Geschwindigkeit. Agilität. Sicherheit.

Fachartikel
Martin Burkhart, Dr. sc. ETH Zürich
Head of Product Management Airlock, Ergon Informatik AG

Erschienen im Ergon Magazin 2019
SMART insights

ergon

Die digitale Transformation erfasst immer mehr Branchen und beschleunigt die Evolution von Web-Technologien. Diese Entwicklung macht auch vor Sicherheitslösungen nicht Halt. Der Trend zeigt klar in Richtung einer Konvergenz von Application Security, API Security und Access Management. Die Nutzen dieses integrierten Ansatzes sind vielseitig und zeigen sich beispielsweise in einer kürzeren Time-to-Market für Projekte und einer tieferen Total Cost of Ownership. Die erfolgreiche Digitalisierung erfordert aber eine effektive Kombination aus Management und IT-Kompetenzen. Security-Spezialist Martin Burkhart gibt Einblicke.

Web Application Firewalls müssen dazulernen

Eine WAF (Web Application Firewall) ist ein Filter, der sich vor einer Web-Applikation (auch Web-Anwendung) befindet und den eingehenden Datenverkehr auf potenzielle Bedrohungen und bösartige Aktivitäten untersucht. Es ist eines der gebräuchlichsten Mittel zum Schutz vor Angriffen auf der Applikationsebene. Nachlässigkeiten beim Schutz vor applikatorischen Bedrohungen können sich schnell und nachhaltig schädigend auswirken, beispielsweise indem sensible Kundendaten verloren gehen und der Ruf des Unternehmens leidet.

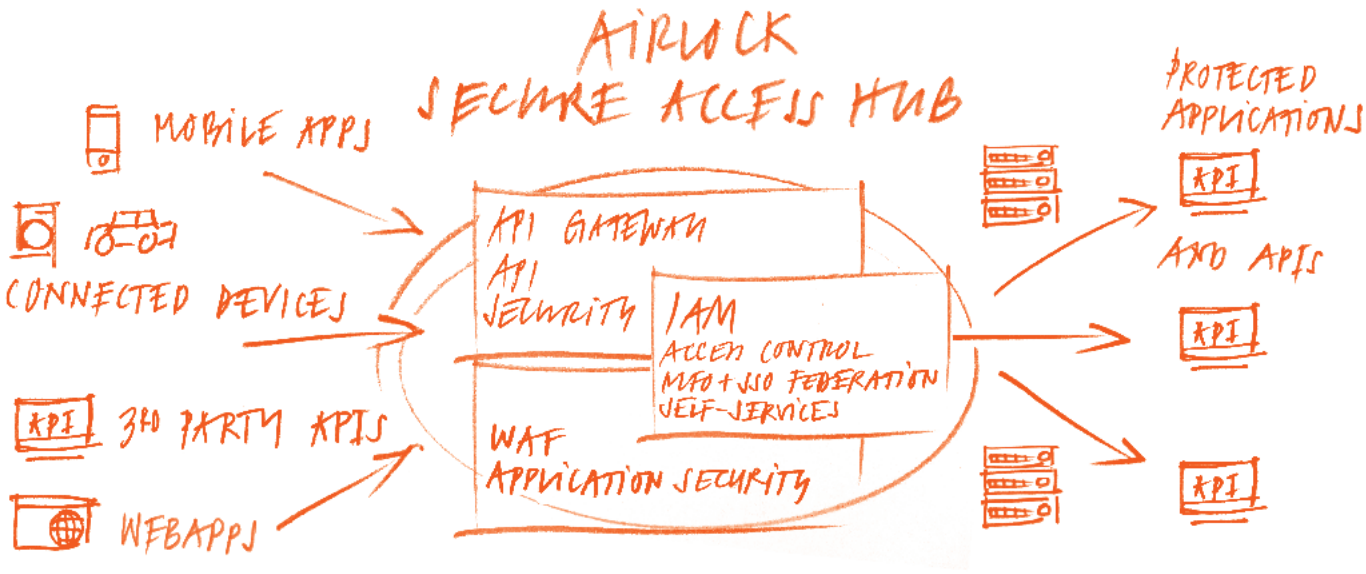
Durch die fortschreitende Digitalisierung und die damit einhergehende starke Verbreitung von Web-Applikationen ist der heutige WAF-Markt global, milliardenschwer und hochkompetitiv geworden. Doch es gibt bereits Anzeichen für bevorstehende Verwerfungen. Die digitale Evolution treibt auch die Anforderungen an ein besseres und interaktiveres Nutzererlebnis voran. Web-Applikationen werden deshalb heute nach einem neuen Paradigma entwickelt, welches vermehrt auf die Integration und Vernetzung von unterschiedlichen Diensten, sogenannten APIs (Application Programming Interfaces), setzt. Herkömmliche Web-Applikationen, für die WAFs ursprünglich entwickelt wurden, werden mit der Zeit aussterben. Das Analystenhaus Gartner prognostiziert, dass bis 2021 65% der neuen Web-Applikationen auf APIs basieren.

APIs als Business Enabler

Die Verwendung solcher APIs eröffnet Unternehmen neue geschäftliche Chancen, stellt sie aber auch vor technische Herausforderungen. APIs vereinfachen die schnelle Bereitstellung innovativer Dienstleistungen, womit neue Umsatzquellen erschlossen werden können. Das Benutzererlebnis kann zudem verbessert und Dienste von Drittanbieten, wie z.B. Partnerdienste, können einfacher in eigene Dienstleistungen integriert werden.

«In naher Zukunft könnte dies bedeuten, dass Kunden Google oder Facebook benutzen, um Rechnungen zu bezahlen.»

Martin Burkhart, Dr. sc. ETH Zürich,
Head of Product Management Airlock
martin.burkhart@ergon.ch



Im Airlock Secure Access Hub konvergieren verschiedene Security-Technologien

API Security bedeutet Web-Security
Die Verwendung von APIs bringt allerdings auch neue Risiken mit sich. Business-Schnittstellen und interne Daten werden durch APIs viel direkter im Internet exponiert als früher. Mobile Apps und smarte «Things» nutzen die APIs direkt und global. Die Kapselung durch eine umfangreiche Anwendung, wie dies bei herkömmlichen Web-Applikationen der Fall war, entfällt weitestgehend. Auch Angreifer können nun direkt auf die unterliegenden APIs zugreifen. Damit sind APIs prinzipiell denselben Sicherheitsrisiken (z.B. den OWASP Top 10) ausgesetzt wie jede Web-Applikation.

Traditionelle Sicherheitsprodukte für APIs (z.B. XML Gateways) sind nur bedingt tauglich, den geforderten Schutz in der schönen neuen Welt zu leisten. Die modernen Anwendungen sind durch Agilität und Leichtgewichtigkeit geprägt. In den letzten Jahrzehnten kamen APIs meist im geschützten B2B-Umfeld zum Einsatz und die Interaktionsmöglichkeiten waren durch umfangreiche Standards eingeschränkt. Web-Security-Themen waren dabei von untergeordneter Bedeutung. Was es braucht, sind moderne API Gateways, welche mit den heutigen Anforderungen an APIs klarkommen und Web-Security-Aspekte zuverlässig abdecken.

APIs brauchen Access Management
Der wichtigste Grund für den Einsatz von API Gateways ist allerdings die Zugriffskontrolle (Access Management). Der Zugriff auf APIs muss von aussen ermöglicht und mittels verschiedener Standards (wie z.B. OAuth 2.0, OpenID Connect und SAML) abgesichert werden können. Dazu gehört nicht nur die Autorisierung, sondern auch eine Authentisierung der Benutzer. Dies wiederum erfordert eine Integration mit einem einheitlichen Web-Login, einem Single-Sign-On sowie einem Identity und Access Management (IAM) System.

Mittlerweile gibt es sogar regulatorische Richtlinien, die die Öffnung von APIs fordern. Ein Paradebeispiel hierfür ist PSD2, die European Payment Services Directive 2, eine neue EU-weite Richtlinie, die das Bankwesen, wie wir es kennen, verändern wird. Kurz gesagt, PSD2 ermöglicht es Bankkunden, sowohl Verbrauchern als auch Unternehmen, Drittanbieter für die Verwaltung ihrer Finanzen zu nutzen. In naher Zukunft könnte dies bedeuten, dass Bankkunden Facebook oder Google verwenden, um Rechnungen zu bezahlen, Überweisungen zu tätigen oder ihre Ausgaben zu analysieren, während ihr Geld immer noch sicher auf ihrem Bankkonto liegt. Banken sind in der EU dazu verpflichtet, diesen Drittanbietern über offene APIs Zugang zu den Konten ihrer Kunden zu gewähren. Dies wird es Dritten ermöglichen, Finanzdienstleistungen zusätzlich zu den Daten und der Infrastruktur der Banken aufzubauen. Dieser Zugriff muss selbstverständlich stark authentisiert erfolgen, um Sicherheitsrisiken im Zaum zu halten.

IAM und die Kunden
IAM-Produkte dienen generell der Kontrolle von Benutzerzugriffen auf kritische Informationen innerhalb eines Unternehmens. Bei der Identitäts- und Zugriffsverwaltung geht es darum, die Rollen und Zugriffsrechte einzelner Benutzer und Benutzergruppen zu definieren und zu verwalten. Umstände, unter denen Benutzern diese Rechte gewährt oder verweigert werden, werden definiert. Diese Benutzer können interne Mitarbeiter, aber auch externe Partner oder Kunden sein.

Im Unterschied zu Enterprise-IAM-Systemen sind sogenannte Customer IAM (cIAM) Lösungen besser auf die Verwaltung von heterogenen, externen Benutzergruppen ausgelegt. cIAM-Systeme bieten einfache Skalierbarkeit mit grossen Benutzerzahlen und ein nahtloses Nutzererlebnis durch integrierte Benutzeroberflächen. Mittels sogenannter User-Self-Services können Benutzer ihren Zugriff und ihre Daten eigenständig verwalten. Dazu gehören Funktionen wie z.B. ein Passwort zurücksetzen, Profildaten aktualisieren, Geräte registrieren oder die Zustimmung zur Verarbeitung persönlicher Daten (DSGVO/GDPR). Dies sind wichtige Aspekte, denn Benutzer digitaler Kanäle sind nicht bereit, Zeit in Helpdesk-Warteschleifen zu verschwenden. Sie möchten Probleme selbst lösen können, dann, wenn sie Zeit haben. Natürlich soll der Zugriff nicht unnötig durch mühsame mehrstufige Authentisierungsverfahren erschwert werden. Dafür ist eine hohe Flexibilität gerade auch in der Benutzerauthentisierung entscheidend. Abhängig von der gewünschten Aktion und dem Kontext des Zugriffs kann das identifizierte Risiko variieren. Eine adaptive Authentisierung muss sicherstellen, dass die Sicherheitsanforderungen erfüllt werden, ohne die Benutzer mit unnötigen Fragen zu belästigen.

Mehr als die Summe seiner Teile
Wohin führt das alles? WAFs müssen also APIs schützen, API Gateways wiederum müssen Web-Security lernen, APIs brauchen Access Control und die Benutzer, die daherkommen, lassen sich schlecht mit herkömmlichen Enterprise-IAM-Systemen verwalten. Zudem wissen wir alle um die Nachteile von «Spot Solutions», die nicht über den eigenen Tellerrand blicken und viele Lücken an den Übergängen offenlassen.

Der Airlock Secure Access Hub integriert zukünftige Anforderungen an sicheres Access Management in einer abgestimmten und kohärenten Lösung, bestehend aus einer WAF, einem API Gateway und einem Customer-IAM-System. Durch intelligente Schnittstellen sind die einzelnen Komponenten aufeinander abgestimmt. Aufgrund unserer mittlerweile 20-jährigen Erfahrung im Schutz von sensiblen Web-Applikationen sind wir überzeugt, dass dies der richtige Weg für nachhaltige digitale Sicherheit ist.

Verkrustete Organisationsstrukturen – ein unerwartetes Hindernis
Ein weiteres, auf den ersten Blick eher unerwartetes Problem ist oftmals organisatorischer Natur: Wie kauft man einen Secure Access Hub, auf dem diverse Technologien zu einem grossen Ganzen konvergieren? Heute ist die Verantwortung für diese Themen meist in unterschiedlichen Abteilungen angesiedelt wie z.B. bei der IT-Infrastruktur, dem Netzwerkbetrieb, dem CIO oder der Benutzeradministration. Der Nutzen eines integrierten Ansatzes wie beispielsweise tiefere Total Cost of Ownership und schnellere Time to Market spürt wiederum das Business und die nahtlose Kundenerfahrung das Marketing, welche beide meist nicht in die Beschaffung von IT- Security-Lösungen involviert sind.

Die Digitalisierung verändert nicht nur Technologien, sondern erfasst auch Business-Prozesse und löst verkrustete Organisationsstrukturen auf. Grössere Flexibilität, Kollaboration und Agilität sind gefragt. Der Ball liegt damit nicht zuletzt beim Unternehmen selbst. Fortschrittliche Firmen stellen sich deshalb bereits heute den Fragen zu integrierter Security und bauen eine solide Basis für die digitale Zukunft.