Den Lebenszyklus sensibler Benutzerdaten richtig managen

Digitale Identitäten und User-Life-Cycle

Viele Betreiber einer Internetanwendung richten ihr Augenmerk auf die Authentifizierung und setzen diese immer häufiger mithilfe externer Identity-Provider um, wie Facebook, Microsoft oder Verimi. Im Gegensatz dazu versuchen die Betreiber den Rest, zum Beispiel die Speicherung der Accountdaten oder die Berechtigungsvergabe, innerhalb der Anwendung zu lösen – oft mit archaischen Methoden. Besser und sicherer wäre es, Benutzerinformationen und wichtige Berechtigungen in einem dedizierten User-Life-Cycle-Prozess abzulegen.

Von Stephanie Ta, Syntlogo GmbH

Damit ein Benutzer in einer Online-Anwendung frei navigieren und selbst Aktionen durchführen kann, muss er sich authentifizieren. Einige Unternehmen setzen hierfür einen externen Identity-Provider ein. Allerdings braucht es für das Management einer digitalen Identität mehr, als nur die Identifizierung der Person, die sich gerade einloggt. Dafür benötigt man ein funktionierendes User-Life-Cycle-(ULC)-Management.

Wie Abbildung 1 zeigt, beginnt ein „Lebenszyklus“ mit einer datenschutzkonformen Registrierung und der Genehmigung zur Verwendung der Daten des Benutzers. Danach erhält er Zugang zum System und besitzt die Basisrechte eines registrierten Benutzers. Er verfügt jedoch nicht automatisch über weitreichendere Befugnisse. Diese muss er entweder in einem weiteren Schritt beantragen oder das System weist sie ihm aufgrund bestimmter Merkmale zu. Die Merkmale ergeben sich aus den Daten des Benutzers. Beispiele für unterschiedliche Rechte sind:

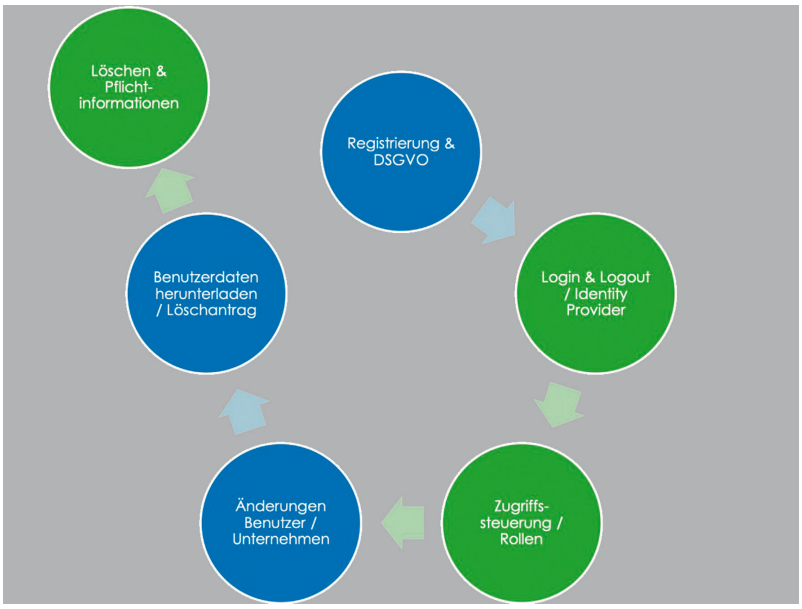

Abbildung 1: Der User-Life-Cycle eines Benutzers; blau = größtenteils durch den Benutzer gesteuert, grün = Steuerung durch das System

_____ Lieferanten, Versender, Spediteure und weitere Akteure greifen auf die gleiche Portalwebseite eines Industriekunden zu (z. B. Supply-Chain-Plattform)

_____ Behörden, die gleichermaßen Bürger, Firmen oder Länder als Benutzer ihrer Portale haben (z. B. Autozulassung)

_____ B2C-Anwendungen: Nur „Prime“-Kunden dürfen gewisse Leistungen abrufen oder Produkte bestellen

Die Komplexität wird erhöht durch mehrere Anwendungen, die über Single-Sign-On erreichbar sind. Dabei ist die Implementierung des Single-Sign-On nicht die Schwierigkeit, sondern die Vergabe der Benutzerberechtigung in der jeweiligen Internetanwendung selbst. Denn das ist ein Relikt aus „alten“ Zeiten, als die Applikation noch selbst für alles verantwortlich war: Zugriff, User-ID-Zuordnung und die Berechtigungsvergabe. Besser ist es, das zu bündeln und zwar durch ein zentrales Management der Identitäten und Rollen. Das lohnt sich schon aus Compliance-Gründen. Es vereinfacht die Aufgabe, die Systemarchitektur rechtskonform zu gestalten.

Token passen in die Zero-Trust-Zukunft

Um die Berechtigungsvergabe und die Zugriffsrechte kümmert sich in der Regel ein Rollenmanagement. Das ist in mehr als 90 Prozent der Fälle als RBAC aufgebaut. Aber RBAC ist schwerfällig. Es ist so unflexibel, dass man durch die Gruppenzuteilung nur riesige, undurchschaubare Berge von Verantwortlichkeiten und zugehörigen Gruppen anhäuft. Eine moderne Art der Zugriffssteuerung – leicht, flexibel, sicher – ist die der Token-Based Authorization. Ein digital signierter Token überbringt die Rollen-Information zur Berechtigung. Er ersetzt nicht den Security-Token von OpenID Connect (OIDC) oder anderen Authentifizierungsprotokollen, sondern er sitzt im Inneren eines OIDC-Token. Die Syntlogo GmbH hat das Konzept SecuRole genannt. Durch die Trennung zwischen Service-Providern, Anwendungen und Unternehmensnetzwerken brauchen Unternehmen ein solches Framework, das die rechtliche und physische Trennung einzelner Akteure und Systeme ohne Probleme überwindet.

Datenminimierung dank zentralem IMS

Ein zentrales Identity-Management-System (IMS) hält das DSGVO-Prinzip der Datenminimierung ein. Die Anwendungen verantworten nicht mehr selbst die Zugriffsrechte, sondern das zentrale IMS speichert die Informationen zum Zugriff der Benutzer. So führen die Applikationen ihre eigentlichen Kernaufgaben aus.

Anwendungen können sehr unterschiedlich aufgebaut sein, was die Benutzerverwaltung betrifft:

_____ Voll integriert – ist mit der User-Registry verbunden. Führt keine eigenen Prozesse durch zur Einhaltung der DSGVO.

_____ Provisioniert – besitzt eine eigene, lokale User-Registry. Das zentrale IMS agiert mit ihr und pflegt sie.

_____ Autonom – sammelt selbst persönliche Benutzerdaten. Das IMS führt einen Dialog mit ihr zur Einhaltung der DSGVO.

Für jede Form der Benutzerverwaltung einer Anwendung gibt es demnach eine Lösung. Das zentrale IMS verwaltet die Identitäten mehr oder weniger allein. Bei der Neuentwicklung einer Anwendung oder einem Release kann man durch eine zentrale Identitätsverwaltung die Systemarchitektur schlank gestalten.

Automatische Pflege des Account-Lebenszyklus

Änderung und Entwicklung gehören zum Leben und zur Geschäftswelt. So auch die Veränderung im Lebenszyklus eines Benutzers. Die entstandene History braucht man nicht nur für das Audit. Dazu gehört die Information, ob ein Portalnutzer längere Zeit inaktiv war. So kann man einen Benutzer sperren, wenn er seit zwei Jahren nicht mehr online war. Nach zehn Jahren darf der Account gelöscht werden. Dieser Löschvorgang entspricht ebenfalls dem Gebot der Datensparsamkeit laut DSGVO. Durch ein zentrales IMS und voreingestellte Workflows, laufen diese Aufgaben automatisiert ab ohne manuelle Eingriffe.

Einen großen Vorteil können Unternehmen aus der History eines IMS ziehen, in der das System bestimmte Ereignisse protokolliert. Es zeichnet zum Beispiel den letzten Login eines Benutzers auf und stößt dazu einen Workflow an. Nach einem halben Jahr Inaktivität informiert ein ULC-Prozess das Customer-Relationship-Management-(CRM)-System oder es versendet automatisch eine E-Mail an den Benutzer. Bei einem Geschäftsmodell, welches über eine Subscription läuft, kann das ULC-Management den Nutzer vier Wochen vor Ablauf daran erinnern. Diese und ähnliche regelmäßige Tätigkeiten kann ein System übernehmen und somit interne Ressourcen unterstützen.

Identity-Life-Cycle immer up to date

Ohne manuellen Eingriff sollte ein Benutzer seine Daten herunterladen oder auch löschen können („Vergiss-mich Antrag“). Das System entfernt Pflichtinformationen, wie Rechnungen oder Verträge, erst nach zehn Jahren. Unternehmensseitig sollte das ULC-Management einen Account automatisch deaktivieren, wenn der Benutzer nicht mehr beim Geschäftspartner arbeitet oder aus anderen Gründen aus dem Portal ausscheidet. Eine Vertreterregelung beim Geschäftspartner hält die Kontaktdaten und die Information zum Benutzerstatus à jour. Die delegierte Administration entlastet den eigenen Support von solchen Aufgaben.

Zu guter Letzt ist die Deaktivierung eines Benutzer-Accounts eine größere Aufgabe. Der Benutzer durchläuft damit den letzten Schritt des User-Life-Cycle.

An jedem Punkt im Benutzer-Lebenszyklus unterstützen Tools zur Automatisierung und sicheren Übertragung von Informationen den Betrieb von Internetportalen. Und nicht nur das, diese Vorgehensweise ist von Anfang bis zum Ende DSGVO-konform. Es steigert den Kunden- oder Benutzerwert von HTTPS-browserbasierten Anwendungen noch mehr. Die Einbindung eines Identity-Providers stellt nur einen Bruchteil der Gesamtlösung in der Zugriffsverwaltung dar. Intern gesteuerte ULC-Prozesse entlasten den Support von aufwendigen manuellen Obliegenheiten und unterstützen weitere Bereiche, wie den Vertrieb oder den Einkauf. ■