okta

Der strategische Wert von Identity-Management für CIOs

Unternehmen beschleunigen den Umstieg in die Cloud und versuchen verstärkt, durch IT-gestützte Effizienz Wettbewerbsvorteile zu erzielen. In diesem Zuge hat sich das Identity-Management für CIOs mit ihrem Fokus auf das Business Enablement zu einem kritischen Faktor – und oft auch zu einem Engpass – entwickelt. Dieser Executive Brief fasst die Erkenntnisse aus einer Studie* zusammen, die von der Enterprise Strategy Group in Zusammenarbeit mit Okta zu dieser Entwicklung durchgeführt wurde. Dies sind die fünf wichtigsten Erkenntnisse zur Bedeutung von Identity-Management für CIOs:

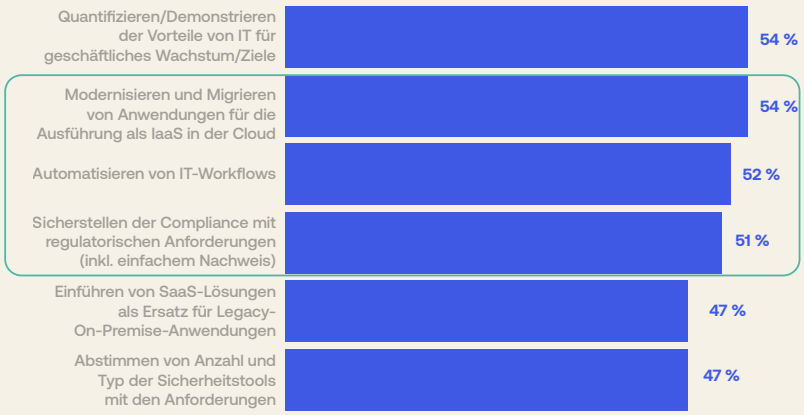
1. Die grundlegende Herausforderung für CIOs besteht darin, Business Enablement und Schutz für das Unternehmen optimal aufeinander abzustimmen
2. Fehlende Identity-Automatisierung hemmt die IT-Effizienz
3. Identity-Programme sind der ausschlaggebende Faktor für erfolgreiches Business Enablement
4. Fragmentierung ist eine unterschätzte Hürde für das Identity-Management
5. CIOs sind sich bewusst, das ihr Identity-Management dringend optimiert werden muss

WICHTIGE ERKENNTNIS Nr. 1:

Die grundlegende Herausforderung von CIOs besteht darin, Business Enablement und Schutz für das Unternehmen optimal aufeinander abzustimmen

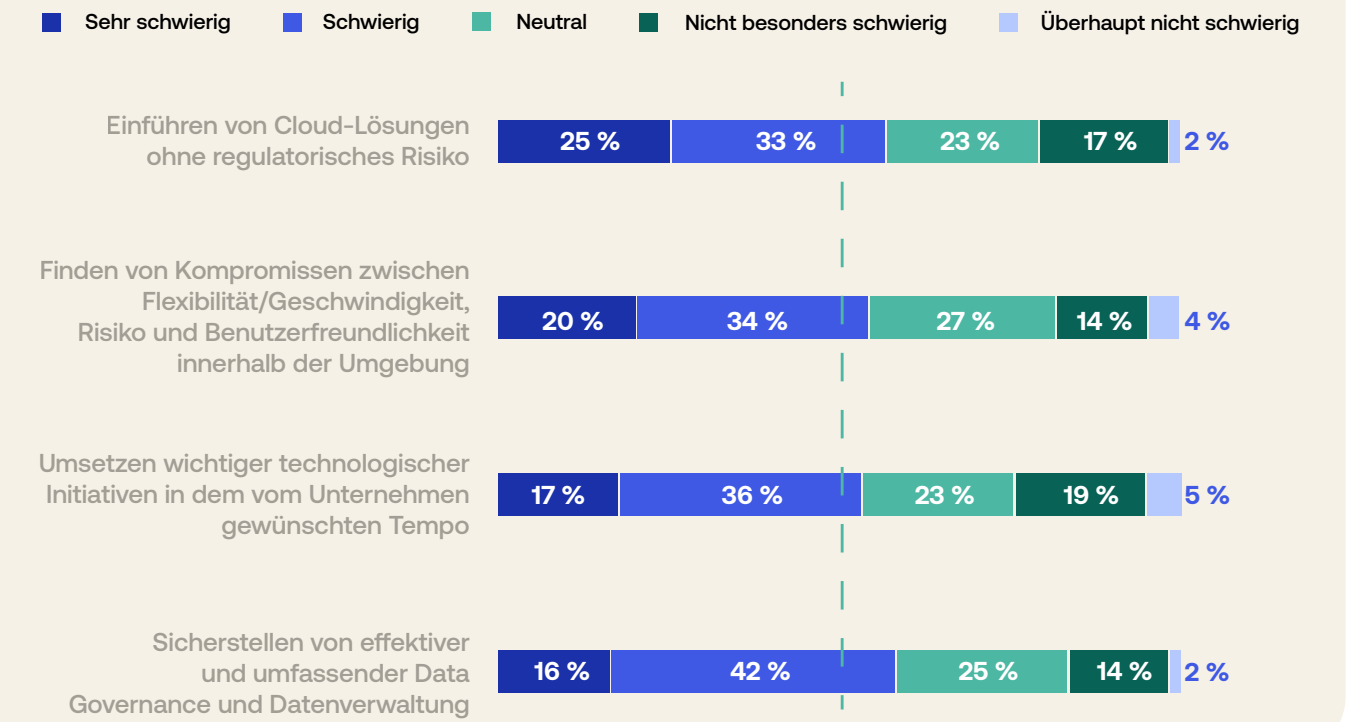
Wenig überraschend müssen CIOs überzeugend darlegen, wie die IT wichtige Geschäftsziele unterstützt und das geschäftliche Wachstum insgesamt möglich macht. Doch die Antworten zu anderen Top-Prioritäten lassen kritische Spannungen erkennen, die sich daraus ergeben, dass einerseits geschäftliche Abläufe beschleunigt und die Effizienz gesteigert werden sollen und gleichzeitig weder Sicherheit noch Compliance beeinträchtigt werden dürfen.

Wichtigste Aufgaben der CIOs



Die genauere Analyse der wichtigsten Herausforderungen von CIOs zeigt deutlich, dass die Gratwanderung zwischen Business Enablement und Schutz des Unternehmens äußerst schwierig ist. Denn dazu müssen Cloud-Lösungen in Einklang mit regulatorischen Anforderungen eingeführt, Kompromisse zwischen Flexibilität und Risiko gefunden, wichtige technologische Initiativen beschleunigt und gleichzeitig Daten angemessen kontrolliert und verwaltet werden.

Größte Herausforderungen für CIOs

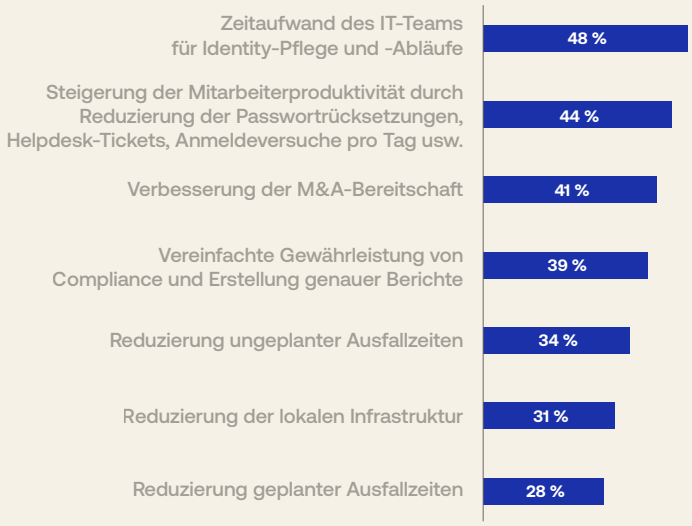


WICHTIGE ERKENNTNIS Nr. 2:

Fehlende Identity-Automatisierung hemmt die IT-Effizienz

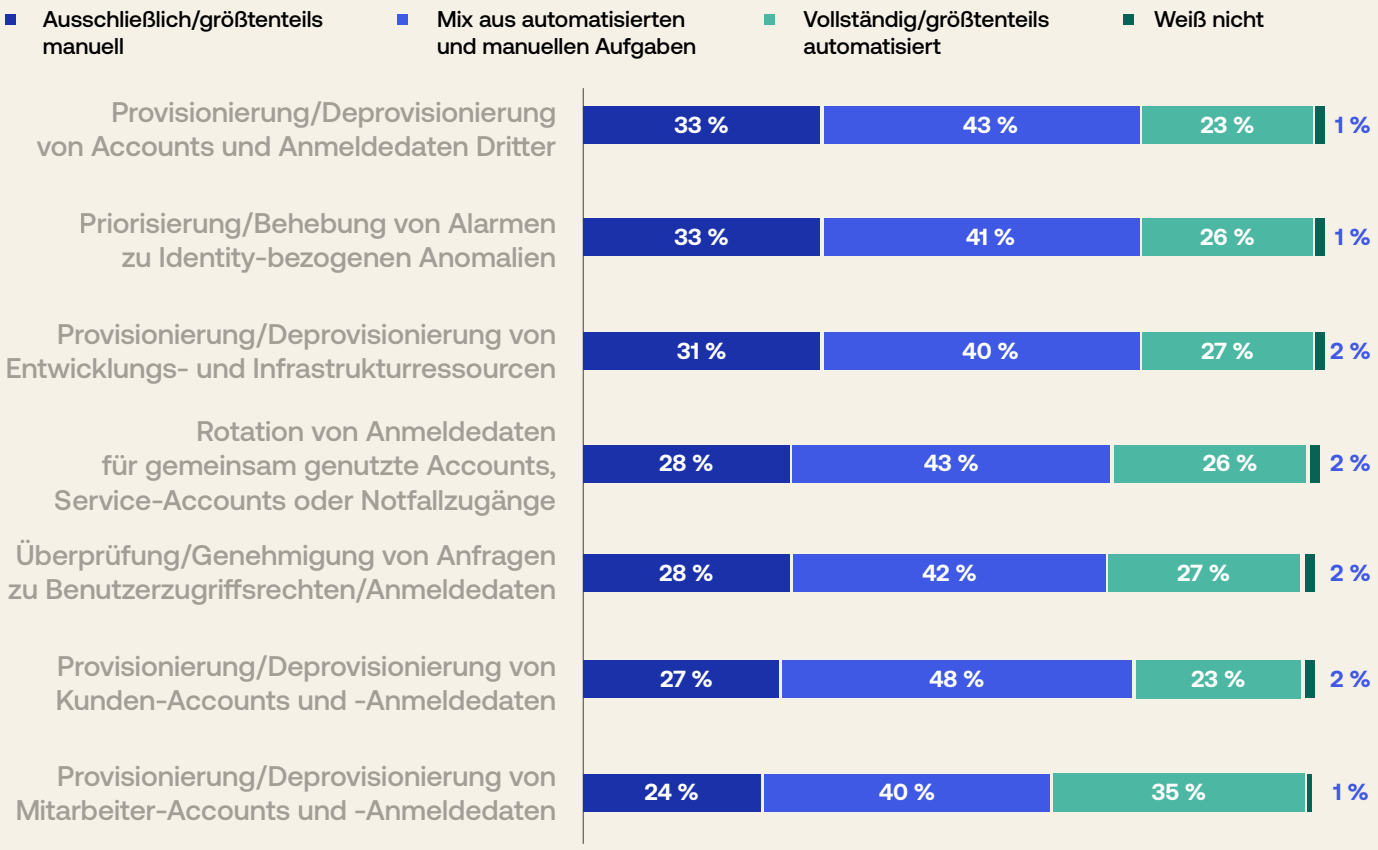
Das Automatisieren von IT-Workflows gehört zu den wichtigsten Prioritäten der CIOs. Die Befragung der CIOs ergab, dass der Zeitaufwand des IT-Teams für Identity-Pflege und -Abläufe inzwischen die wichtigste Leistungskennzahl darstellt (gefolgt von der Reduzierung der Produktivitätsbeeinträchtigungen durch Identity-bezogene Probleme wie Passwortrücksetzungen oder übermäßig viele Anmeldungen pro Tag). Überraschenderweise rangieren diese Identity-bezogenen KPIs vor klassischen KPIs wie die Reduzierung geplanter und ungeplanter Ausfallzeiten oder die Reduzierung der lokalen Infrastruktur.

Wichtigste KPIs für CIOs



Die IT-Effizienz wird jedoch häufig durch fehlende Automatisierung ausgebremst. Bei Identity-Workflows ist Automatisierung sogar die Ausnahme und weit von der Norm entfernt. Weniger als ein Drittel der befragten CIOs gab an, grundlegende Identity-Aufgaben automatisiert zu haben.

Wie stark sind Ihre grundlegenden Identity-Aufgaben automatisiert?



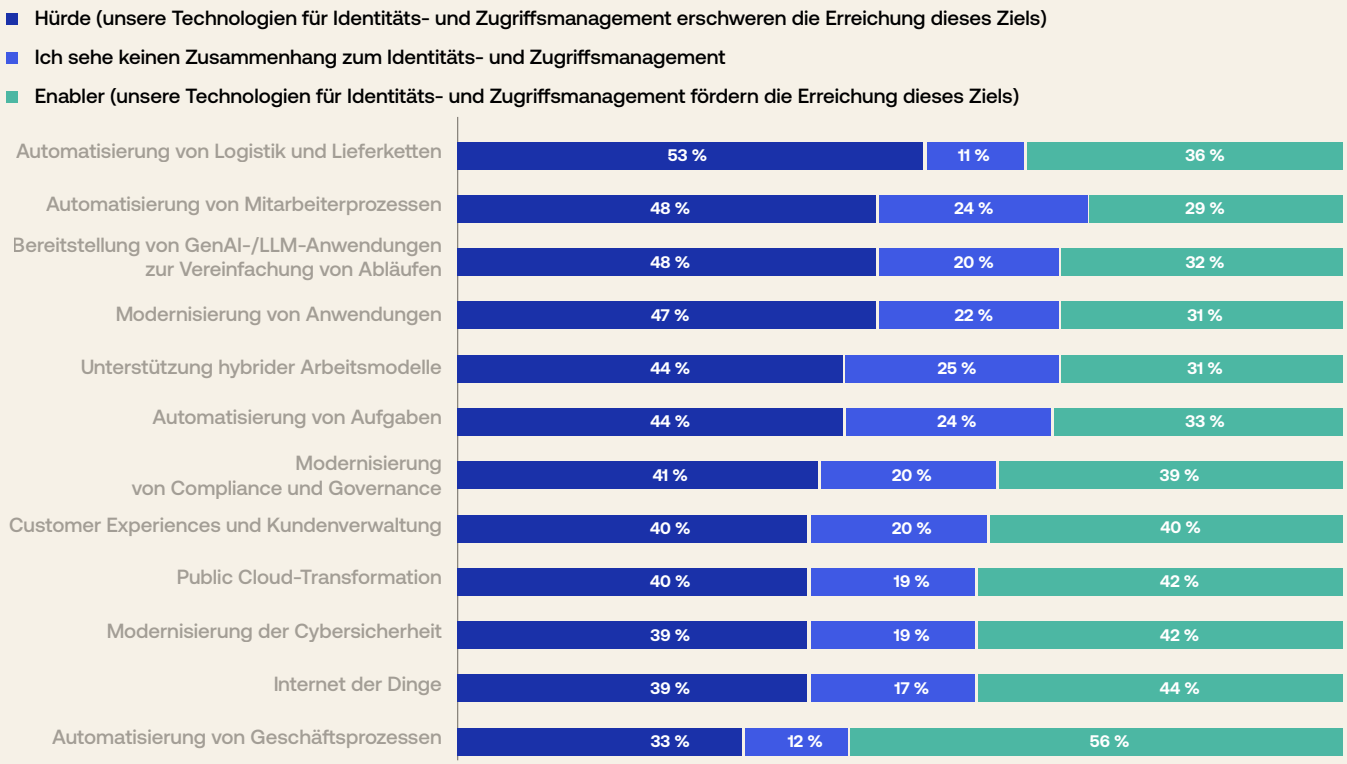
WICHTIGE ERKENNTNIS Nr. 3:

Identity-Programme sind der ausschlaggebende Faktor für erfolgreiches Business Enablement

Allgemein betrachtet, räumt der Großteil der befragten CIOs ein, dass Identity-Programme ein kritischer Faktor dafür sind, ob sie in ihrer Funktion als Business Enabler erfolgreich sind – oder eben nicht. Leider sagt fast die Hälfte von ihnen, dass ihre derzeitigen Identity-Lösungen für das Business Enablement eher kontraproduktiv sind.

Viele CIOs sind der Meinung, dass ihr derzeitiger Identity-Ansatz für die Initiativen, mit denen sie eigentlich vorankommen möchten, eher hinderlich ist.

Zwischen 38 % und 48 % geben an, dass ihr Identity-Tech-Stack sie einschränkt. Und zwischen 75 % und 81 % sind sich bewusst, dass ihr Identity-Stack wichtige geschäftliche Initiativen beeinflusst.



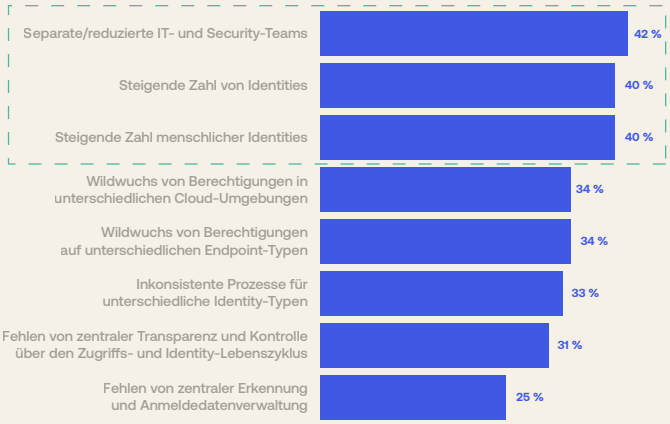
WICHTIGE ERKENNTNIS Nr. 4:

Fragmentierung ist eine unterschätzte Hürde für das Identity-Management

Erwartungsgemäß bewerteten CIOs die steigende Zahl menschlicher und nicht-menschlicher Identities als eine der größten Herausforderungen für das Identitäts- und Zugriffsmanagement (IAM). Die Zunahme der Identities ist die Hauptursache für den Berechtigungswildwuchs, der auf der Liste der Herausforderungen ebenfalls ganz oben steht.

Ein weiteres großes Problem ist die Fragmentierung der zuständigen Teams und der für die Verwaltung all dieser Identities und Berechtigungen eingesetzten Technologien. CIOs nennen vor allem separate IT- und Security-Teams als wichtigsten erschwerenden Faktor. Das Fehlen von zentraler Erkennung, Transparenz, Kontrolle und Verwaltung der Identities und Anmeldedaten rundet die Liste ab.

Größte Problembereiche der CIOs mit Blick auf das Identitäts- und Zugriffsmanagement



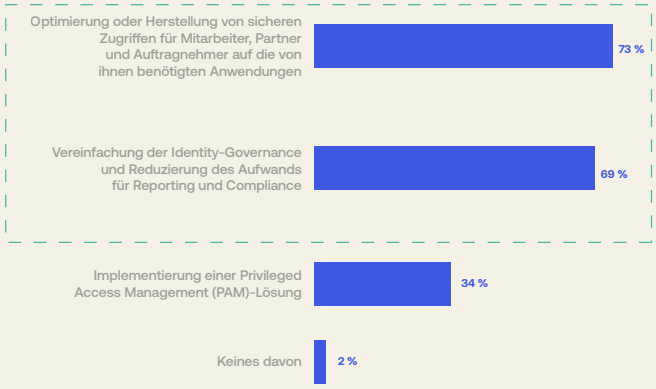
Interessanterweise erkennen die CIOs den Wildwuchs an Sicherheitstechnologie als wesentlichen Faktor für Fragmentierungsprobleme. Möglicherweise unterschätzen sie dennoch die Tragweite dieses Problems. Die befragten CIOs gaben an, im Durchschnitt mit 44 verschiedenen Cybersicherheitsanbietern zu arbeiten. Obwohl diese Zahl bereits beunruhigend hoch ist, liegt sie noch weit unter den Schätzungen der CISOs, die sich bei knapp 60 unterschiedlichen Sicherheitstools bewegten.

WICHTIGE ERKENNTNIS Nr. 5:

CIOs sind sich bewusst, das ihr Identity-Management dringend optimiert werden muss

Die Untersuchung endete mit einem positiven Ergebnis: Der Großteil der CIOs ergreift entschiedene Maßnahmen, um die Herausforderungen mit Blick auf das Identity-Management zu überwinden, die sowohl der Effizienz als auch dem Business Enablement im Weg stehen. Konkret planen rund 70 % der CIOs für 2025 umfassende Initiativen zur Optimierung sicherer Zugriffe und Vereinfachung der Identity-Governance. Dies ist ein Indiz dafür, dass die befragten CIOs die Notwendigkeit modernisierter Identity-Programme ganz eindeutig erkannt haben. Zudem planen sie ganz klar Investitionen in Lösungen, mit denen sich für diesen Eckpfeiler von IT-gestütztem Business Enablement ein höheres Maß an Effizienz, Automatisierung und Kontrolle umsetzen lässt.

CIOs planen für 2025 Investitionen in Identity-Management



Lösungen von wie vielen Cybersicherheits-anbietern sind bei Unternehmen im Einsatz?

CIOs: ca. 44

CISOs: ca. 60

Mit Okta zu einer Identity-zentrierten Sicherheitsstrategie

Die Studie von ESG zeigt, dass sich Identity-Management zu einem wesentlichen Faktor von Business Enablement entwickelt hat. Die derzeitigen Identity-Programme stellen hingegen eine permanente Hürde für wichtige Initiativen dar, da insbesondere durch die fehlenden Automatisierungsmöglichkeiten und die allgegenwärtige Fragmentierung des Identity-Managements Reibungsverluste entstehen. Die einheitliche Identity-Plattform von Okta geht genau diese Herausforderungen an, da sie CIOs moderne Identity-Tools zur Verfügung stellt, mit denen sich die Effizienz steigern und die digitale Transformation beschleunigen lässt.

* Die Studie/Umfrage wurde von Enterprise Strategy Group in Zusammenarbeit mit Okta durchgeführt. Dazu wurden im Januar und Februar 2025 mehr als 150 CIOs in Nordamerika, EMEA und APJ befragt.

Möchten Sie mehr über die Plattform erfahren?

Gerne sprechen wir mit Ihnen über Ihre konkreten Herausforderungen und zeigen Ihnen, die Okta Sie unterstützen kann.

Mehr erfahren