Die Krux mit den Log-ins

Täglich loggen wir uns in Onlineportale oder auf Social-Media-Plattformen ein – oft mit denselben Log-ins. Die Systeme, die im Hintergrund ablaufen, sind komplex. Am Identity & Access Management beissen sich Enterprise-Organisationen und Softwarehersteller die Zähne aus, aber auch der Betrieb der involvierten Systeme hat es in sich.

Der Autor
Kaspar Geiser, CEO, Aspectra

Log-ins für Webanwendungen gehören zu unserem Alltag. Dabei geht es aber längst nicht mehr nur um öffentliche Websites, sondern immer häufiger um anwenderbezogene Informations- und Transaktionsplattformen. Solche Applikationen werden von verschiedenen Anwendern und Verwaltern genutzt und beherbergen häufig sensitive und personenbezogene Daten. Typische Beispiele sind E-Health- oder E-Government-Portale sowie firmeninterne Anwendungen. Vor allem letztere rücken vermehrt in den Fokus, da diese den eigenen Mitarbeitern 7×24 zur Verfügung gestellt werden. Die Vergabe und Steuerung von Rechten in einer solchen Anwendung stellen hohe Anforderungen an Prozesse, Technik und Sicherheit.

Authentisierung ist nicht gleich Autorisierung

Aus technischer Sicht wird unterschieden zwischen Authentisierung und Autorisierung. In beide Prozesse sind unterschiedliche Komponenten involviert. Die Authentisierung wird typischerweise unabhängig von der Anwendung durchgeführt. Nach einem erfolgreichen Log-in (Benutzername, Passwort sowie zweiter Faktor) erhält der Benutzer eine sogenannte Rolle, die an die eigentliche Anwendung weitergegeben wird. Dabei werden Rolle und andere Angaben mittels Tokens (SAML, OAuth, OpenID Connect) sicher übertragen. In der Anwendung selbst findet anschliessend die Autorisierung statt. Dabei entscheidet die Anwendung aufgrund der Rolle des Benutzers, welche Daten dieser sehen und bearbeiten darf. Die Autorisierung ist somit anwendungsbezogen, die Authentisierung nicht.

Das Bereitstellen von Identity-and-Access-Management-as-a-Service hat es in sich.

Social-Media-Log-ins

Für immer mehr Anwendungen im Web müssen sich Benutzer im Vorfeld registrieren. Das hat Vorteile: Die Inhalte werden kundenspezifisch angezeigt und Nutzer können ihre Sicherheitseinstellungen selbst verwalten und entscheiden, ob sie etwa ihre Daten in einer Anwendung mit Freunden teilen wollen. Der Nachteil ist, dass die Hürde für den Besuch der Website gross ist. Um diese zu senken, bieten viele Anbieter das Log-in via Social-Media-Plattformen wie Facebook oder dem persönlichen Google-Log-in an. Bei der Verwendung dieser externen Identitätsverwalter übernehmen Identity-and-Access-Management-Systeme (IAM) die Funktion der Rollenzuteilung für die entsprechende Zielanwendung. So machen sich die Anbieter aber abhängig von Fremdsystemen und müssen darauf vertrauen, dass der Identitätsprovider den Benutzer geprüft hat. Zudem legt er dem Provider offen, welche Anwendung ein Kunde nutzt. Welche Daten dabei zwischen zum Beispiel Facebook und der eigentlichen Anwendungen effektiv ausgetauscht werden, ist häufig unklar. Der Einsatz von Social-Media-Log-ins sollte deshalb wohlüberlegt sein. Vor allem für firmeninterne Systeme empfehlen sich interne identitätsprüfende Systeme.

IAM-as-a-Service

In den letzten Jahren haben sich verschiedene IAM-Lösungen im Markt etabliert. Diese agieren als Schnittstelle zwischen Anwendern und den Verwaltern von Anwendungen und stellen sicher, dass nur korrekt authentisierte Benutzer ein System erreichen. Doch auch solche IAM-Lösungen sind komplex in der Konfiguration und im Betrieb. Hieraus entstand die Dienstleistung «IAM-as-a-Service» (IAMaaS). IAMaaS ermöglicht ein System, das sich selbst aktuell hält, die Kapazität automatisch anpasst und damit höchstmögliche Verfügbarkeit bietet. Ein weiterer Vorteil von IAMaaS ist, dass es nicht am selben Ort wie die eigentliche Anwendung betrieben werden muss. So werden nur erfolgreich authentisierte Benutzer, mit einem gültigen Token versehen, an die Zielanwendungen geleitet. Für cloudbasierte Lösungen bedeutet das, dass dank des IAMaaS der Eintrittspunkt für die Benutzeranmeldung sowie der Speicherort der TLS-Keys und Benutzerdaten wie Benutzername, Passwort und zweiter Faktor an einem bekannten und gesicherten Ort geschehen.

Architektur und Betrieb

Die Trennung zwischen eigentlicher Anwendung und dem IAM bringt weitere Vorteile mit sich. So werden Funktionen wie On- und Offboarding nur am Log-in-System vollzogen und nicht in dem System, in dem die sensiblen Daten, wie etwa Gesundheitsdaten, gespeichert sind. Dies verkleinert die Anzahl Systeme,

die ihrerseits Zugang zu internen Verzeichnisdiensten wie Active Directory (AD) oder Lightweight Directory Access Protocol (LDAP) und Passwörter haben. Auch Funktionen wie «Passwort vergessen» oder das Wechseln eines One-Time-Password-Verfahrens finden unabhängig von den eigentlichen Kernanwendungen statt.

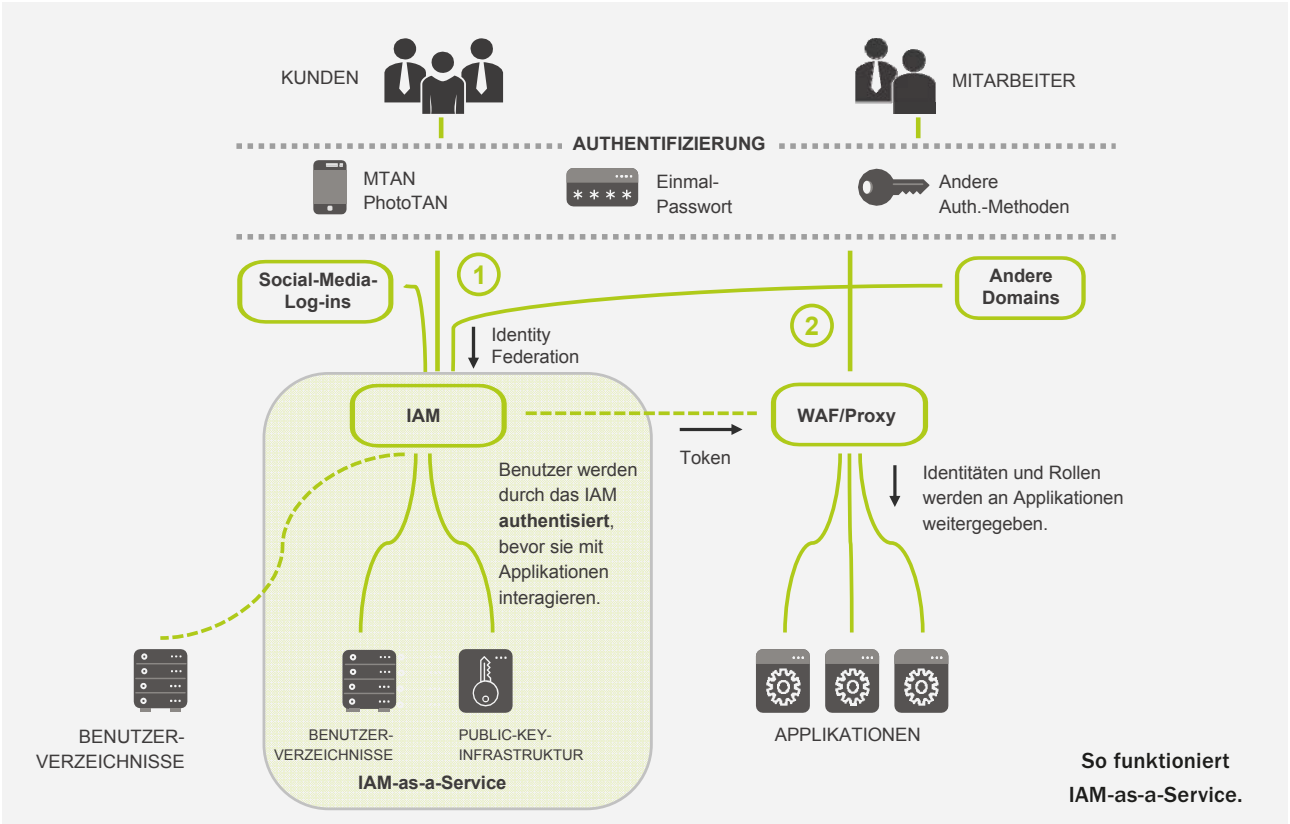
Mit der Architektur stellt sich auch die Frage des IAMaaS-Anbieters. Public Clouds verfügen über solche Services und preisen diese mit maximaler Sicherheit, Performance und Verfügbarkeit an. Wie bei allen Cloud-Diensten ist aber fraglich, wer effektiv Zugriff auf die Randdaten wie IP-Adresse, Benutzername und -rollen hat und ob diese an Dritte weitergegeben werden. Unklar ist häufig auch, wo die Daten liegen und welches Rechtssystem die Daten schützt. Hier lohnt sich die Evaluation der Anbieter. Ausser den Public Clouds gibt es auch eine Vielzahl von Software- und Serviceanbietern, die auf individuelle Sicherheitsbedürfnisse wie lokaler Standort oder bekanntes Administrationspersonal eingehen können. Denn unabhängig vom Service müssen für das IAM die Verantwortlichkeiten und Aufgaben festgelegt werden. Und auch hier hilft eine lokale Beratung. Schliesslich sind Ziel und Nutzen von IAMaaS, dass «nur» das Pflegen der Benutzerdaten und Rollen als Aufgabe übrigbleibt. Da das IAM zugleich ein wichtiger Perimeterschutz ist, empfiehlt es sich, die IAM-Logs in das eigene SIEM einzubinden, oder aber den Managed-Service-Provider damit zu beauftragen, Sicherheitsproblemen rund um das IAM zu erkennen.

Blick in den Maschinenraum

Das Bereitstellen von IAMaaS hat es in sich. Zwar beherbergt ein IAMaaS-Anbieter keine eigentlichen Datensätze von Anwendungen. Mit den Informationen in den IAM-Systemen kann sich jedoch unter Umständen jemand Zugang zu den Drittsystemen verschaffen. Weil sich das IAM nicht unbedingt am selben Ort wie die zu schützenden Anwendungen befindet, ist es beim Einsatz eines IAMaaS sinnvoll, die eigene Anwendung mit einem vorgelagerten System (WAF/Proxy) zusätzlich zu schützen. Die Aufgabe dieses Proxys besteht darin, die Session und Tokens zu verifizieren und den Benutzer erst nach erfolgreicher Prüfung auf die Zielanwendung weiterzuleiten.

IAM-Betreiber müssen das IAM daher maximal schützen. Ausser der klassischen System- und Leistungsüberwachung müssen sie insbesondere auch die Logs aktiv überwachen und in Echtzeit auf Anomalien prüfen. Ein solches atypisches Verhalten ist zum Beispiel, wenn die IP-Adresse respektive das Herkunftsland eines Benutzers innert Minuten wechselt. Oder aber, wenn ein systematisches Prüfen von generischen Benutzernamen und Passwörtern stattfindet, etwa aus bereits bekannten Quellen von Datenlecks. Zudem müssen alle ins IAM involvierten Systeme maximal isoliert und Zugang nur berechtigten Personen erteilt werden.

Schliesslich sind auch IAM-Systeme nicht immer fehlerfrei und loggen – unter gewissen Bedingungen – gar Benutzernamen und Passwörter. Daher müssen auch das Aufbewahren und Löschen von Logs, Dumps und Backups geregelt und überwacht werden. Ansonsten könnte auch noch Jahre nach dem Bekanntwerden einer Schwachstelle in der IAM-Software Datensätze daraus extrahiert werden.



So funktioniert IAM-as-a-Service.