Whitepaper

Ihr Leitfaden zur Steigerung des Identity-Reifegrads

Eine Roadmap zur Steigerung der Produktivität, Verbesserung der User Experiences und Optimierung der Sicherheit mit Identity

Inhaltsverzeichnis

Identity unterstützt Geschäftsziele

Hinter der digitalen Identität stand einst ein einfacher Dienst zur Verwaltung von Benutzernamen und Passwörtern. Mittlerweile ist Identity eine tragende Säule moderner Unternehmen, die damit auf sichere Weise mit ihrer Belegschaft, Kunden und Partnern interagieren – ganz gleich, wo diese sich befinden und welche Geräte sie nutzen – und diese Interaktionen überwachen und kontrollieren können. Identity ist integraler Bestandteil jedes Aspekts unserer Online-First-Welt. Sie führt zu ansprechenden oder enttäuschenden User Experiences, verbessert oder erschwert Sicherheitsuntersuchungen, spart oder kostet Zeit und Geld für die IT-Abteilung und unterstützt oder verkompliziert die GRC-Initiativen (Governance, Risiko und Compliance) des Unternehmens. Aus diesem Grund spielt Identity eine Rolle für viele Geschäftsergebnisse, darunter operative Effizienz, Kostenkontrolle und Umsatzwachstum, und leistet ihren Beitrag bei der Stärkung der Cybersicherheit. Angesichts dieses Stellenwertes überrascht es kaum, dass die Modernisierung und Verbesserung der Kunden- und Mitarbeiteridentitätssysteme für viele Unternehmen eine Herausforderung darstellt.

Identity spielt eine wichtige Rolle dabei, wie Unternehmen mit Benutzern interagieren, und leistet daher einen Beitrag zum Erreichen der Geschäftsziele:

Umsatzsteigerung:

In vielen Branchen haben User Experiences einen enormen Einfluss auf die Wettbewerbsfähigkeit, und Identity hat einen hohen Stellenwert bei der Optimierung dieser Experiences.

60 %

der Benutzer würden wahrscheinlich mehr Geld ausgeben, wenn die Anmeldung einfach, sicher und reibungslos erfolgt.[1]

Geringere Kosten und höhere Effizienz:

Die mit einer Identity-Plattform einher gehende Konsolidierung, Integration und Automatisierung trägt dazu bei, dass die IT-Abteilung und die Belegschaft effizienter arbeiten können, die Software-Ausgaben optimiert werden und die Time-to-Market verkürzt wird.

22 %

Unternehmen, die stark in Automatisierung investieren, können ihre Kosten im Vergleich zu Nachzüglern um 22 % senken.[2]

Stärkere Cybersicherheit:

Als wichtigster Angriffsvektor in der aktuellen Bedrohungslandschaft spielt Identity in Ihrer Sicherheitsumgebung eine zentrale Rolle.

61 %

der Unternehmen betrachten die Verwaltung und Absicherung digitaler Identitäten als Top-3-Priorität ihres Sicherheitsprogramms.[3]

[1] Der Customer Identity Trends Report, Okta, 2023

[2] Bain and Company, 2023

[3] 2023 Trends in Securing Digital Identities, Identity Defined Security Alliance

Das Identity-Reifegrad-modell

Untersuchungen[4] zeigen, dass bei Mitarbeiter-identität führende Unternehmen folgende Vorteile verzeichnen:

3,9 mal

häufiger Verbesserung der geschäftliche Flexibilität durch Identity-Lösungen

3,4 mal

häufiger deutliche Verbesserung der Incident Response durch Identity-Lösungen

3,6 mal

häufiger Verbesserung der Mitarbeiterproduktivität durch Identity-Lösungen

3,2 mal

häufiger deutliche Verbesserung beim Stoppen von Bedrohungen durch Identity-Lösungen

Das Identity-Reifegradmodell von Okta ist ein Framework zur Bewertung des aktuellen Zustands und der Effektivität Ihrer Identity-Lösung, zur Entwicklung eines Plans für die Reifegrad-Verbesserung sowie für die Bewertung der Erfolge und des Mehrwerts. Wenn Sie den Reifegrad Ihrer Identity-Umgebung kennen und wissen, wie Sie durch Verbesserungen an dieser Stelle Ihre Geschäftsziele leichter erreichen und einen höheren Mehrwert erzielen, können Sie Ihre Maßnahmen und Investitionen am besten konzentrieren.

Ausgehend von den Mustern und Best Practices, die wir bei Tausenden Okta-Kunden beobachtet haben, haben wir ein detailliertes Reifegradmodell entwickelt, das Ihnen dabei hilft, eine Identity-Journey zu planen und alle relevanten Kriterien zu evaluieren. Dieses Whitepaper stellt die verschiedenen Aspekte vor, die den Reifegrad der Mitarbeiteridentität für Angestellte, Auftragnehmer und Partner bzw. der Kundenidentität für Kunden, Lieferanten und andere bestimmen. Untersuchungen und Kundenberichte zeigen, dass der Einfluss von Identity auf den geschäftlichen Erfolg mit zunehmendem Identity-Reifegrad wächst.

Analyse des Identity-Reifegrads und Bewertung des Erfolgs

Der erste Schritt ist eine gründliche und realistische Analyse Ihrer bestehenden Identity-Lösung. Dabei untersuchen wir Identity in drei Kategorien: operative Flexibilität, User Experiences sowie Sicherheit und Compliance. Während des Ausbaus Ihrer Identity-Lösung sollten Sie überlegen, wie Ihre Maßnahmen zu Ihren Geschäftsergebnissen beitragen. Durch die kontinuierliche Messung der KPIs (Key Performance Indicators) und ihre Zuordnung zu Geschäftsergebnissen (siehe Tabelle 1) können Sie Fortschritte nachweisen und sich zusätzliche Unterstützung im Unternehmen sichern.

Abgesehen von diesen drei Kategorien empfiehlt jede Stufe Maßnahmen, mit denen eine unternehmensweite Identity-Strategie definiert, optimiert, implementiert und evaluiert wird.

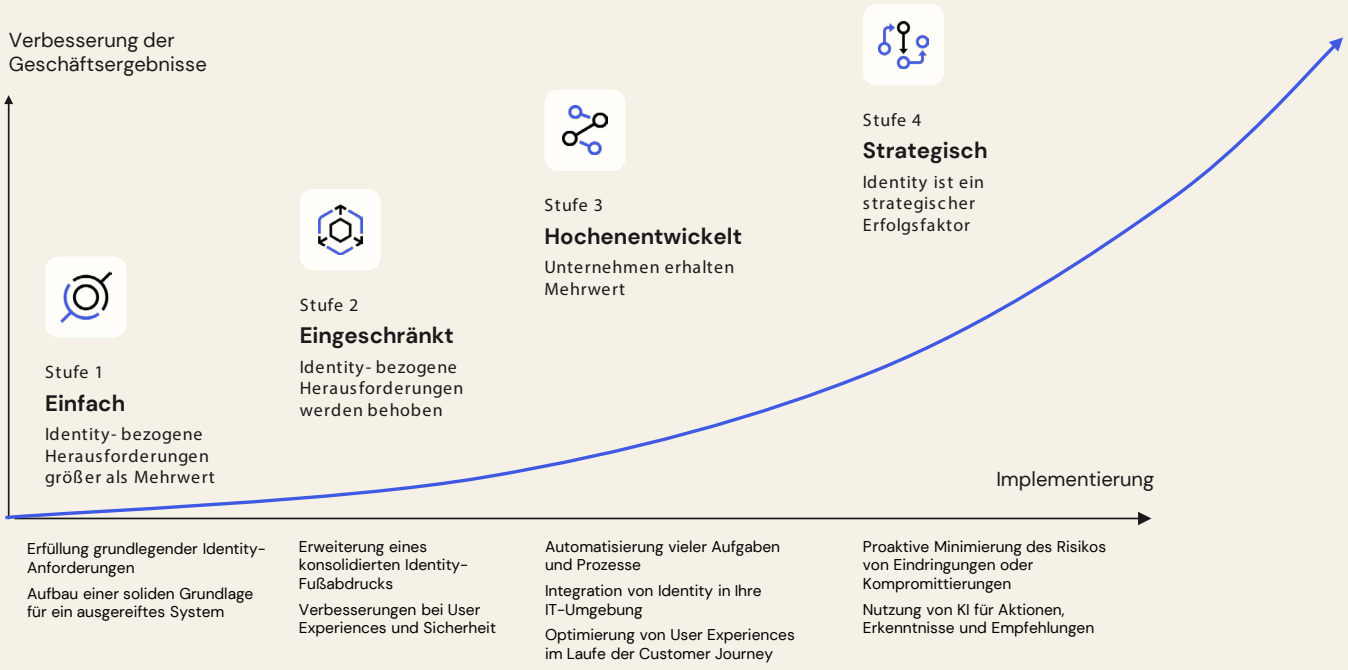
[4] The benefits of a mature approach to Identity Management, Enterprise Strategy Group, im Auftrag von Okta

Kategorie	Beschreibung der Möglichkeit	Kennzahlen zur Messung des Identity-Erfolgs	Beitrag zu Geschäftsergebnissen
Operative Flexibilität	**Entwicklung, Bereitstellung und Verwaltung von Identity-Services und -Prozessen,** z. B. • Integration von Identity in neue digitale Kanäle oder Anwendungen • Verwaltung des Workforce Lifecycle • Bereitstellung neuer oder verbesserter Identity-Funktionen • Schnelle Bereitstellung neuer Angebote für Kunden • Einfache und schnelle Skalierung bei Nachfrageschwankungen	• IT-Vollzeitmitarbeiter-Stunden für Identity-Verwaltung und Support • Zeit zur Implementierung und Bereitstellung von Anwendungen • Kosten oder Zeit für die Pflege der Identity-Infrastruktur • Anzahl der Helpdesk-Tickets zu Zugriffsproblemen oder Zugriffsanfragen für Anwendungen • Zeit zur Behebung von Identity-Helpdesk-Problemen • Time-to-Market für Kundenanwendungen	Geringere Kosten und höhere Effizienz • Entwicklung und Pflege von Identity mit weniger Aufwand • Vereinfachte M&As und schnellere Wertschöpfung Höherer Umsatz • Kürzere Time-to-Market
User Experiences	**Bereitstellung effektiver, ansprechender und unkomplizierter User Experiences,** z. B. Für alle: • Einheitliche, zuverlässige Experiences für alle digitalen Lösungen und Kanäle Für Mitarbeiter: • Nahtloser Remote-Zugriff • Vom ersten Tag an verfügbare Anwendungen • Effizienter Self-Service für Antragsteller und Prüfer Für Kunden: • Reibungslose Prozesse für Registrierung, Anmeldung usw. • Self-Service • Personalisierung	• Werte für Mitarbeiterzufriedenheit (eSAT) • Metriken für Customer Experiences (z. B. NPS, CSAT) • Zeitaufwand für Benutzer, die sich anmelden oder auf Anforderungen der Step-up-Authentifizierung reagieren • Zeitaufwand für Benutzer, die auf den Zugriff auf neue Anwendungen oder auf das Onboarding warten • Abbrüche durch Kunden bei Registrierung und Anmeldung • Kunden-Konversionsraten (vom Besucher bis zum registrierten Account) • Ungeplante Ausfallzeiten pro Monat	Höhere Effizienz • Optimierung des Endbenutzer-Zugriffs Höherer Umsatz • Steigerung der Konversionsrate bei Anmeldung/Registrierung • Personalisierung von Customer Experiences • Entwicklung nahtloser User Experiences auf allen Kanälen • Vereinfachtes Onboarding für Enterprise-Kunden
Sicherheit und Compliance	**Proaktive Minimierung und Behebung von Bedrohungen, Umsetzung des Least-Privilege-Ansatz und Unterstützung der Vorschriften-Compliance,** z. B. • Sicherer Zugriff für Mitarbeiter und Kunden • Reduzierung der Identity-Angriffsfläche • Unterstützung für Identity Governance-Initiativen • Verwaltung privilegierter Zugriffe • Unterstützung für Zero-Trust-Prozesse • Unterstützung von Datenschutz-Anforderungen • Schutz vor Identitätsdiebstahl	• Anzahl der Identity-bezogenen Sicherheitsvorfälle • Zeit und Kosten für die Erkennung und Behebung Identity-bezogener Sicherheitsvorfälle und Kompromittierungen • Zeit und Kosten für Audit- und Compliance-Berichte • Akzeptanz der erweiterten Authentifizierung bei Mitarbeitern • Anzahl der Account-Hacking-Vorfälle	Geringere Kosten und höhere Effizienz • Vereinfachung von Governance und Compliance • Optimierung der Software-Ausgaben • Höherer Umsatz • Steigerung des Kundenvertrauens ohne Beeinträchtigung der User Experiences Stärkere Cybersicherheit • Proaktive Behebung von Identity-bezogenen Bedrohungen • Stoppen von Phishing-Angriffen • Schaffung von Vertrauen bei Kunden

Planen Sie Ihre Journey Schritt für Schritt

Das Identity-Reifegradmodell von Okta besteht aus vier Stufen mit Fokus auf verschiedene Identity-Funktionen. Es zeigt, wie Sie die gewünschten Geschäftsergebnisse und den maximalen Nutzen für Ihr Unternehmen erzielen können. Wir stellen die für jede Stufe typischen Herausforderungen für Unternehmen vor, empfehlen nächste Schritte zur Behebung von Schwierigkeiten und das Erreichen der nächsten Stufe und gehen darauf ein, welche Ergebnisse Sie erwarten können. Für jede Stufe empfehlen wir Maßnahmen zum Aufbauen, Implementieren und Bewerten einer unternehmensweiten Identity-Strategie. Auch wenn es keinen allgemeingültigen Identity-Ansatz gibt, ist dieses Framework flexibel genug, um allen an der Verbesserung ihres Identity-Reifegrads interessierten Unternehmen wertvolle Hinweise zu geben.

Identity-Reifegradmodell



Stufe 1: Einfach

Betrachten Sie Identity als Gesamtkonzept und nicht nur als Sammlung von Funktionen

In dieser ersten Reifegradstufe kann für Unternehmen Folgendes gelten:

- Sie beginnen damit, ihren Kunden digitale Services oder Online-Portale anzubieten.
- Sie müssen Ineffizienzen und eine große Angriffsfläche bewältigen, da die Identity-Lösungen für ihre Belegschaft und die Partner nicht miteinander verknüpft sind.

Wenn keine Identity-Strategie festgelegt wurde, wenden Entwickler erhebliche Zeit und Ressourcen für den Aufbau und die Pflege lokaler oder eigenentwickelter Identity-Funktionen auf. Die Verwaltung der Mitarbeiteridentitäten ist aufgrund von M&A-Aktivitäten, der Erweiterung auf die Cloud sowie wegen des Einsatzes von Legacy-Anwendungen auf mehrere User Stores und Systeme verteilt. User Experiences sind eher schlecht: Die Prozesse zur Registrierung von Kunden sind in den verschiedenen Bereichen inkonsistent, während die Produktivität der Mitarbeiter durch begrenzte Föderation und die Abhängigkeit von mehreren Passwörtern beeinträchtigt wird. Die Zuverlässigkeit und Verfügbarkeit der Identity stellt eine Herausforderung dar – und die Prozesse sind nur minimal oder gar nicht automatisiert. Es gibt nur wenige oder komplizierte Integrationen mit anderen Systemen, die zudem erheblichen Aufwand aufseiten der Administratoren erfordern. Der Identity-Wildwuchs und die daraus resultierende fehlende Transparenz führen zu wachsenden Sicherheitsrisiken. Gleichzeitig sind alle Identity-bezogenen Sicherheitsmaßnahmen reaktiv.

In dieser Phase liegt der Fokus darauf, grundlegende Identity-Anforderungen zu erfüllen (z. B. das Onboarding von Kunden über ein einziges Portal ermöglichen, einige Identity-Sicherheitskontrollen implementieren) und gleichzeitig eine robuste und zuverlässige Grundlage für die Steigerung des Reifegrads zu schaffen.

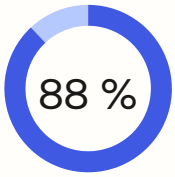
Die strategischen Schritte in dieser Phase sind:

- Erstellen eines Inventars aller On-Premise- und Cloud-Anwendungen, die im Unternehmen eingesetzt werden
- Abstimmen der Programme für Kunden- und Mitarbeiteridentitäten mit gemeinsamen geschäftlichen und Governance-Zielen

Aufbau und Pflege einer eigenentwickelten Customer Identity-Lösung bremst die Time-To-Market aus[5]

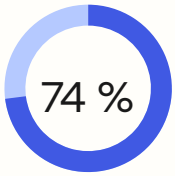
3. Platz bei Zeitaufwand

Bei den zeitaufwändigsten Aufgaben bei eigenentwickelten Anwendungen nimmt Aufbau und Pflege der Authentifizierung Platz 3 ein.



der Unternehmen, die eine SaaS-Plattform eines Drittanbieters für die Authentifizierung nutzen, konnten ihre Time-to-Market verkürzen

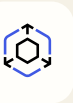
vs.



der Unternehmen, die auf eigenentwickelte Authentifizierung setzen

[5] Wie Development-Teams ihre SaaS-Dienste beziehen, SD Times, im Auftrag von Okta

Kategorie	Herausforderungen für das Identity-Management	Was Sie tun sollten	Wie Ihr Business profitiert
Operative Flexibilität	• Aufbau/Pflege von On-Premise-, eigenentwickelten oder fragmentierten Identity-Services ist schwierig und für Administratoren und Entwickler mit hohem Zeitaufwand verbunden	• Implementierung eines einheitlichen Benutzerverzeichnisses, um User-Repositories für alle Legacy-Verzeichnisse und Aufzeichnungssysteme konsolidieren und synchronisieren zu können • Implementierung einer grundlegenden Administrator-UI zur User Lifecycle-Verwaltung	Weniger Zeitaufwand für das IT-Team in diesen Bereichen: • Pflege und Synchronisation von User Stores • Verwaltung von Benutzer- und Gruppenzugriffen
User Experiences	• Probleme in Bezug auf Zuverlässigkeit und Verfügbarkeit • Erhebliche Reibungspunkte bei der Anmeldung, keine Anpassungsmöglichkeit bei User Experiences • Isolierte Identity-Lösungen für einzelne Geschäftsbereiche	• Einführung einer hochverfügbaren Infrastruktur mit Failover, Disaster Recovery und SLA-Standards von mehr als 99,9 % • Bereitstellung grundlegender Single Sign-On-Funktionen (SSO) und Authentifizierung für Cloud-Anwendungen für Mitarbeiter • Bereitstellung grundlegender SSO-Funktionen für die Kunden mit einigen Social Authentication-Optionen (zur Nutzung bestehender Anmeldedaten) • Implementierung einfacher Self-Service-Funktionen (z. B. Passwort-Recovery)	• Höhere Mitarbeiterproduktivität und Kundennutzung durch schnelleren Zugang zu Anwendungen • Weniger Reibungspunkte für Kunden durch Self-Service-Optionen für einfache Account-Verwaltungsaufgaben
Sicherheit und Compliance	• Sicherheitsrisiken aufgrund von Passwort-Wildwuchs, fehlender Transparenz zu Anwendungszugriffskontrollen, isolierten User Stores, fehlender Richtliniendurchsetzung usw.	• Installation eines Autorisierungsservers, der moderne Standards und grundlegende Zugriffsrichtlinien für APIs unterstützt • Schutz von Identity-Daten mit grundlegender Verschlüsselung und Hashing • Einführung von MFA (Multi-Faktor-Authentifizierung) für Mitarbeiter, die RADIUS und LDAP nutzt und moderne und ältere Anwendungen unterstützt • Einrichtung von Zugriffsrichtlinien für Mitarbeiter, die Anforderungen der Benutzergruppen und Netzwerk-Zonen berücksichtigen	• Stärkere Gesamtsicherheit für die Mitarbeiter • Weniger Account-Sperren bei Kunden durch Cyberangriffe



Stufe 2: Eingeschränkt

Erweitern Sie die Identity-Reichweite und -Funktionen und beginnen Sie mit der Automatisierung

In dieser Phase kann für Unternehmen Folgendes gelten:

- Sie haben bereits mehrere Kundenanwendungen oder Portale eingeführt und möchten weitere bereitstellen.
- Sie haben bei der Konsolidierung der Mitarbeiteridentitäten erste Erfolge erzielt und suchen nach Möglichkeiten, dies auf weitere Anwendungen auszuweiten und weitere Identity-Funktionen zu implementieren.

In dieser Phase geht es darum, auf den Erfolgen der ersten Phase aufzubauen und die konsolidierte Identity-Reichweite auf neue Anwendungen, Services, Anwendungsfälle und Benutzer auszuweiten. Wenn Unternehmen neue digitale Services bereitstellen, um ihren Marktanteil und den Kundenstamm zu erweitern, richtet sich der Fokus auf die Erstellung differenzierter, vertrauenswürdiger User Experiences für Privat- und Business-Kunden.

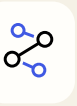
Unternehmen, die vor Ort eine kritische IT-Infrastruktur und proprietäre Technologie betreiben, können durch die Ausweitung der Identity-Funktionen auf diese Ressourcen die User Experience, die administrativen Prozesse und die Sicherheitslage verbessern.

Wenn Identity in immer mehr Bereichen genutzt wird, müssen Unternehmen sicherstellen, dass ihre Identity-Infrastruktur diese Nachfrage bewältigen kann, ohne dass Kompromisse bei der Service-Qualität nötig sind oder das IT-Team ständig mit der Skalierung und Unterstützung der Infrastruktur beschäftigt ist. Unternehmen sollten außerdem mit der Automatisierung der Identity-Prozesse beginnen, damit die Erweiterung die IT und die Anwendungsverantwortlichen nicht zu sehr belastet. Da die meisten Unternehmen bei der Cybersicherheit auf einen Zero-Trust-Ansatz setzen, ist dies eine gute Gelegenheit, Identity auch für diesen Bereich zu nutzen.

Die strategischen Schritte in dieser Phase sind:

- Kommunikation zwischen IT-, Technologie- und Security-Teams, um sich in Bezug auf Identity und Zuständigkeiten sowie Kompetenzen abzustimmen
- Bewertung von Lücken in der Identity-Infrastruktur als Grundlage für Behebungs- und Investment-Pläne

Kategorie	Herausforderungen für das Identitäts-management	Was Sie tun sollten	Wie Ihr Business profitiert
Operative Flexibilität	• Manuelles On- und Offboarding für Mitarbeiter, Kunden und Partner • Fragmentierte Identity-Repositories aus Legacy-Systemen, die sich nur schwer pflegen lassen • Spitzen/Steigerungen in der Nachfrage führen zu Leistungs- und Verfügbarkeits-problemen	• Beginn der Automatisierung des User Lifecycle Management, der Provisionierung für On- und Offboarding, der Verwaltung nachgelagerter Zugriffsrechte für Anwendungen usw. • Minimierung bzw. optional Verzicht auf Legacy-Systeme, die sich schwer pflegen/aktualisieren lassen, eigene User Stores verwenden, keine oder komplexe Integrationsfunktionen besitzen bzw. keine SSO/Föderation-Optionen bieten • Integration von Identity mit Anwendungen, die Standards wie SAML, OIDC, OAuth2 usw. verwenden • Beginn der Implementierung einiger SDKs und APIs • Gewährleisten, dass die Infrastruktur zuverlässig Spitzen/Steigerungen bei der Nachfrage bewältigen kann, ohne die Service-Qualität zu beeinträchtigen	Weniger Aufwand bzw. Kosten in diesen Bereichen: • Pflege der Identity-Infrastruktur • Helpdesk-Anfragen zu Zugriffsproblemen • Pflege und Synchronisation von User Stores • Verwaltung von Benutzer- und Gruppenzugriffen • Skalierung der Identity-Lösung Schnellere Provisionierung und Deprovisionierung von Benutzern Vereinfachte M&As für Ihre Mitarbeiter und Kunden
User Experiences	• Mehrere Anwendungen/ Portale mit inkonsistenten Login-Prozessen • Verzögerungen beim Onboarding neuer Mitarbeiter • Verfügbarkeit sicherer Authentifizierung aufgrund von On-Premise-RADIUS-Servern usw.	• Ausweitung der Integrationen für Kunden-anmeldungen auf andere Social-Media-Anbieter, z. B. Apple, Google, usw. • Unterstützung von SSO-Föderation für Kunden, Partner und Auftragnehmer, die bei anderen Identity-Anbietern bereits Identities haben • Minimierung von Reibungspunkten bei Kundenanmeldungen und -registrierungen, indem nur erforderliche Attribute abgefragt werden • Ausweitung von SSO für die Belegschaft auf geschäftskritische On-Premise-Anwendungen • Implementierung von passwortloser Authentifizierung für die Belegschaft • Launch weiterer Self-Service-Funktionen	• Weniger Reibungspunkte durch bessere Prozesse für Anmeldung und Registrierung • Höhere Produktivität und Zufriedenheit der Mitarbeiter durch Birthright-Zugriffsrechte für wichtige Anwendungen und schnellere Gewährung von Zugriff auf andere Anwendungen • Verbesserte Zuverlässigkeit mit weniger Ausfällen aufgrund von On-Premise- oder nicht redundanten Servern
Sicherheit und Compliance	• Globale Zugriffs-richtlinien führen zu einer Umgebung mit zu umfangreichen Berechtigungen • Begrenztes MFA für Belegschaft führt zu Sicherheitslücken • Ziele für Customer Experiences lassen sich nur mit Kompromissen bei der Sicherheit erreichen	• Konsolidierung der Zugriffskontrollen für die Belegschaft auf Cloud- und On-Premise-Anwendungen • Implementierung von rollenbasierter Zugriffskontrolle (RBAC) • Ausweitung starker MFA für Mitarbeiter (mit Besitzfaktoren und biometrischen Faktoren) auf Partner und Auftragnehmer und auf geschäftskritische On-Premise-Anwendungen, oder Implementierung von passwortlosen Zugriffen • Implementierung von MFA für Kunden mit Besitzfaktoren und biometrischen Faktoren, oder Implementierung von passwortlosen Zugriffen • Erste Schritte zur Einführung von Zero Trust (z. B. dynamische Zugriffsrichtlinien) • Integration mit standardbasierten API-Gateways für einen einheitlichen Blick auf die Autorisierung von Kunden • Einführung einiger Audit- und Monitoring-Tools	• Stärkere Gesamtsicherheit • Verbesserung der Compliance mit Least-Privilege-Access-Vorgaben und MFA-Zugriffskontrollen (z. B. SOX) • Weniger Zeitaufwand und Kosten für die Vorbereitung auf Audits und Compliance-Prüfungen



Stufe 3: Hochentwickelt

Steigern Sie die Automatisierung und Integration und verbessern Sie die User Experiences

Unternehmen ziehen in dieser Phase erheblichen Mehrwert aus der Identity. Der Fokus liegt dabei auf diesen Bereichen:

- Optimierung der User Experiences, um die Konversionsrate zu steigern
- Beginn der Integration von Identity in den allgemeinen Technologie-Stack, um die Effizienz zu steigern
- Implementieren eines proaktiven Ansatzes für Identity-Sicherheit

Die Integration von Identity mit anderen Systemen ermöglicht die Automatisierung von Aufgaben und Prozessen und bietet einen besseren Überblick über Benutzer und ihre Umgebung. Durch starke Integrationen mit HR-Systemen können Unternehmen zum Beispiel die Erstellung von Benutzeridentitäten, das On- und Offboarding sowie die Mitarbeiterprovisionierung automatisieren. Dadurch lassen sich die Produktivität der Belegschaft und die Effizienz der IT-Verwaltung steigern. Gleichzeitig sinken die Kosten für Software und die Sicherheitsrisiken durch Überprovisionierung werden reduziert. Durch die Integration der Kundenidentität mit Marketing- und Daten-Engines werden Daten-Silos konsolidiert. Außerdem erhalten Sie einen einheitlichen Blick auf User Profiles, sodass Sie auf allen Kanälen eine konsistente Marken-Experience umsetzen können. Unternehmen erfahren außerdem mehr über ihre Kunden und deren Präferenzen, was Personalisierung ermöglicht. Die zunehmende Automatisierung gibt Entwicklern und IT-Teams zudem die Möglichkeit, sich auf Projekte zu konzentrieren, die das Unternehmen voranbringen.

Wenn Unternehmen ihre Tätigkeitsbereiche und ihren digitalen Fußabdruck erweitern, werden sie immer häufiger von raffinierten Cyberangriffen ins Visier genommen. Als Reaktion darauf sind verschiedene Sicherheitstools entstanden. Tools für Identity Threat Detection and Response (ITDR) und Identity Security Posture Management (ISPM) helfen dabei, bestehende Sicherheitslücken zu schließen und die Reaktion auf Bedrohungen zu verbessern. Wenn Sie diese Funktionen in Ihr Identity-System integrieren, können Sie Veränderungen bei Identity-bezogenen Risiken bewerten und automatisch darauf reagieren.

Die strategischen Schritte in dieser Phase sind:

Zusammenarbeit mit verschiedenen Teams, um die Strategie für Mitarbeiter- und Kundenidentitäten umzusetzen

Einführung formalisierter, kontinuierlicher Prozesse für die Bewertung der Identity-bezogenen Sicherheitslage

Messungen und Entscheidungen basierend auf Identity-basierten KPIs

Kategorie	Herausforderungen für das Identitäts-management	Was Sie tun sollten	Wie Ihr Business profitiert
Operative Flexibilität	• Ineffiziente Geschäftsprozesse, die technologische Entwicklungen ausbremsen, wobei manuelle Aktivitäten zu Verzögerungen führen und die Fehleranfälligkeit erhöhen • Unterstützung verschiedener Identity-Anwendungsfälle, ohne die Entwickler zu belasten	• Automatisierung der meisten Lifecycle Management-Prozesse, einschließlich Bereitstellung von Birthright-Zugriffsrechten und Klärung von Zugriffsanfragen, damit Entwickler und das IT-Team möglichst selten eingreifen müssen • Nutzung einiger Out-of-the-Box-Integrationen mit Business- und Marketing-Systemen • Automatisierung der Re-Zertifizierung von Mitarbeiterzugriffen bei Rollen- oder Job-Änderungen • Unterstützung einer Vielzahl von SDKs und APIs mit umfassendem Support und Dokumentation	Weniger Zeitaufwand in diesen Bereichen: • Entwicklung individueller Integrationen (IT- und Entwicklungsteams) • Manuelle Re-Zertifizierung von Kampagnen und Audits (IT- und GRC-Teams) • Prüfung von Zugriffen (Management und Anwendungsverantwortliche) Schnellere Einführung von Business-Lösungen und -Anwendungen
User Experiences	• Hohe Kundenerwartungen an reibungslose, konsistente und nahtlose User Experiences • Reibungspunkte für Mitarbeiterzugriffe: unflexible Zugriffsrichtlinien, die sich nicht an Benutzer oder Kontext anpassen, oder zeitaufwändige Prozesse für den Zugriff auf Anwendungen	• Gewährleistung von Resilienz durch redundante Server und Load Balancer • Automatisierte Verknüpfung/Zusammenführung von User Accounts • Progressive Profilerstellung, mit der Kundenattribute im Laufe der Zeit erfasst und die User Profiles nach und nach angereichert werden • Implementierung von Authentifizierung ohne Passwort für alle Touchpoints (Geräte, Anwendungen, Accounts) bzw. mithilfe von Passkeys, Hardware- oder Software-Authentifizierungslösungen • Verbesserung der Onboarding-Prozesse für Kunden mit Identity-Proofing und Account-Verifizierung • Unterstützung von Zugriffsanforderungen per Self-Service für die Belegschaft	• Nahtlose Customer Experiences auf allen Kanälen • Steigerung der Konversionsrate bei Anmeldung/Registrierung durch besseres Targeting bzw. stärkere Personalisierung • Höhere Mitarbeiterproduktivität durch mehr Automatisierung per Self-Service und schnellere Gewährung von Zugriff • Weniger Betrugsfälle dank erweiterter Account-Verifizierung
Sicherheit und Compliance	• Risiken durch Remote-Belegschaft und deren Geräte/Netzwerke • Ziel von zahlreicheren und raffinierteren Cyberbedrohungen	• Ausweitung von äußerst sicheren MFA-Funktionen für Mitarbeiter bei der Anmeldung am Computer • Gewährleistung von Phishing-resistenter MFA für Mitarbeiter bei allen Ressourcen • Einrichtung von attributbasierter Zugriffskontrolle (ABAC) • Integration mit ITDR- und ISPM-Tools • Implementierung von sicherem passwortlosem Zugriff auf kritische Infrastruktur wie Server, Kubernetes-Cluster, Datenbanken usw. • Bereitstellung von Identity Security Posture Management zur Erkennung von Risiken durch Konfigurationsfehler, Benutzer mit zu umfassenden Berechtigungen usw. • Einführung von kontinuierlicher Authentifizierung zur Unterstützung von Zero Trust und Zugriffs-entscheidungen basierend auf aktuellen Daten • Implementierung von automatisierten Sicherheits-reaktionen auf Identity-bezogene Risiken • Einführung wiederholter (geplanter) Re-Zertifizierungen von Benutzerzugriffen, um Least-Privilege-Prinzipien durchzusetzen • Integrationen mit Datenschutz- und Compliance-Tools, um Kundenpräferenzen überwachen zu können	• Geringere Angriffsfläche • Vereinfachte Governance und Compliance, da Zugriffsprüfungen und Zugriffsanfragen automatisiert werden • Stoppen von Phishing-Angriffen

Stufe 4: Strategisch

Erzielen Sie mit Identity einen strategischen Vorteil

In dieser Phase sind Unternehmen sich der Bedeutung von Identity für den Erfolg bewusst und betrachten sie als wichtigen Faktor für das Erreichen der geschäftlichen Ziele. Sie verfügen häufig über eine starke globale, digitale Präsenz und haben Teams, die kontinuierlich gemeinsam an Identity-Initiativen arbeiten, mit denen die Belegschaft gestärkt und auf mehreren Kanälen bessere Beziehungen mit ihren Kunden aufgebaut werden sollen.

In dieser Phase konzentrieren Unternehmen sich auf Folgendes:

- Optimierung der Identity-Infrastruktur, um die Effizienz zu steigern und operative Ziele zu erreichen
- Integration der Identity in die Sicherheitstechnologie, um Bedrohungen in Echtzeit zu erkennen und abzuwehren
- Nutzung von künstlicher Intelligenz (KI) und der Cloud, um herausragende User Experiences zu ermöglichen und die Identity-Sicherheit proaktiv zu verbessern

Wenn Identity vollständig in den Technologie-Stack integriert ist, können Unternehmen Daten aus der gesamten Infrastruktur erfassen, normalisieren und korrelieren. Dadurch wird Identity zur primären Kontrollebene für die Verwaltung des Zugriffs auf Ressourcen und ein wichtiges Element jeder Cybersicherheitsstrategie. Im Hinblick auf GRC ermöglicht die Identity-Integration einen besseren Überblick sowie detaillierte Kontrolle darüber, welche Benutzer und Geräte Zugriff auf bestimmte digitale Ressourcen haben und über welche Berechtigungen sie in ihrem Unternehmen verfügen. Außerdem lassen sich die Datenschutzeinstellungen der Kunden besser im Blick behalten. In Kombination mit weitflächiger Identity-Automatisierung und KI für Einblicke und Empfehlungen können Unternehmen sich einfacher und schneller an sich ändernde Kundenerwartungen, geschäftliche und gesetzliche Anforderungen sowie an die Bedrohungslandschaft anpassen.

Die strategischen Schritte in dieser Phase sind:

Nutzung ausgereifter Prozesse für Governance und operative Abläufe, mit denen sichergestellt ist, dass Identity sich kontinuierlich weiterentwickeln kann und Mehrwert bietet

Kategorie	Herausforderungen für das Identity-Management	Was Sie tun sollten	Wie Ihr Business profitiert
Operative Flexibilität	• Einheitliche Übersicht über die Identity für Cloud-, On-Premise- und Hybrid-Umgebungen • Anpassung an sich ändernde Marktanforderungen, Benutzererwartungen, Vorschriften usw.	• Zentralisierung aller Identity-Daten für alle Benutzer, Anwendungen und Berechtigungen • Vollständige Automatisierung der Richtlinien, des User Lifecycle Management, der Identity-bezogenen Abläufe und der Threat-Response-Workflows • Nutzung von KI-Empfehlungen zur Verbesserung von Identity-Sicherheit, Governance und User Experiences sowie zur Vereinfachung von Konfiguration und Entwicklung	• Kürzere Time-to-Market durch höhere Effizienz der IT-, Administratoren- und Entwicklungsteams
User Experiences	• Unterschiedliche User Experience auf unterschiedlichen Geräten und Kanälen • Verständnis des Kundenverhaltens zur Verbesserung von Targeting und Sicherheit	• Gewährleistung anpassbarer und erweiterbarer User Experiences für den Kundenzugriff auf allen Kanälen • Auslösen kontextbezogener Fragen bei Registrierung und Anmeldung, um Zero-Party-Daten von Kunden zu erhalten	• Erstellen nahtloser, konsistenter User Experiences auf allen Kanälen • Hyperpersonalisierung dank integrierter Zero-Party-Daten
Sicherheit und Compliance	• Veraltete Standing-Privilegien für verschiedene Anwendungen und die Infrastruktur • Cloud-bezogene und andere Identity-Konfigurationsfehler • Schnelle Reaktion auf Sicherheitsereignisse	• Gewährleisten, dass keine Standing-Privilegien verbleiben, Verwalten gemeinsam genutzter Anmeldedaten für privilegierte Ressourcen in sicheren Vaults • Vereinheitlichen der Identity-Sicherheit (IAM, PAM und IGA) • Erfassen von Bedrohungsdaten aus Drittanbieter-Sicherheitstools, um bessere Threat Insights zu erhalten • Bereitstellen risikobasierter, feingranularer Autorisierung • Automatisierung der Re-Zertifizierung von Mitarbeiterzugriffen basierend auf Risikoindikatoren • Gewährleisten, dass die Infrastruktur dynamisch mit Nachfragespitzen skalieren kann, und Nachweisen von Vorschriften-Compliance in den Bereichen Zuverlässigkeit und Sicherheit	• Proaktive Minimierung und Behebung von Identity-bezogenen Bedrohungen • Schnellere Erkennung und Reaktion auf Bedrohungen • Stärkeres Vertrauen, ohne dabei die Customer Experiences zu beeinträchtigen • Mehr Kundenvertrauen dank erweiterten Funktionen für Sicherheit und Betrugsschutz

Den geschäftlichen Mehrwert von Identity nutzen

Sobald Sie wissen, wo Ihr Unternehmen beim Identity-Reifegrad steht, können Sie die nächsten Schritte besser planen und die erzielten Erfolge im Blick behalten. Und wenn Sie verstehen, wie Identity innovative digitale Erlebnisse ermöglicht, vor Sicherheitsbedrohungen schützt und das geschäftliche Wachstum unterstützt, bleiben Sie Wettbewerbern jederzeit einen Schritt voraus.

Als führender unabhängiger Anbieter von Identity-Management-Lösungen arbeitet Okta mit Tausenden Unternehmen in verschiedensten Branchen weltweit zusammen und unterstützt sie dabei, ihre digitale Transformation voranzubringen und sichere Zugriffe, Authentifizierung und Automatisierung umzusetzen. Okta schafft für Ihr Unternehmen wertvolle Freiräume, damit Sie sich auf Ihre Kernkompetenz – Ihre Produkte und Services – konzentrieren können, während wir die Identity- und Sicherheitsumgebungen im Blick behalten und weiterentwickeln.

Ein Glossar der Identity-Begriffe finden Sie hier: https://www.okta.com/resources/identity-and-access-management-glossary/

Über Okta

Okta ist das weltweit führende Identity-Unternehmen. Als ein führender unabhängiger Identity-Anbieter ermöglichen wir es unseren Partnern und Kunden, jede Technologie sicher zu nutzen – überall, mit jedem Gerät und jeder Anwendung. Die weltweit renommiertesten Marken vertrauen beim Schutz von Zugriff, Authentifizierung und Automatisierung auf Okta. Im Mittelpunkt unserer Okta Workforce Identity Cloud sowie der Okta Customer Identity Cloud stehen Flexibilität und Neutralität. Mit unseren individualisierbaren Lösungen und unseren über 7.000 vorkonfigurierten Integrationen können sich Führungskräfte und Entwickler ganz auf neue Innovationen und eine rasche Digitalisierung konzentrieren. Wir entwickeln eine Welt, in denen Ihre Identity ganz Ihnen gehört. Mehr unter okta.com/de.