Kombination bietet höchstmögliche Sicherheit

Filterung und Authentifizierung schützen Web-Applikationen

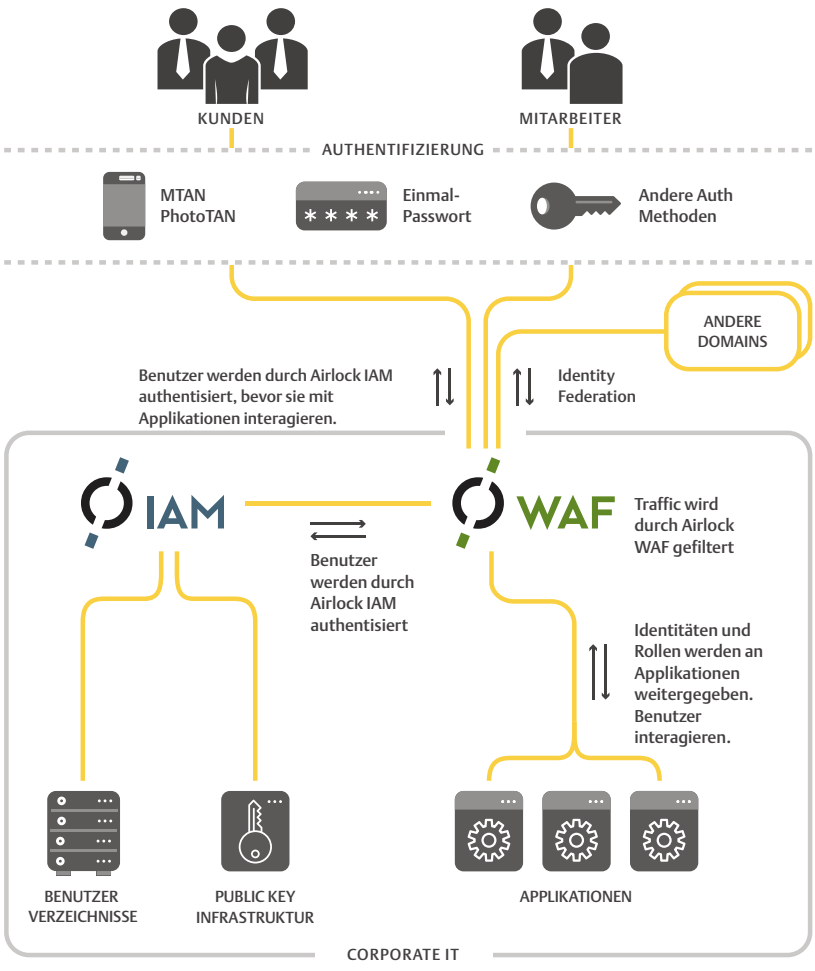
Angriffe auf Web-Applikationen setzen heute nicht mehr auf der Netzwerkebene an. Techniken wie SQL Injection oder Cross-Site Scripting zielen direkt auf die Applikationen und die dahinter liegenden Geschäftsdaten. Als Schutzmechanismus wird deshalb eine kombinierte Lösung aus vorgelagerter Filterung und Zugriffskontrolle unerlässlich. Damit reduzieren sich zugleich die Betriebskosten, und die Flexibilität für zukünftige Anforderungen steigt.

Von Martin Burkhart, Ergon Informatik AG

Der Trend weg von Rich-Clients mit darauf installiertem Software-Arsenal hin zum Fernzugriff auf Web-Applikationen ist ungebrochen und erhält durch vielfältige Cloud-Lösungen neuen Schub. Die Entwicklung beeinflusst inzwischen nahezu alle Szenarien des IT-Einsatzes: Mitarbeiter, die mobil auf alle Daten zugreifen wollen, Lieferanten, die online direkt im Bestellwesen arbeiten, oder Kunden, die über E-Banking, E-Commerce oder Kundenplattformen hochvertrauliche Daten erfassen. Nahezu jedes Unternehmen verwendet Microsoft Exchange und SharePoint oder ähnliche Systeme, um seinen Angestellten Arbeit an beliebigen Orten zu ermöglichen. ERP- und CMS-Lösungen bieten über das Web ihre Informationen auch online an. Die nächste Welle des Trends wird mit dem „Internet der Dinge" (IoT) bereits absehbar: TV-Geräte, Kühlschränke, Heizungen, Autos – nahezu für jedes technische Gerät ist bereits eine Internet-Anbindung via App verfügbar. Der Benutzerkomfort steigt, das Leben wird einfacher.

Neue Vorteile – neue Risiken

Eine schöne neue Welt also. Doch gilt dies uneingeschränkt? Mit den vielen Vorteilen entstehen leider auch viele neue Risiken, welche durch die integrierten Sicherheitsmaßnahmen der Web-Applikationen und die üblichen Security-Strategien meist nur unzureichend abgedeckt sind. Außerdem steigen Instandhaltungs- und Betriebskosten für Anbieter und Unternehmen. Web-Applikationen müssen unterschiedlichste Benutzerverzeichnisse anbinden, zwischen verschiedenen



WAF und IAM im Verbund (Bild: Ergon)

Gängige Denkfehler

Die Risiken, die von Angriffen auf Web-Applikationen ausgehen, werden häufig unterschätzt. Typische Reaktionen von CISOs lauten beispielsweise so:

— „Über Web-Applikationen erhält man keinen Zugriff auf die Systeme und Daten." Dies ist eine grundlegend falsche Annahme. Mittels Malware, Identitätsdiebstahl oder durch das Ausnutzen von Sicherheitslücken bei Standardkomponenten ist es für Hacker fast ein Kinderspiel, in die Systeme einzudringen und an die Daten zu kommen.

— „Die Sicherheit ist in den Applikationen bereits integriert." Auch dies stimmt leider nicht. Programmierer sollten ihr Möglichstes tun, um einen gewissen Grad an Security in die Anwendungen zu integrieren, aber die Mittel hierzu sind begrenzt. Schutz ist nur gegen bereits bekannte Risiken möglich, und das Ergebnis ist statisch. Das Stopfen immer wieder neu entdeckter Sicherheitslücken in den Applikationen wird aufwändig und zeitraubend, und oft ist es gar nicht möglich, wenn der Anwender nicht auch Hersteller der Software ist.

— „SSL reicht." Heartbleed hat eindrucksvoll bewiesen, wie verwundbar auch weltweite Standards wie SSL sein können.

— „Regelmäßiges Patching und Scanning genügt." Beides ist von immenser Bedeutung für die Sicherheit, greift aber erst nach Bekanntwerden von Exploits. Der BSI-Studie „Die Lage der IT-Sicherheit in Deutschland 2014" zufolge wurden während des Jahres 2014 in 13 ausgewählten gängigen Softwareprodukten 705 kritische Schwachstellen entdeckt, die effektiv von Angreifern ausgenutzt wurden. Die Schäden durch Zero-Day Exploits waren hierbei beträchtlich.

— „Bei uns ist noch nie etwas passiert", oder: „Es gab Angriffe, aber es wurde nichts gestohlen" – dies beides sind trügerische Annahmen. Bei gezielten Cyber-Spionage-Angriffen können nach Aussage von Isabel Münch, Referatsleiterin „Allianz für Cyber-Sicherheit" beim BSI, die Angreifer im Durchschnitt 243 Tage im Netzwerk des Opfers unbemerkt herumstöbern. Sagenhafte zwei Drittel dieser Angriffe werden dann zuerst von außenstehenden Personen entdeckt – noch bevor die betroffenen Security-Beauftragten aufmerksam werden.

— „Reverse Proxy und Netz-Firewall genügen" – auch dies trifft nicht zu, eben weil heutige Angriffe auf der Applikations- und nicht auf der Netzwerkebene stattfinden.

Zugriffsstufen unterscheiden und diverse Anmeldetechnologien unterstützen.

Und wie sieht es auf der Angriffsseite aus? Nirgends sind Angreifer so nah am gewünschten Ziel wie bei Web-Applikationen. Besonders schützenswerte Daten gelangen über das Standardprotokoll HTTP oft bis an die Außengrenze der „Line of Defense". Deshalb sind Web-Applikationen heute das attraktivste Ziel für elektronische Angriffe mit kriminellem Hintergrund. Heartbleed, Shellshock, Dragonfly, Soak-Soak oder Ebury zeigen eindrücklich, wie unzureichend aktuelle Security-Konzepte tatsächlich sind und wie schnell sensitive Informationen in falsche Hände gelangen können.

Die Konsequenzen einer Attacke sind häufig weitreichend: Imageverlust durch negative Presse, Erpressbarkeit, rechtliche Folgen aus dem unzureichenden Schutz vertraulicher Daten, Schadenersatzforderungen oder der Verlust vertraulicher Informationen. Die finanziellen Schäden können dabei so gravierend sein, dass sogar die Unternehmensfortführung auf dem Spiel steht. Deshalb sind Schutzmaßnahmen unerlässlich geworden, die die jeweils aktuelle Gefahrenlage direkt adressieren.

Schutz durch kombinierte Techniken

Um Web-Applikationen optimal abzusichern, braucht es die Kombination zweier schlagkräftiger Komponenten: Zunächst filtert eine zentrale Web Application Firewall (WAF) Angriffsversuche auf Applikationsebene heraus, dann forciert sie im Zusammenspiel mit einem Authentisierungsserver die Authentifizierung von Anwendern und die Autorisierung von Anfragen an die Applikationen. Dieses Gespann arbeitet zentral, vorgelagert und in einem Zug für alle Applikationen. Weiter stärken lässt sich der Schutz durch eine starke und flexible Multi-Faktor-Authentifizierung. Damit kann sichergestellt werden, dass Anfragen nur auf die Applikationen treffen, wenn sie

1. von autorisierten Benutzern kommen und
2. frei von Angriffsversuchen sind.

So wird effektiv auch das Ausnutzen von Sicherheitslücken unterbunden, da anonyme Angreifer aus dem Internet gar nicht mehr bis zu den Applikationen vordringen, um diese beispielsweise zu scannen.

Zentrale Sicherheit ermöglicht innovative Lösungen

Die Kombination aus WAF und vorgelagerter Authentisierung schützt nicht nur gegen die „OWASP Top 10" oder ermöglicht rasche PCI-DSS-Compliance. Entsprechende Lösungen sichern auch die Investitionen der Anwender und bilden ein solides Fundament für zukünftige Security-Anforderungen. Insbesondere erlaubt eine zentrale, integrierte Authentisierungsplattform die Umsetzung eines firmenweiten Single-Sign-On-Konzepts (SSO). Gleichgültig, ob Zugriffe vom internen Arbeitsplatz, vom mobilen Gerät unterwegs oder vom Zuhause der Kunden aus erfolgen – mit vorgelagertem Zugriffsschutz werden alle Access-Anfragen kontextabhängig verarbeitet und die Benutzeridentitäten passend zu den Applikationen

Fakten

- Zentraler und vorgelagerter Schutz gegen Angriffe auf Applikationsebene
- Steigerung der Verfügbarkeit und Performance der Applikationen durch Load Balancing, SSO und Beschränkung auf zugelassenen Traffic
- Schnelle Reaktionsfähigkeit auf neue Sicherheitsrisiken dank Virtual Patching für alle Applikationen
- Kostenreduktion durch User-Self-Service
- Gesteigerter Benutzerkomfort durch SSO
- Schnelle Erfüllung der PCI-DSS-Vorgaben
- Flexibel für alle Branchen einsetzbar
- Rechtliche Absicherung durch Schutz vertraulicher Daten
- Schutz gegen Imageverlust

weitergeleitet. Eine breite Auswahl an Authentifizierungsmitteln vereinfacht die flexible Umsetzung von starker Authentifizierung auf allen Kommunikationskanälen, ohne dass jede Zielapplikation jede Technologie selbst unterstützen muss. Dank moderner Standards wie SAML 2.0, OAuth 2.0 und OpenID Connect ist SSO auch über Unternehmensgrenzen hinweg und bei Zugriff auf Cloud-Lösungen möglich.

Ein weiterer Vorteil von vorgelagerter Authentisierung ist es, die Implementierung von Self-Services für Benutzer zu erleichtern. Gerade bei hohen Nutzerzahlen sind Helpdesks häufig mit einfachen, repetitiven Aufgaben ausgelastet – wie dem Registrieren oder Entsperren von Accounts oder dem Zurücksetzen von Kennwörtern. Self-Services entlasten die Support-Mitarbeiter, reduzieren aus diesem Grund erheblich die Kosten und verkürzen zudem die Wartezeiten der Nutzer.

Made in Switzerland

IT-Sicherheit und Datenschutz sind nicht erst seit der Spionage-Affäre um Edward Snowden ein breit diskutiertes Thema. Deshalb setzen immer mehr Kunden bei kritischen Infrastrukturen auf europäische Lösungen. Die Airlock Suite der Schweizer Ergon Informatik AG deckt alle beschriebenen Anforderungen an Sicherheit für Web-Applikationen in einem einzigen Produkt ab. Das Unternehmen Ergon gilt als Pionier auf diesem Gebiet im Banken- und Versicherungsumfeld und entwickelte bereits im Jahr 1997 die erste E-Banking-Plattform in der Schweiz.

Messestand: Halle 6, Stand G27