Ihr Unternehmen vor App-Angriffen und Datendiebstahl schützen wollen, dann sollten Sie eine fortschrittliche WAF in Betracht ziehen.

Wie bei jedem guten Werkzeug gibt es auch bei WAFs diverse Optionen. Für jede Ausgangssituation gibt es eine Lösungsvariante, die am besten geeignet ist.

[2] https://techbeacon.com/security/30-app-sec-stats-matter



EINE WAF SPART CLOUD-KOSTEN UND ERGIBT BESSERE BUSINESS INTELLIGENCE

Indem Sie Ihren Cloud-Apps eine WAF vorschalten, sparen Sie bares Geld und gewinnen obendrein die datentechnischen Erkenntnisse, die Ihr Unternehmen braucht. Weil eine WAF unerwünschten Traffic herausfiltert, profitieren Sie außerdem von weniger verrauschten Protokollen und einem geringeren Aufwand bei Analysen und Vorfallsreaktion.

Ein paar weitere Fragen werden Ihnen helfen, das für Ihr Unternehmen geeignete Bereitstellungsmodell mit den für Sie entscheidenden WAF-Funktionen zu finden.

1 KÖNNEN SICHERHEITSWERKZEUGE ECHTEN MEHRWERT BRINGEN?

Sicherheitsausgaben zu rechtfertigen, ist oft schwierig. Klar, wir wissen alle, dass wir eine solide Verteidigung brauchen; und wir hoffen sehr, dass wir im Fall eines Angriffs sicher sind. Aber man weiß ja nie, wann man angegriffen wird, und schon gar nicht, ob Firewall oder IPS dann in der Lage sind, das Netzwerk effektiv zu schützen. Sicherheit wird oft als notwendiges Übel betrachtet, das keinen quantifizierbaren ROI abwirft. Manchmal aber doch.

In der Welt von Cloud Computing und Big Data können gute Sicherheitslösungen tatsächlich Geld sparen. Denn sie tragen dazu bei, Ihre Web-Anwendungen und digitalen Assets zu optimieren – und zwar indem sie Ihr Unternehmen vor Angriffen schützen. Moderne WAF-Lösungen filtern den Datenverkehr, sodass Sie besser zwischen automatischen Bots und echten Menschen unterscheiden können. Das ist wichtig, denn weil immer mehr Cloud-Service-Provider nach Verbrauch abrechnen, kann der betriebswirtschaftlich wertlose Bot-Traffic Ihre Infrastrukturkosten gewaltig in die Höhe treiben.

Wenn Sie eine WAF den größten Teil dieses Bot-Traffics eliminieren lassen, so optimieren Sie damit zugleich Ihre Web-Assets auf Ihre anvisierte Kundenbasis. Nutzlosen oder schädlichen Datenverkehr zu reduzieren, führt außerdem zu erheblichen Kosteneinsparungen. Sie können dann sicher sein, dass Sie nur für Ihre wirklichen bzw. potenziellen Kunden arbeiten. Ihre Sicherheitstools bieten also einen echten Mehrwert, indem sie helfen, Ihre Cloud-Kosten zu kontrollieren.

Hinzu kommt noch, dass die Daten zur Interaktion mit den Kunden an Qualität gewinnen, sodass Sie mit einer WAF auch Ihre Business Intelligence stärken. Mit belastbaren Daten, denen Sie trauen können, sind Sie besser in der Lage, effektiv an Ihre wirklichen Kunden zu vermarkten.

OPTIONEN ZUR AUSWAHL

IM EIGENBETRIEB

Eine WAF, die vom Unternehmen selbst gemanagt wird – ob vor Ort oder in einer Cloud –, gibt Ihnen volle feingranulare Kontrolle: Sie können sie exakt so konfigurieren, dass sie Ihre Anwendungen optimal schützt. Eine WAF, die jede Anwendungsarchitektur unterstützt, ob klassisch oder in Containern, bietet echten Mehrwert, der weit über die reine Schutzfunktion hinausgeht. Mit dynamischen Signaturen blocken Sie selbst neue, zuvor unbekannte Bedrohungen.

ALS CLOUD-SERVICE (SaaS)

Eine WAF as a Service senkt Ihre Kosten und den Aufwand für den Betrieb der Lösung – bei fast ebenso großem geschäftlichem Nutzen: Der Funktionsumfang ist vergleichbar mit einer eigenen WAF vor Ort, nur dass diese Option sofortigen Schutz vor Anwendungsschwachstellen leistet. Das bedeutet weniger Risiken und weniger Kosten im Ernstfall.

In der Welt von Cloud Computing und Big Data können Sie mit Sicherheitslösungen tatsächlich bares Geld sparen.

2 WOLLEN SIE SICH MIT SECURITY HERUMSCHLAGEN? ODER SICH UM IHR KERNGESCHÄFT KÜMMERN?

Laut State of Application Services Report 2020 von F5 klagen 71% der Unternehmen über Fachkräftemangel im Bereich Sicherheit. Wo das Know-how im Umgang mit den notwendigen Sicherheitstools fehlt, wächst naturgemäß der Zweifel daran, ob diese Werkzeuge die vertraulichen Daten des Unternehmens auch wirklich schützen können. Verschärft wird dieses Qualifikationsdefizit noch dadurch, dass es gilt, Security einheitlich und ohne Rücksicht auf Anwendungsarchitekturen und Infrastrukturen zu gewährleisten – in vielen Fällen sogar über mehrere Cloud-Anbieter hinweg. Obendrein sind bestimmte Bedrohungsvektoren, speziell Angriffe, die gezielt ein bestimmtes Unternehmen oder deren digitales Eigentum ins Visier nehmen, nur schwer zu kontern. Das Problem ist letztlich – es sei denn, Sie haben ein Sicherheitsteam mit unbegrenzten Ressourcen –, dass Sie wahrscheinlich nicht Ihre ganze Zeit damit verbringen wollen, die vielen einzelnen Sicherheitsrisiken Ihrer Apps zu managen.

Sie wollen vermutlich eine Sicherheitslösung, die einfach funktioniert, damit Sie sich auf andere, geschäftskritische Ziele konzentrieren können. Zum Glück gibt es WAF-Optionen, die genau das können. Noch besser: Laut Application Protection Report 2019 von F5 Labs bietet eine WAF genau die technischen Kontrollen, die Sie brauchen, um sich vor vielerlei Bedrohungen zu schützen, die Datenverluste zur Folge haben können, etwa vor Injection-Angriffen und Credential Stuffing.

Dass eine WAF immer dazu da ist, Ihre Anwendungen zu schützen, ist klar. Aber je nach Art der Implementierung eignet sich die ein oder andere Form besser für ein bestimmtes Unternehmen. Glücklicherweise gibt es mehrere Optionen.

OPTIONEN ZUR AUSWAHL

ALS CLOUD-SERVICE (SaaS)

Aktivieren Sie einfach eine WAF as a Service, und schon sind Ihre Anwendungen vor tausenderlei Bedrohungen sicher, die von F5 identifiziert und mit Wahrscheinlichkeitswerten gewichtet sind, damit Fehlalarme auf ein Minimum beschränkt bleiben. Ohne Infrastruktur-Overhead wie Hardware und Software oder die Sorge um Updates ist dies eine passgenaue Lösung, mit der Ihre Entwicklerteams bei wenig Aufwand vernünftige Sicherheit integrieren können.

ALS MANAGED SERVICE

Damit schützen Sie Ihre Web-Apps und Online-Daten vor Bedrohungen, die sich laufend weiterentwickeln, und bekommen dazu 24×7-Support. Eine WAF als Managed Service ergänzt (oder ersetzt) Ihre eigenen internen Ressourcen, sie wird komplett in einem Security Operations Center eingerichtet, bereitgestellt und gewartet, und zwar von zertifizierten Experten, die Ihren Datenverkehr immer im Blick behalten.

Wenn Sie eine Sicherheitslösung suchen, die einfach funktioniert, gibt es dafür eine ganze Reihe von Möglichkeiten.

3 WOLLEN SIE VORSCHRIFTEN ERFÜLLEN? ODER HABEN SIE MEHR VOR?

Viele Unternehmen sind mit ihrer Security ganz zufrieden, erwägen aber die Einführung einer WAF aufgrund von Compliance-Anforderungen oder Audit-Ergebnissen. Dann bieten sich diverse Einsteiger-WAFs an, mit denen man diesen Punkt abhaken kann. Es zeigt sich jedoch bald, dass eine solche „WAF nach Vorschrift“ unterm Strich teuer kommt.

Einfache WAFs bringen Sie vielleicht durchs Audit, aber sie sind schlicht nicht mit Blick auf die betriebliche Handhabung entwickelt und bereiten oft mehr Kopfschmerzen als sie beseitigen (nämlich falsch positive bzw., schlimmer noch, falsch negative Meldungen). Weil sie außerdem nicht den Funktionsumfang einer voll ausgebildeten, robusten WAF bieten, sind Sie unter Umständen nicht wirklich besser geschützt – obwohl Sie soeben Geld dafür ausgegeben haben.

Das können Sie besser. Wenn Sie aus Compliance- oder Audit-Gründen eine WAF brauchen, warum dann nicht gleich eine, die mehr als nur das Mindestmaß an Schutz bietet? Mit einer ordentlichen WAF erfüllen Sie Ihre Vorgaben und verschaffen sich außerdem die Transparenz, die Sie brauchen, wenn Sie Ihr tatsächliches Risiko richtig einschätzen wollen (statt nur auf das wahrgenommene Risiko zu reagieren). Da gibt es meist Grund zum Staunen. Das hat zuletzt eine Studie von 2019 gezeigt, aus der hervorgeht, dass 75 % des Softwarecodes von Unternehmen Schwachstellen aufweisen.

OPTIONEN ZUR AUSWAHL

IM EIGENBETRIEB ODER ALS CLOUD-SERVICE (SaaS)

Entweder kann ihr Team die WAF selbst implementieren und veralten – egal ob in klassischen Umgebungen oder in Container-Szenarien mit Automatisierungspipelines –, oder Sie beziehen die WAF als Cloud-Service, der einen Großteil der Betreuung übernimmt. In beiden Fällen bekommen Sie feingranulare Analytics-Resultate an die Hand. Die Auditoren sind damit zufrieden – und die Sicherheitslage Ihres Unternehmens hat sich damit effektiv verbessert.

ALS MANAGED SERVICE

Am bequemsten ist natürlich die Option, bei der Sie sich nicht selbst um die Compliance-Aufgaben Ihrer WAF kümmern müssen. Diese Verantwortung liegt bei dem Expertenteam, das Ihre Anwendungen vor Angriffen schützt – und damit jenseits von Audits und Compliance echten Schutz bietet.

Mit einer WAF werden Sie Ihren Compliance-Anforderungen gerecht und bekommen gleichzeitig das Plus an Sicherheit und Sichtbarkeit, das Sie fürs Geschäft brauchen.

4 WOLLEN SIE DEN ÜBERFLÜSSIGEN BOT-TRAFFIC LOSWERDEN UND SICH LIEBER IHREN ECHTEN KUNDEN WIDMEN?

Selbst wenn Ihre App-Entwicklung bereits stark und gesichert abläuft und Sie die Anwendungen, die Sie freigeben, im Prinzip für hinreichend sicher halten, haben Sie wahrscheinlich mit einem weiteren Problem zu kämpfen: dass ein hoher Prozentsatz des Webtraffics auf Ihren Seiten und bei Ihren Services von Automaten oder Bots herrührt. Auf den ersten Blick erscheint das als legitimer Datenverkehr. Aber Klicks von Bots nicht dasselbe wie Klicks von Menschen. Ungebetener und unrentabler Traffic kann Ihre Analysen und Ihre Marktwahrnehmung verzerren, weil er die Systeme mit täuschenden Daten überflutet.

Darüber hinaus werden Automatisierungstechniken auch von Angreifern verwendet, die damit Ihre Anwendungen systematisch nach Schwachstellen absuchen, Zugangsdaten abgreifen oder DoS-Angriffe (Denial of Service) reiten. Eine fortschrittliche WAF mit proaktivem Bot-Schutz stellt sich diesen automatisierten Angriffen, sie kombiniert Realbefunde mit verhaltensbasierten Techniken, um Bot-Traffic zu identifizieren und zu stoppen – gute Nachrichten also für alle Unternehmen, die mit einer ständig zunehmenden Bot-Last auf ihren digitalen Assets zu kämpfen haben. Eine anpassungsfähige WAF enthebt Sie dieser lästigen Aufgabe, sodass Sie sich auf Ihre echten Kunden konzentrieren können.

OPTIONEN ZUR AUSWAHL

IM EIGENBETRIEB

Damit starten Sie einen proaktiven Bot-Schutz, der Ihre Anwendungen vor Layer-7-DoS-Angriffen, Web Scraping und Brute-Force-Attacken schützt – bevor sie den Ruf Ihres Unternehmens ruinieren.

ALS MANAGED SERVICE

So sichern Sie Ihre Web-Apps vor Bot-Bedrohungen und bekommen dazu noch 24×7-Support. Weil sie bösartige Bots erkennt, die Standard-Erkennungsmethoden bereits umgehen, schützt eine betreute Cloud-Lösung auch vor Betrugsmaschen über Anwendungen wie Kontoübernahme, Missbrauch bei der Erstellung neuer Konten, Betrug mit Treuekonten und mehr.

Mit einer anpassungsfähigen WAF-Technologie bekommen Sie unerwünschten Bot-Traffic in den Griff.

5 WISSEN SIE, WAS IHRE APIS TREIBEN? OB SIE AUCH SICHER SIND?

Weil der wahre Wert der meisten Apps sich erst aus der Vielzahl von Partnerschaften und Integrationen ergibt, werden praktisch alle neuen Anwendungen mit eingebauten Schnittstellen (APIs) entwickelt. Wenn man aber die rasant wachsende Zahl von Vorfällen aufgrund von fehlkonfigurierten APIs als Gradmesser nimmt, dann sind die APIs das Erste, was es zu schützen gilt.

API-Management und API-Sicherheit müssen an den strategischen Punkten der Entwicklungspipeline implementiert werden. Um sicherzustellen, dass alle APIs geschützt sind, senden Sie Ihre Swagger- bzw. OpenAPI-Dateien automatisch an die WAF, damit deren Schutz von Anfang an greift. Eine voll ausgebildete WAF bewahrt APIs vor allen gängigen Web-Angriffen, z. B. vor Injection oder Cross-Site-Scripting (XSS), kann aber auch noch andere Attacken auf Serverressourcen abwehren, etwa indem sie den Grad der Exponiertheit einschränkt, Protokollkonformität erzwingt oder den Durchsatz begrenzt.

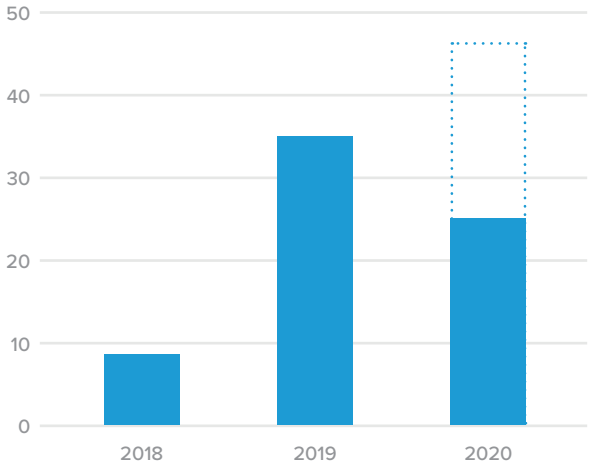


Abb. 1: API-Vorfälle 2018 bis Mitte 2020.
Bei der derzeitigen Zunahme werden sich für 2020 mehr API-Vorfälle ergeben als in den beiden vorangegangenen Jahren zusammen.[3]

[3] https://www.f5.com/labs/articles/threat-intelligence/2020-apr-vol1-apis-architecture

OPTIONEN ZUR AUSWAHL

IM EIGENBETRIEB

Eine WAF schützt APIs vor all den Angriffen, denen jede Web-Anwendung ausgesetzt ist. Aber sie muss außerdem die automatische Übergabe benutzerdefinierter Sonderregeln für jede einzelne exponierte API ermöglichen. Eine fortschrittliche WAF, die vor die Anwendung geschaltet oder in die Komponenten einer Container-Anwendung integriert ist, ermöglicht Ihnen ein effektives Management Ihrer API-Sicherheit.

ALS MANAGED SERVICE

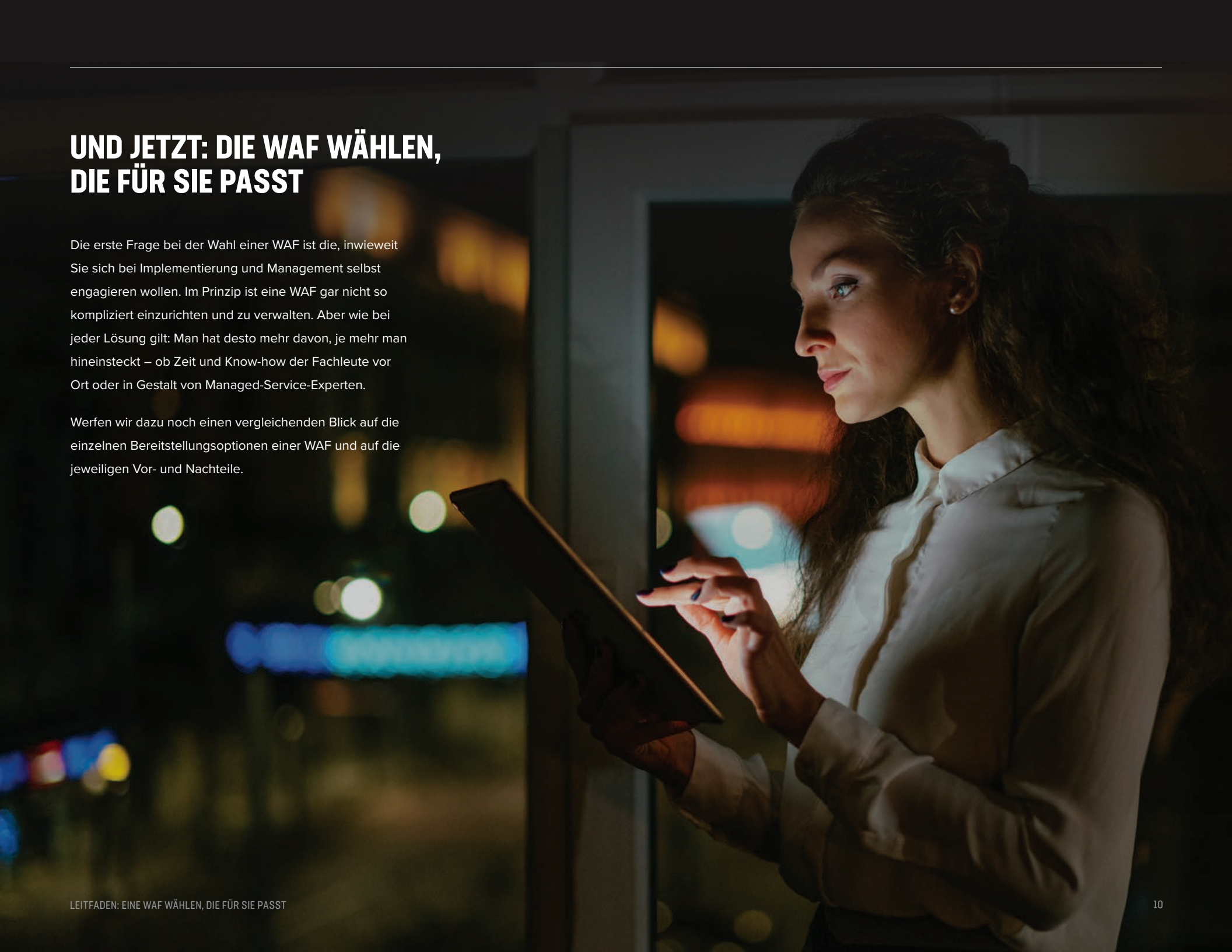
Eine vergleichbare Integration funktioniert auch als Managed Service, der dann automatisch die übergebenen API-Konfigurationsdateien aufnimmt. Das Resultat: 24×7 Schutz und Support für Ihre Apps und deren Schnittstellen. Status und Performance der Anwendungen werden genau verfolgt, sodass Ihre Experten vor Ort bei Bedarf jederzeit Richtlinienänderungen vornehmen können.

Eine fortschrittliche WAF sorgt für API-Sicherheit direkt aus der Entwickler-Pipeline.

UND JETZT: DIE WAF WÄHLEN, DIE FÜR SIE PASST

Die erste Frage bei der Wahl einer WAF ist die, inwieweit Sie sich bei Implementierung und Management selbst engagieren wollen. Im Prinzip ist eine WAF gar nicht so kompliziert einzurichten und zu verwalten. Aber wie bei jeder Lösung gilt: Man hat desto mehr davon, je mehr man hineinsteckt – ob Zeit und Know-how der Fachleute vor Ort oder in Gestalt von Managed-Service-Experten.

Werfen wir dazu noch einen vergleichenden Blick auf die einzelnen Bereitstellungsoptionen einer WAF und auf die jeweiligen Vor- und Nachteile.



OPTIONEN DER WAF-BEREITSTELLUNG

	PRO	CONTRA
 **ALS MANAGED SERVICE**	Mit dieser Option wählen Sie den schnellsten und bequemsten Weg, um Ihren Apps eine WAF samt DDoS- und Betrugsabwehr vorzuschalten. Diese Variante dürfte auch das beste Mittel sein, Anwendungsbetrug zu erkennen und zu stoppen, weil sie mit Threat Intelligence aus Angriffsprofilen und Risikooberflächen arbeitet, was maximale Wirksamkeit verspricht – zusätzlich zu den Service-Experten rund um die Uhr.	Eine komplett gemanagte WAF as a Service ist das Bereitstellungsmodell, das am schnellsten gestartet ist. Allerdings haben Sie architektonisch nicht ganz so viel Freiraum, bei manchen Angeboten z. B. keine direkte Admin-Kontrolle über Ihre Sicherheitsrichtlinien. Und: Ein Managed Service ist in der Regel die teurere Option (wenn auch immer noch günstiger als die entsprechenden Security-Vollzeitstellen).
 **IM EIGENBETRIEB**	Größtmögliche Flexibilität und Policy-Portabilität auch über komplexe Multi-Clouds hinweg, bei voller Kontrolle über Traffic-Management und Sicherheitsrichtlinien – diese Karte zieht man bei anspruchsvollsten Bereitstellungsszenarien, in denen es auf architektonische Freiheit, optimierte Leistung und erweiterte Security-Anforderungen ankommt.	Beim Bereitstellungsmodell Eigenbetrieb müssen Security-Team und App-Eigentümer selbst Hand anlegen und die Sicherheitsrichtlinien erstellen und implementieren, die für Ihre Anwendungen gelten sollen. Das rentiert sich für diejenigen Unternehmen, die ein derart flexibles Modell brauchen.
 **ALS CLOUD-SERVICE**	Dies ist eine der einfachsten Möglichkeiten, eine Cloud-WAF zu starten: Mit Auto-Provisioning setzen Sie eine Sicherheitsrichtlinie in Kraft, die Ihrem Bedarf nach einfachem, kostengünstigen Sofortschutz gerecht wird.	Je nach der Architektur Ihrer Anwendungen bietet dieses Modell möglicherweise nicht so viel Flexibilität wie andere.

FAZIT

Auch wenn die Auswahl nicht ganz leicht fällt – der Zeitpunkt, sich für eine Web Application Firewall zu entscheiden, war noch nie so günstig wie heute. WAF-Technologie ist heute einfacher zu bekommen, erschwinglicher und leichter zu verwalten als je zuvor – und das ist auch gut so, denn Unternehmen brauchen den Schutz, den eine WAF bietet, heute mehr denn je.

Mehr Infos zur Auswahl der WAF, die für Sie passt, finden Sie auf f5.com/security.

APP-SICHERHEIT ALS ERSTES

Apps, die always on und immer connected sind, können Ihr Unternehmen wachsen lassen und verändern – aber sie sind auch Einfallstore zu Daten, die Ihre Firewall nicht mehr schützen kann. Weil die meisten Angriffe auf Apps abzielen, schützen Sie Ihr Geschäft am besten, indem Sie die Apps absichern, die es nach vorne bringen.

Mehr Security-Infos finden Sie auf f5.com/solutions.

US Headquarters: 801 5th Ave, Seattle, WA 98104 | 888-882-4447 // Americas: info@f5.com // Asia-Pacific: apacinfo@f5.com // Europe/Middle East/Africa: emeainfo@f5.com // Japan: f5j-info@f5.com