Eine »Schlüsselposition« moderner IT

Frank Strecker Computer und Arbeit 1/2022 Ab Seite 17

Nutzerverwaltung **Wenn man als fachfremde Person Administrator:innen zuhört, versteht man mitunter wenig. Wissen Sie, was mit »Azure« oder »ADD« gemeint ist? Dabei handelt es sich um eine zentrale Nutzerverwaltung, die bei Microsoft-Produkten zum Einsatz kommt. Warum Sie sich dafür zumindest ein bisschen interessieren sollten, verrät unser Autor.**

Darum geht es

1. Kann man mit einer Anmeldung auf mehrere Programme zugreifen, ...

2. ... steht dahinter meist eine zentrale Nutzerverwaltung.

3. Hier werden die Aktivitäten der Nutzer:innen protokolliert.

Wenn man mit einer Anmeldung auf mehrere Programme oder Geräte zugreifen kann, steht dahinter meist eine zentrale Nutzerverwaltung, auch IAM (»Identity and Access Management«, englisch für Nutzer- und Zugriffsverwaltung) genannt. Zu dieser Kategorie gehören beispielsweise das Microsoft »Active Directory« samt Cloud-Ableger »Azure Active Directory«. Solche Dienste dienen der sicheren unternehmensweiten Nutzung von Cloud-Diensten und eigenen Servern.

Die Nutzerverwaltung unterliegt der Mitbestimmung, denn die individuelle Anmeldung ist ein Merkmal der Eignung von Software zur Leistungs- und Verhaltenskontrolle gemäß § 87 Abs. 1 Nr. 6 Betriebsverfassungsgesetz (BetrVG). Trotzdem wird das Thema in Dienst- und Betriebsvereinbarungen noch nicht immer genügend beachtet. Das mag daran liegen, dass die Bedeutung erst in den letzten Jahren zugenommen hat, aber auch daran, dass diese IT-Infrastruktur für Endanwender:innen so wenig sichtbar ist wie der Eisberg unter der Wasserlinie. Wir möchten die Funktion an einem Beispiel erklären und Hinweise geben, was eine zeitgemäße Regelung enthalten sollte.

Hauptfunktionen der Nutzerverwaltung

Eine zentrale Nutzerverwaltung ist so etwas wie eine Hotelrezeption; sie dient der Sicherheit im Haus und registriert, wer kommt und geht. An der Rezeption legitimieren sich die Hotelgäste, bekommen Zutritt zum Haus und den Zimmerschlüssel, den sie dort auch wieder abgeben sollen. Dort wird ein Konto für die Gäste geführt und es können Nachrichten hinterlassen werden. An dem Beispiel können wir uns die drei Hauptfunktionen der Nutzerverwaltung ansehen:

- Identifizierung,
- Berechtigung sowie
- Protokollierung und Auskunft.

Die Identifizierung (fachlich: »Authentifizierung«) ist die Grundlage für alle anderen Funktionen der Nutzerverwaltung. Sie hilft bei der Aufgabe, jederzeit sicher zu klären, wer ein IT-System bedient hat und Urheber:in bestimmter Eingaben ist. Die Identität im System (Kennung oder Konto) soll möglichst einer natürlichen Person zugeordnet werden können. Sichere Authentifizierung setzt also voraus, dass ein Benutzerkonto immer nur von einer einzigen Person genutzt wird. Eine Person könnte aber über mehrere Konten verfügen und z. B. zusätzlich ein (ebenfalls persönliches) Konto für Administrationsaufgaben haben.

Gruppenkonten mit entsprechenden Gruppenpasswörtern sind eine zwiespältige Angelegenheit. Sie werden manchmal genutzt, um eine individuelle Leistungs- und Verhaltenskontrolle zu verhindern. Nach heutigen Maßstäben sprechen aber meist Sicherheitsbedenken und Datenschutz-Erfordernisse dagegen, denn der Umgang mit personenbezogenen Daten muss nachvollziehbar sein.

Wie kommen die Daten ins System?

Benutzerkonten werden oft automatisiert in der Nutzerverwaltung angelegt, aus anderen Systemen, die über eine Schnittstelle mit der Nutzerverwaltung verbunden werden. Die Konten für Beschäftigte können etwa beim Eintritt in das Arbeitsverhältnis (»Onboarding«) aus dem Personalsystem heraus angelegt und beim Austritt auch wieder deaktiviert werden. Dagegen ist prinzipiell nichts einzuwenden, solange transparent gemacht wird, was wohin übermittelt wird.

Man kommt aber nicht mit einer einzigen Nutzerverwaltung aus, wenn lokale Systeme und Cloud-Nutzung zusammentreffen oder mehrere Cloud-Mandanten und Clouds verschiedener Provider als »Multicloud« genutzt werden. Es würde in solchen Fällen zu lange dauern und wäre zu fehleranfällig, jedes Mal bei den jeweils anderen Stellen nachzufragen.

Meist werden die Benutzerverzeichnisse des Unternehmens dann so miteinander verbunden, dass sie weiter selbstständig funktionieren, aber die erforderlichen Benutzer-Stammdaten regelmäßig miteinander abgleichen (synchronisieren).

Um Missbrauch und Datenlecks vorzubeugen, werden Passwörter, Fingerabdrücke etc. nicht in Klarform gespeichert, sondern nur als Hash. Das ist eine durch Verschlüsselungstechnik verkürzte Angabe, mit der das Geheimnis geprüft, aber nicht wieder ausgelesen werden kann. Nur diese Prüfsumme wird auch mit den verbundenen Systemen geteilt. Dann kann mit geringem Zeitversatz überall das gleiche Passwort genutzt werden.

Welche Daten werden gespeichert?

Eine sichere Authentifizierung braucht Belege und Beweise. Im Hotel lässt sich die Rezeption auch den Ausweis oder die Kreditkarte zeigen, wenn Gäste nicht persönlich bekannt sind.

Die Authentifizierung allein durch Passwort oder Pin verliert an Bedeutung, weil Passwörter unsicher sind: Sie werden häufig vergessen, mehrfach genutzt, erraten oder weitergegeben. Stand der Technik ist die Kombination mehrerer Verfahren, die sogenannte Multifaktor-Authentifizierung (MFA). Bei einer Anmeldung durch den Nutzer oder die Nutzerin kann es dann nötig sein, nach der Eingabe eines Passworts zusätzlich auch den Fingerabdruck zu überprüfen, um die Identität zweifelsfrei zu bestätigen. Damit die Nutzer:innen sich nicht zu oft umständlich authentifizieren müssen, wird persönlichen Geräten vertraut, nachdem diese (z. B. durch MFA) unzweifelhaft einer Person zugeordnet worden sind.

Neben der Benutzerkennung (meist in Form einer E-Mail-Adresse) werden im Benutzerverzeichnis weitere Merkmale zum Benutzerkonto verwaltet, wie z. B. Name, Telefonnummer, Personalnummer, Büro, Organisationseinheit und Vorgesetzte. Meist besteht zudem die technische Möglichkeit, für die Verwendung in Online-Verzeichnissen ein Foto hochzuladen. Technisch versierte Administrator:innen können das Verzeichnis auch um eigene Einträge erweitern.

In der Berechtigungsprüfung (Autorisierung) wird geprüft, ob eine Benutzeridentität auf eine bestimmte Ressource zugreifen darf. Das kann alles Mögliche sein: Geräte, Lesen oder Schreiben von Dateien, Zugang zu großen Programmsystemen oder der Aufruf einer ganz bestimmten kleinen Funktion. Die Autorisierung kann völlig unbemerkt im Hintergrund erfolgen. Die Benutzer:innen müssen sich nicht bei jeder Ressource separat anmelden, denn ihre Identität ist bereits auf dem Gerät hinterlegt oder als Cookie im Webbrowser vorhanden. Die Ressource fragt anhand dessen die Rechte an – in etwa so, wie der Barkeeper im Hotel für seine Anfrage, ob etwas angeschrieben werden darf, nicht den Namen des Gastes erfragen muss, wenn er die Schlüsselnummer kennt.

Protokollierung und Leistungskontrolle

Die Nutzerverwaltung protokolliert alle An- und Abmeldungen und jede Nutzung der kontrollierten Ressourcen mit Personenbezug, was die Sicherheit und Nachvollziehbarkeit des Gesamtsystems erhöhen soll. Genau hierin liegt gleichzeitig die Möglichkeit zur Kontrolle von Leistung und Verhalten der Beschäftigten. Das ist per se nicht neu.

Neu ist aber das Ausmaß dieser Kontrollmöglichkeit. Wir erleben den Wandel der IT-Landschaften weg von großen einheitlichen Anwendungen mit tausenden Funktionen, in denen man den ganzen Tag angemeldet bleibt, hin zu tausenden von kleinen Apps mit wenigen Funktionen, die jeweils einzeln aufgerufen und berechtigt werden – so z. B. die »Fiori« von SAP; auch Microsoft will die Office-Anwendungen in immer kleinere Bausteine auflösen. Mit jedem Aufruf eines solchen »Microservice« kann eine personenbezogene Protokollzeile in den Aktivitätsprotokollen der Nutzerverwaltung entstehen. Diese Protokolle werden mit weiterem Fortschreiten zur Serviceorientierung ein immer vollständigeres Bild der Aktivität einzelner Benutzer:innen zeigen und damit immer tiefer in das Informationsgrundrecht der Beschäftigten eingreifen. Umfangreiche Auswertungen aus der Nutzerverwaltung heraus mögen zu Sicherheitszwecken im SIEM (»Security Incident and Event Management«, englisch für ein Sicherheitssystem zur Abklärung von Vorfällen und Verdachtsfällen)

vielleicht – bei umfangreichen Datenschutzmaßnahmen – noch vertretbar sein. Auswertungen zu anderen Zwecken aber in der Regel nicht, denn eine lückenlose Überwachung am Arbeitsplatz ist nach der Rechtsprechung des Bundesarbeitsgerichts (BAG) rechtswidrig (BAG 27.3.2003 – 2 AZR 51/02).

Fazit: Genau hinschauen

Die Kontrollmöglichkeiten rund um zentrale Nutzerverwaltungen werden derzeit stark ausgebaut, um Sicherheitsrisiken rund um das Cloud-Computing zu begegnen, manchmal auch ohne besondere Absichten, einfach »weil es geht«. Es lohnt genauer hinzusehen:

- Welche Stammdaten der Beschäftigten werden in den Nutzerverwaltungen verarbeitet, und welche davon werden wohin übermittelt? Zu welchem Zweck wird übermittelt?
- Welche Verbindungen zu externen Nutzerverwaltungen sind verabredet?
- Für welche Ressourcen werden über die Nutzerverwaltung Berechtigungen vergeben?
- Welche Rechte sind mit einer Rolle verbunden?
- Welche Anmelde- und Aktivitätenprotokolle werden erstellt und wohin werden sie übermittelt?

Das Identitäts- und Zugriffsmanagement ist eine Schlüsselposition der modernen IT-Landschaft. Es braucht ausbalancierte Regelungen, die sowohl die IT-Sicherheit wie auch den Schutz der Beschäftigten vor Leistungskontrolle gewährleisten können.

Frank Strecker berät u. a. zur Personaldatenverarbeitung und zu Office 365.

www.tbs-nrw.de

– IT-Mitbestimmung