Dr. Martin Burkhart, *Head of Product Management, Airlock*

SICHERE KUNDEN-LOGINS SIND EINFACH

Anders als bei klassischen Lösungen fürs Identity and Access Management (IAM) ist bei Consumer IAM (cIAM) eine besonders hohe Flexibilität gefragt. So müssen Kunden-Login-Systeme schier endlos skalierbar sein und dürfen vor allem Erstanmelder nicht durch Umstandskrämerei abschrecken.

Für ein Kunden-Zugangssystem gelten völlig andere Anforderungen als bei einer IAM-Lösung für Mitarbeiter. Eine Consumer-IAM-Lösung muss zum Beispiel eine weitaus größere Anzahl von Identitäten erkennen. Aus diesem Grund ermöglichen dedizierte cIAM-Lösungen eine extrem hohe Anzahl an Identitäten bei gleichzeitigen Sessions. Darüber hinaus sind sie für Millionen von Benutzern bei hoher Performance skalierbar ausgelegt. Auch preislich macht eine spezialisierte cIAM-Lösung einen großen Unterschied zur klassischen Variante, was bei einer großen Anzahl an Identitäten durchaus ins Gewicht fällt.

User-Selfservice und Helpdesk

Einer der wichtigsten Vorteile von cIAM-Lösungen sind User-Selfservices. Die Anmeldung und die Erweiterung eines Kundenprofils sind hier ohne Eingriff eines Administrators oder des Helpdesks möglich. Dadurch entlasten User-Selfservices die Support-Mitarbeiter, reduzieren die Kosten erheblich und verkürzen die Wartezeiten der Nutzer. Hinzu kommt, dass auch die bestehenden Applikationen spürbar weniger Last zu bewältigen haben, weil sie nun nicht mehr selbst Routinen für die Authentifizierung und Autorisierung bereitstellen müssen. Ist doch einmal Helpdesk-Unterstützung nötig, kann dieser über delegierte Administrationsrechte auf das Kundenkonto zugreifen. Mit Co-Browsing kann der Helpdesk-Mitarbeiter sogar gemeinsam mit dem Kunden einzelne Arbeitsschritte durchgehen.

Hinzu kommt, dass die Eintrittsbarriere bei einer schnellen Selbstregistrierung deutlich niedriger ist, was die Zahl der Kunden und Interessenten steigen lässt. Durch die Anbindung an beliebige Benutzerverzeichnisse wie Microsoft Active Directory oder LDAP und durch diverse integrierte Token-Lösungen kann die Benutzerverwaltung flexibel und dynamisch gestaltet werden.

Auf diese Weise verbessert ein cIAM den Benutzerkomfort und damit auch die Sicherheit und die Kundenzufriedenheit: Durch Single Sign-on müssen sich Benutzer nur einmalig anmelden. Mithilfe des Step-up-Verfahrens kann auch eine starke Authentifizierung für erhöhte Sicherheits- oder Compliance-Anforderungen umgesetzt werden. User-Selfservices ermöglichen es den Benutzern auch, ihre Passwörter schnell und einfach zurückzusetzen.

Flexibilität bei der Authentifizierung

Unternehmen sollten die Möglichkeit haben, zwischen verschiedenen Formen der Authentifizierung wählen und wechseln zu können. Die Methoden beginnen beim einfachen Passwort und gehen bis hin zu modernen, starken Authentifizierungsverfahren. Auch hier ist meist kein Eingriff des Administrators oder Helpdesks notwendig.

Ein Beispiel für eine einfache Authentifizierung ist die Anmeldung über Social-Media-Accounts. Dabei bringen die Kunden ihre bereits bestehende digitale Identität gleich mit (Bring Your Own Identity). Das steigert die Zahl der Registrierungen enorm, weil die Nutzer keine langen Registrierungsformulare ausfüllen müssen. Als störend empfinden Benutzer vor allem interaktive Authentifizierungsschritte. Dabei müssen sie einen zusätzlichen Handlungsschritt tätigen, um ihre Identität zu verifizieren. In komplexeren Umgebungen, wie zum Beispiel bei der digitalen Eröffnung eines Kontos, empfiehlt sich daher eine risikobasierte (adaptive) Zugriffskontrolle, zum Beispiel das Digital Onboarding bei der Identitätsverifizierung.

Bei der risikobasierten Authentifizierung berücksichtigt eine smarte Sicherheitssoftware Kontextinformationen während des Zugriffs auf eine Anwendung und registriert zahlreiche Informationen wie die Tageszeit, den Ort des Zugriffs, die Geräte-ID sowie Browser-Informationen (Client und Session Fingerprinting). Mit Dynamic Value Endorsement (DyVE) werden JSON-Objekte dyna-

Die Airlock-IAM-Lösung von Ergon bietet umfangreiche Selfservice- und Sicherheitsfunktionen über den gesamten Lebenszyklus hinweg.

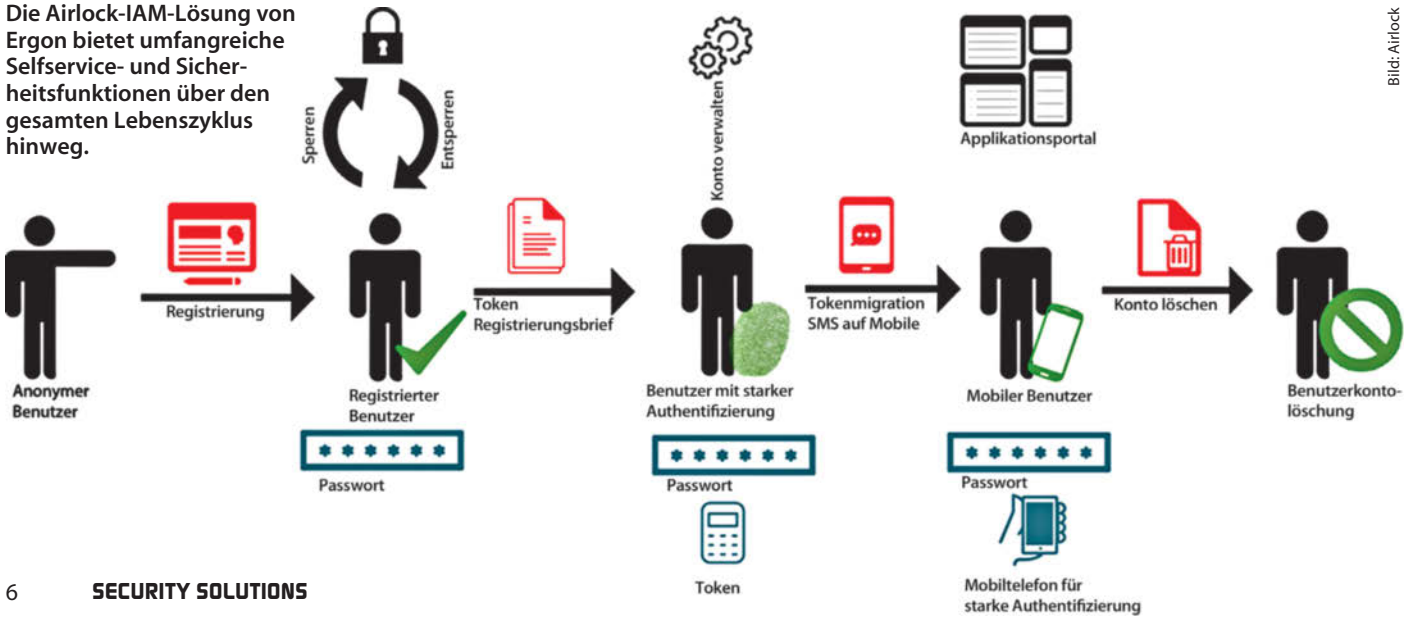

Bild: Airlock

misch nach Werten durchsucht, die für die aktuelle Benutzersession zulässig sind. Parameter oder JSON-Attribute von nachfolgenden Anfragen können dann auf die Verwendung von zulässigen Werten überprüft werden. In Kombination ermöglicht das eine gute Einschätzung, ob der Zugriff regulär erfolgt oder betrugsverdächtig ist. Je nach Applikation wird so ohne größeren Aufwand ein ausreichendes Sicherheitsniveau erreicht, zugleich reduziert sich die Zahl der interaktiven Authentifizierungsschritte.

Sicherheitsstufen nach Anwendung

Unternehmen unterscheiden zwischen Bereichen mit verschiedenen Sicherheitsanforderungen. Der Hypothekenrechner einer Bank ist zum Beispiel nicht sicherheitskritisch, für einen personalisierten Börsenticker braucht es nur eine einfache Authentifizierung, E-Banking muss jedoch stark authentifiziert sein.

Verlangt das Anwendungsumfeld grundsätzlich eine höhere Sicherheitsstufe, erhöht die Software die Akzeptanz beim Nutzer, wenn er als „Gegenleistung" für die starke Authentifizierung Single Sign-on erhält. Dazu tippt der Benutzer zum Beispiel einen SMS-Code ab und erhält dann für den Rest des Tages Zugriff auf alle relevanten Anwendungen. Gerade in Consumer-IAM-Systemen schafft erst Single Sign-on ein nahtloses Kundenerlebnis. Wird dem Kunden das Portal oder die Applikationen mit vielen unterschiedlichen Login-Aufforderungen zu kompliziert, beginnt er, nach Alternativen zu suchen. Federated SSO sollte SAML, OpenID und OpenID Connect unterstützen.

Consumer-IAM-Lösungen sind exponierter und häufiger Opfer von Hackerangriffen als klassische Enterprise-IAM-Lösungen. In Kombination mit einer Web Applikation Firewall (WAF) kann ein cIAM am besten gegen Missbrauch vorgehen. Ein Vorteil der Kombination von cIAM und WAF ist, dass die Interaktionen des Kunden über Formulare (Smart Form Protection) immer gesichert ablaufen und das IAM-System vor Script-Angriffen geschützt ist. Damit wird auch die Fraud Detection umfassend erweitert.

Bei einer cIAM-Lösung ist nicht zuletzt die Integration von APIs wichtig. Das unterstützt einen flexiblen Zugriff auf bestehenden Services und ermöglicht die Einbindungen von Apps auf Mobiltelefonen. Um nahtlos Identitäten aus verschiedenen Benutzerverzeichnissen zusammenzuführen, ist zudem eine Synchronisation der verschiedenen Directory Services in der cIAM-Lösung von Vorteil.

Bild: rvlsoft – Fotolia

cIAM-Lösungen bieten dem Kunden schnellen Zugriff auf alle Applikationen.