Wildwuchs von Web-Anwendungen – nicht nur ein Sicherheitsrisiko

von Dr. Martin Burkhart, Head of Product Management Airlock

In vielen Unternehmen gibt es mittlerweile einen unkontrollierten Wildwuchs an Webanwendungen und Benutzerverzeichnissen für Mitarbeiter, Kunden und Lieferanten. Dies stellt ein großes Sicherheitsrisiko dar – gerade im Hinblick darauf, dass die Bedrohung durch weltweite Cyber-Attacken stark zunimmt. Zusätzlich zum finanziellen Schaden gefährden diese auch die Reputation des Unternehmens. Außerdem können unternehmenskritische Folgen wie Probleme der Verfügbarkeit und Ausfallsicherheit entstehen. Die Aufgabe des CIOs besteht darin, den stabilen Betrieb einer sicheren und gut skalierbaren IT-Infrastruktur als Fundament für ein gut funktionierendes digitales Geschäft zu gewährleisten.

Wie entsteht der Wildwuchs an Webapplikationen?

Die Webapplikationen können verschiedensten Zwecken dienen: vom einfachen Webshop über den mobilen Zugriff auf Unternehmensdaten bis hin zu E-Mails für Mitarbeiter. Aber es gibt noch weitere Anwendungsbeispiele für eine erfolgreiche Digitalisierung wie beispielsweise E-Banking, E-Government, E-Health oder Industrie 4.0. Durch moderne ERP-Systeme (Enterprise-Resource-Planning) wie SAP oder Oracle können Lieferanten direkt auf Systemteilbereiche zugreifen und verschiedene Firmenniederlassungen werden direkt miteinander verbunden, um Produktionsprozesse und Warenbestellungen zu automatisieren und zu optimieren. So kommunizieren etwa Maschinen auf direktem Weg miteinander und machen zum Beispiel zusätzliche Arbeitsschritte durch Mitarbeiter überflüssig. Auch dieser Kommunikationskanal wird immer häufiger mittels sogenannter Webservices von außen zugänglich gemacht. Je größer die Anforderungen für das Unternehmen, für Partner und Kunden werden, desto mehr Webanwendungen kommen zum Einsatz. Diese werden oft von verschiedenen Abteilungen in Einsatz gebracht. Für IT-Abteilungen ist es schwierig, hier den Überblick zu behalten.

Verbunden mit deren Nutzung sollte aber immer eine sichere, digitale Authentifizierung der jeweiligen User sein. Die Integrität von Daten und Identitäten der User muss absolut gewährleistet sein. Eine lückenlose Sicherung und Kontrolle der Webapplikationen ist daher unverzichtbar, gestaltet sich aber dennoch schwierig: Häufig sind in jeder einzelnen Anwendung spezielle Funktionen für die Sicherheit und Authentisierung enthalten. Eine einheitliche Authentifizierung mit Benutzerselbstverwaltung ist dadurch kaum zu realisieren und die Benutzerfreundlichkeit - ein entscheidender Faktor für den Erfolg der Digitalisierung - sinkt. Die digitalen Identitäten lassen sich nur schwer wieder zusammenführen. Durch die Umsetzung von Sicherheit und Authentisieren in jeder einzelnen Applikation entsteht ein weiterer entscheidender Nachteil: Die Entwicklung von Applikationen wird langwieriger, komplexer und ineffizienter.

Aus der Praxis: Beispiel eines Versicherungsunternehmens

Bei einem großen, internationalen Versicherungskonzern greifen derzeit insgesamt 7.000 externe und interne Mitarbeiter auf die verschiedenen Brokersysteme zu – um Offerten zu

erstellen oder ihre Portfolios zu managen. Der Zugriff der externen Nutzer auf die firmeninternen Applikationen war aber zu kompliziert: Das Authentifizierungssystem basierte auf fünf verschiedenen Produkten bzw. Webanwendungen von mehreren Anbietern. Ein neues System von Airlock reduzierte mit Single Sign-On, d.h. mit einer einmaligen Authentifizierung, die Komplexität und ermöglichte allen Nutzern erweiterte Services. Die sogenannte cIAM-Lösung (Customer Identity & Access Managementlösung) hilft bei der Verwaltung einer großen Anzahl von Identitäten wie Kunden, Partnern und Mitarbeitern. Ein Vorteil ist der hohe Automatisierungsgrad der Nutzerverwaltung durch User Self-Services, der auch den Helpdesk entlastet. Auch die Benutzerfreundlichkeit ist wichtig, damit Kunden und Mitarbeiter das neue System gut annehmen: Beim cIAM genügt eine einzige Anmeldung für den Zugriff auf alle Applikationen. Der Versicherungskonzern konnte dadurch die Anrufe beim Support um 30 Prozent reduzieren und insgesamt mit dieser Lösung über 50 Prozent der laufenden Betriebskosten einsparen.

Sicherheit der Web-Anwendungen

Unternehmen sind sich selten der Gefahren bewusst, die durch die Einbindung von Web-Anwendungen entstehen. Klassische Netzwerk-Firewalls schützen nicht gegen Angriffe auf Applikationsebene und oft erhalten schlecht geprüfte Identitäten Zugriff auf sensitive Daten. Die häufig eingesetzten traditionellen Virenschutz- und Firewall-Lösungen greifen hier nicht. Dabei sind 75 Prozent aller Web-Anwendungen verwundbar und damit einer potenziellen Gefährdung ausgesetzt.

■ 90% aller böswilligen Angriffe zielen auf den Application Layer

Wie lässt sich nun dennoch die Sicherheit der Digitalisierung mit vertretbarem Aufwand realisieren? Eine praktikable Lösung bieten moderne Systeme, die vorgelagerten Schutz und Authentisierung ermöglichen. Dadurch sind alle Applikationen geschützt und es werden nur Anfragen von autorisierten Benutzern zugelassen. Web Application Firewalls wie die Airlock WAF können Gefahren abwehren. Sie kontrollieren den Inhalt aller gestellten Anfragen und lassen Gefährdungen nicht durch. Da eine WAF den Anwendungen vorgelagert ist, sind alle Applikationen dahinter sicher: Unternehmen können auch bequem neue Anwendungen hinzufügen und die Web Application Firewall schützt diese automatisch mit. Die Sicherheit der Applikationen und Daten wird jedoch erst ausreichend, wenn nicht nur der Inhalt der Anfragen geprüft wird, sondern auch die Identität der Anfragensteller. Das erledigt eine Authentifizierungsplattform wie Airlock IAM. Erst die kombinierte Anwendung der zwei Tools nimmt Angreifern den Wind aus den Segeln. Die vorgelagerte Kombination aus Authentifizierungsplattform und Web Application Firewall schützt Anwendungen vor den bekannten OWASP Top 10 Bedrohungen.

Fazit

Eine gute Digitalisierungsstrategie bringt dem Unternehmen mehr Nähe zu Kunden und Geschäftspartnern, höhere Effizienz und Kosteneinsparungen. Um für die Zukunft bestens gerüstet zu sein, müssen sich die digitalen Prozesse in Unternehmen flexibel skalieren lassen. Dafür muss eine entsprechende Infrastruktur geschaffen werden, die es erlaubt, Applikationen schneller, sicherer und effizienter auf den Markt zu bringen.

Die grössten Vorteile einer vorgelagerten Security Management Plattform wie der Airlock Suite auf einen Blick:

- Schnellere und effizientere Veröffentlichung von neuen Applikationen, durch vorgelagerte Security und Authentifizierung
- Kosteneinsparungen durch
  - User Self-Services,
  - günstigere Applikationsentwicklung,
  - Konsolidierung vieler verschiedener Lösungen
- Höherer, vorgelagerter Schutz der Daten, Identitäten und Applikationen
- Schnellere Reaktionsmöglichkeit auf Angriffe oder Schwachstellen
- Höhere Benutzerfreundlichkeit durch
  - Single Sign-on,
  - User Self-Services,
  - Applikationsportale,
  - Risikobasierte Authentifizierung
- Schnelle Erfüllung von rechtlichen Anforderungen wie der DSGVO
- Zentrale, vorgelagerte Security Management Plattform
- Identitätsmanagement über den gesamten Lebenszyklus einer digitalen Identität
- Erhöhte Verfügbarkeit und Ausfallsschutz der Applikationen

https://www.airlock.com
sales@airlock.com
+41 44 268 89 00

www.ispin.ch
info@ispin.ch
+41 44 838 31 11