

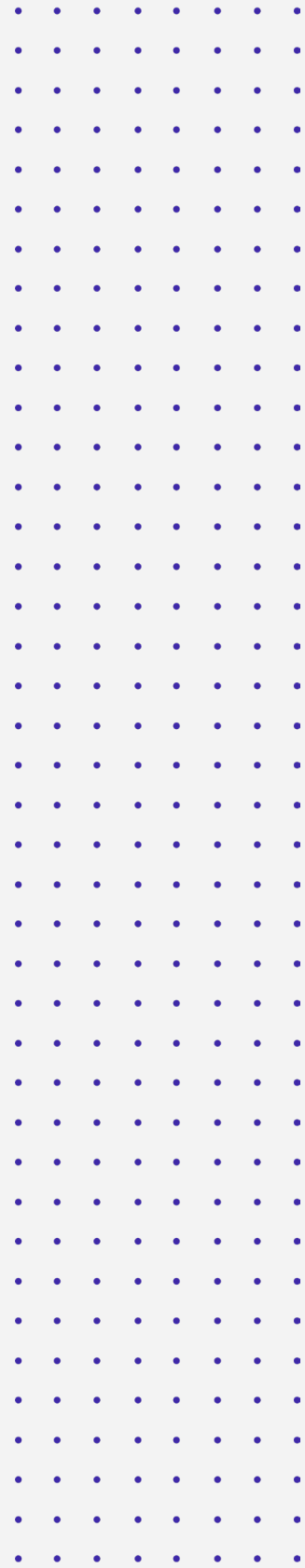
Sichere Authentifizierung von digitalen Kunden- und Mitarbeiteridentitäten

Optimieren Sie Ihr IAM-System mit Identity-as-a-Service



Inhalte

- 3 Überprüfen von Benutzeridentitäten
- 4 Nahtlose Validierung – leicht gemacht
- 5 Kennwortschutz ohne Mühe
- 6 Kriterien für eine effektive Identitäts- und Zugriffsmanagementlösung (IAM)
- 6 IBM Cloud Identity



Überprüfen von Benutzeridentitäten

Der „Schutz der Online-Identität“ ist immer wieder Gesprächsthema in allen Branchen. Die meisten Unternehmen implementieren umfangreiche Maßnahmen zur Überprüfung der Benutzeridentität und zum Schutz ihrer kritischen Assets vor Angriffen, doch Sicherheitsverletzungen und Attacken stellen nach wie vor eine ernsthafte Bedrohung dar.

Der Missbrauch der digitalen Identität ist der Hauptgrund für den Verlust von Benutzerdaten zum Beispiel durch Diebstahl personenbezogener Informationen sowie für den Verlust von Unternehmensdaten durch unberechtigten Zugriff auf firmeninterne Informationen und Kontrollen. Die durchschnittlichen Kosten einer Datenschutzverletzung belaufen sich auf 3,92 Millionen USD und der durchschnittliche Umfang auf 25.575 Datensätze.¹ Unternehmen, die Opfer einer Sicherheitsverletzung werden, verlieren nicht bloß Daten, sondern auch Vertrauen in der Öffentlichkeit. Nach einer Sicherheitsverletzung schätzen viele Konsumenten das betroffene Unternehmen als weniger vertrauenswürdig ein, was geschäftliche Einbußen zur Folge haben kann.

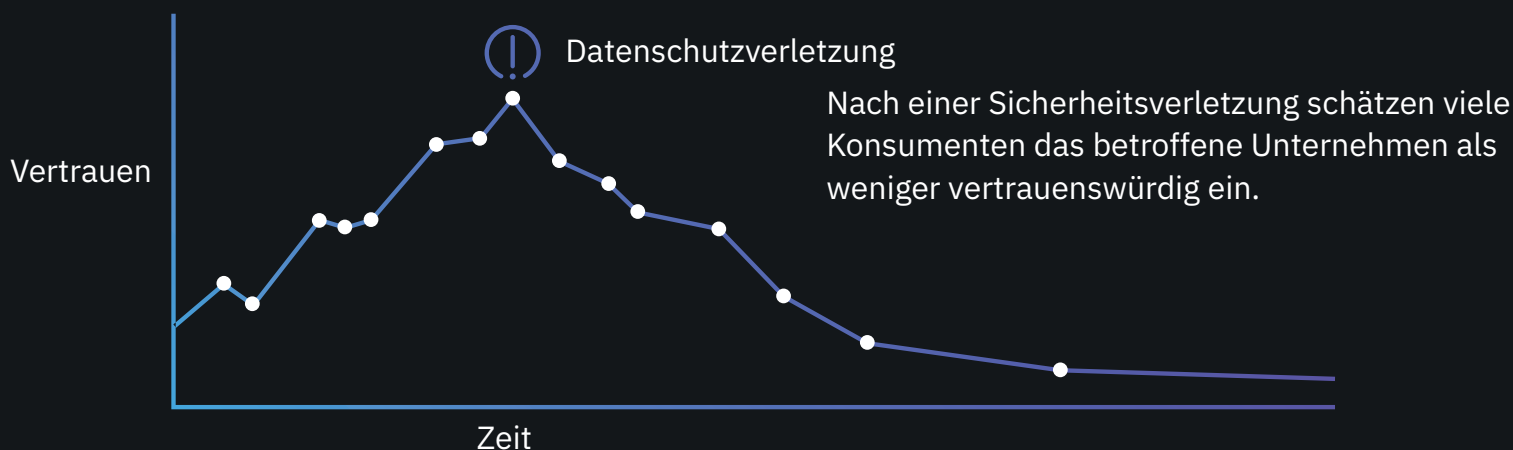
Je mehr Unternehmen Cloud Dienste nutzen, desto größer wird der Bedarf an Sicherheitsmaßnahmen, die interne und externe Benutzer autorisieren und authentifizieren können, ohne die Nutzbarkeit der Systeme zu beeinträchtigen.

Es wird erwartet, dass der Markt für Identity-as-a-Service Lösungen in den nächsten fünf Jahren durchschnittlich um 14,1 % jährlich wächst, da immer mehr Unternehmen die Vorteile des Cloud-Computing für sich nutzen.² Das Ziel für Unternehmen muss eine effektive Identitätsprüfung für Kunden und Mitarbeiter sein, die aber reibungslos und benutzerfreundlich funktioniert.

Muss IDaaS wirklich kompliziert sein?

Verbinden Sie cloudbasierte, mobile und lokale Geräte und Benutzer standortunabhängig mit Geschäftsanwendungen. Entdecken Sie die Möglichkeiten von Identity-as-a-Service (IDaaS) in diesem kurzen Video.

[Video ansehen](#) 



Nahtlose Validierung – leicht gemacht

Beim Identitäts- und Zugriffsmanagement sind Unternehmen heute mit zahlreichen Herausforderungen konfrontiert. Viele entstehen aus der Notwendigkeit, sichere Prozesse zu schaffen, die zugleich eine reibungslose Benutzererfahrung bieten. Für eine benutzerfreundliche Erfahrung sollten Unternehmen:

Identität von Kunden und Mitarbeitern bestätigen

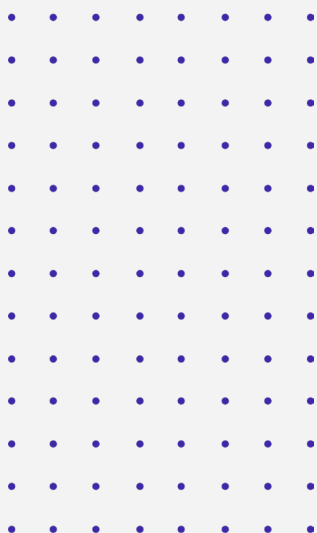
Unternehmen müssen in der Lage sein, alle Benutzerinteraktionen zu bestätigen und reibungslos zu autorisieren sowie eine kontinuierliche Authentifizierung über die gesamte Benutzungsdauer zu gewährleisten.

Authentifizierungsereignisse überwachen

Das Erkennen verdächtiger Verhaltensmuster ist eine schwierige Aufgabe. Um betrügerische Benutzer zu erkennen, brauchen die Unternehmen Einblick in alle Benutzeraktivitäten sowie die Fähigkeit, ungewöhnliches Benutzerverhalten zu erkennen und zu überwachen.

Sicherheit über digitale Plattformen hinweg durchsetzen

Angesichts der rasant zunehmenden mobilen Nutzung benötigen immer mehr Geräte erweiterten Schutz beim Management von Anwendungen sowie IoT- und Mobilgeräten. Dieser Trend macht eine nahtlose Durchsetzung und Sicherung der digitalen Identität erforderlich.



Unternehmen müssen in der Lage sein, alle Benutzerinteraktionen zu bestätigen und reibungslos zu autorisieren sowie eine kontinuierliche Authentifizierung im gesamten Verlauf der User Journey zu gewährleisten.

Mit IBM Cloud™ Identity können Administratoren die Anwendungsnutzung, Leistungsabfälle und Anmeldeaktivitäten mühelos überwachen. Erkunden Sie das Administratordashboard in diesem dreiminütigen Video.

[Video ansehen](#)

Kennwortschutz ohne Mühe

Der Schutz der digitalen Identität eines Benutzers — ob interner Mitarbeiter, Partner oder Kunde — stellt für Unternehmen eine große Herausforderung dar. **Insbesondere Kunden möchten die Gewissheit haben, dass bei der Nutzung einer Anwendung ihre digitale Identität sicher ist. Zugleich wünschen sie sich jedoch eine benutzerfreundliche und komfortable Anwendung.**



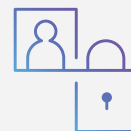
Komplexe Sicherheitsmaßnahmen

Sicherheit ist der entscheidende Faktor, damit Kunden einem Unternehmen vertrauen. Dabei möchten Benutzer jedoch nicht gezwungen sein, mit komplexen Sicherheitsmaßnahmen umzugehen — sie erwarten, dass die Sicherheitskomponenten von Anwendungen im Hintergrund laufen und keinen Komfortverlust für sie darstellen.



Mehrfache Benutzernamen und Kennwörter

Kunden müssen sich für die Anwendungen, die sie nutzen, verschiedene Benutzernamen und Kennwörter merken. Jede Anwendung, die eigene Anmeldeinformationen erfordert, wirkt für Benutzer abschreckend.



Gesicherte Konten

Benutzer wünschen einen reibungslosen Ablauf, doch sie wollen für ihren Komfort nicht den Datenschutz opfern. Wenn sie einem Unternehmen ihre Daten anvertrauen sollen, erwarten sie ein hohes Maß an Schutz.

Benutzer erwarten, dass die Sicherheitskomponenten von Anwendungen im Hintergrund laufen und keinen Komfortverlust für sie bedeuten.



Kriterien für eine effektive Identitäts- und Zugriffsmanagementlösung (IAM)

Für ein reibungsloses und sicheres Identitätsmanagement sollten Sie darauf achten, dass Ihre IAM-Plattformen folgende Merkmale aufweisen:

SSO-Funktionalität (Single Sign-on)

- Vermeiden Sie das lästige Eingeben diverser Benutzernamen und Kennwörter durch die Fähigkeit, sich bei allen Anwendungen mit einem einzigen Satz von Anmeldeinformationen anzumelden.

Mehrfaktorauthentifizierung

- Verstärken Sie die Sicherheit durch Verwendung mehrerer Benutzerauthentifizierungsverfahren.

Benutzer-Lebenszyklusmanagement

- Optimieren Sie die Onboarding- und Offboarding-Prozesse für Benutzer.

Integration in vorhandene Benutzerverzeichnisse und Anwendungen

- Bieten Sie die Option, vorhandene Benutzerverzeichnisse entweder in der Cloud oder vor Ort zu speichern.

Informationen über Benutzer und Geräte

- Verknüpfen Sie die Lösung mit Betrugserkennungs- und Mobilgerätemanagement-Plattformen, um Zugriffsentscheidungen auf der Basis relevanter Informationen zu treffen.

Expertise für eine erfolgreiche Lösung

- Wählen Sie als Partner einen Provider, der auch Planungs-, Support- und Implementierungsservices anbietet.

IBM Cloud Identity

Die IBM Cloud Identity-Lösung unterstützt IT-, Sicherheits- und sonstige Unternehmensverantwortliche nicht nur dabei, das Unternehmen auf Zeitalter des Cloud-Computing auszurichten, sondern bietet auch die nächste Generation von Innovationen im Hinblick auf die Benutzerproduktivität. Mit IBM Cloud Identity machen Sie die Investition in Ihr Identitäts- und Zugriffsmanagement zukunftssicher.

IBM Cloud Identity hilft Unternehmen, einen schnellen, sicheren Zugriff auf Geschäftsanwendungen bereitzustellen. Sehen Sie in diesem zweiminütigen Video, wie die IDaaS-Technologie von IBM® Benutzer und Anwendungen miteinander verbindet.

[Video ansehen](#) 

Quellen

1. Bericht zu den Kosten einer Datenschutzverletzung 2019. Umfrage des Ponemon Institute im Auftrag von IBM Security.

2. „Forrester Analytics: IAM Software Forecast, 2018 to 2023 (Global)“, Forrester Research, Inc., 10. Mai 2019. Im Auftrag von IBM.

IBM Deutschland GmbH

IBM-Allee 1
71139 Ehningen
[ibm.com/de](https://www.ibm.com/de)

IBM Österreich

Obere Donaustraße 95
1020 Wien
[ibm.com/at](https://www.ibm.com/at)

IBM Schweiz

Vulkanstrasse 106
8010 Zürich
[ibm.com/ch](https://www.ibm.com/ch)

Die IBM Homepage finden Sie unter:

[ibm.com](https://www.ibm.com)

IBM, das IBM Logo, [ibm.com](https://www.ibm.com) und IBM Cloud sind eingetragene Marken oder Marken der IBM Corporation in den USA und/oder anderen Ländern. Sind diese und weitere Markennamen von IBM bei ihrem ersten Vorkommen in diesen Informationen mit einem Markensymbol (® oder ™) gekennzeichnet, bedeutet dies, dass IBM zum Zeitpunkt der Veröffentlichung dieser Informationen Inhaber der eingetragenen Marken oder der Common-Law-Marken (common law trademarks) in den USA war. Diese Marken können auch eingetragene Marken oder Common-Law-Marken in anderen Ländern sein. Eine aktuelle Liste der IBM Marken finden Sie auf der Webseite „Copyright and trademark information“ unter: [ibm.com/legal/copytrade.shtml](https://www.ibm.com/legal/copytrade.shtml) Weitere Unternehmens-, Produkt- oder Servicennamen können Marken von anderen Unternehmen sein.

Vertragsbedingungen und Preise erhalten Sie bei den IBM Geschäftsstellen und/oder den IBM Business Partnern. Die Produktinformationen geben den derzeitigen Stand wieder. Gegenstand und Umfang der Leistungen bestimmen sich ausschließlich nach den jeweiligen Verträgen.

© Copyright IBM Corporation 2020



Bitte der Wiederverwertung zuführen
