Das Identity-Reifegradmodell von Okta

Ihre Identity-Management-Roadmap zu stärkerer Sicherheit und Compliance durch Zero Trust, verbesserte User Experiences für Endbenutzer und mehr Flexibilität

Links

Stärkere Sicherheit und viele weitere Vorteile

In der Vergangenheit bezog sich Identity and Access Management (IAM) vor allem auf die Verwaltung von Benutzernamen und Passwörtern. Heute soll IAM gewährleisten, dass Unternehmen sicher mit Mitarbeitern, Kunden und Partnern interagieren können – an jedem Ort, zu jeder Zeit und auf beliebigen Geräten.

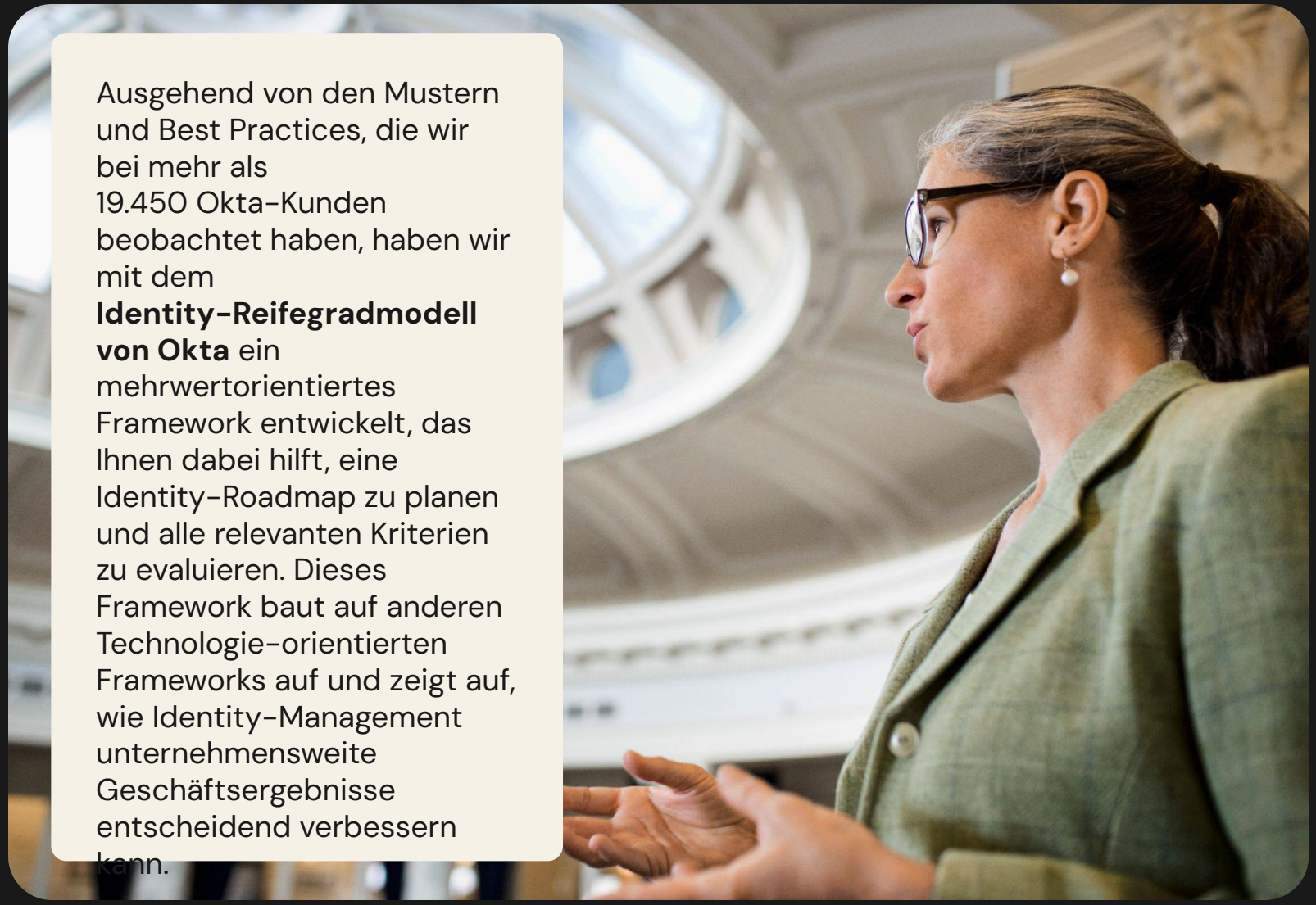
Starke Identity-Sicherheit bietet diese Vorteile:

- Die Sicherheit wird gestärkt und robuste Governance-, Risiko- und Compliance-Maßnahmen (GRC) lassen sich einfacher umsetzen.
- Prozesse laufen dank umfassender Automatisierung und weniger Fehlern schneller ab.
- Benutzer können zum richtigen Zeitpunkt einfacher auf benötigte Ressourcen zugreifen.

Da Identity-Management so viele Bereiche betrifft und so komplex ist, wissen Unternehmen mitunter nicht, wo sie anfangen und wie sie ihren aktuellen Stand bewerten sollen und wie eine Roadmap zum Erreichen der gesetzten Ziele aussehen könnte.

okta

Das Identity-Reifegradmodell von Okta



Ausgehend von den Mustern und Best Practices, die wir bei mehr als 19.450 Okta-Kunden beobachtet haben, haben wir mit dem **Identity-Reifegradmodell von Okta** ein mehrwertorientiertes Framework entwickelt, das Ihnen dabei hilft, eine Identity-Roadmap zu planen und alle relevanten Kriterien zu evaluieren. Dieses Framework baut auf anderen Technologie-orientierten Frameworks auf und zeigt auf, wie Identity-Management unternehmensweite Geschäftsergebnisse entscheidend verbessern kann.

Innerhalb des IMM werden Identity-Funktionen in vier aufeinander folgenden Reifegrad-Stufen eingeteilt.

Einfach
Grundlegende Identity-Anforderungen werden eingehalten und eine solide und zuverlässige Grundlage für ein ausgereiftes System geschaffen.

Eingeschränkt
Weitere Identity-Funktionen werden integriert, um neue Anwendungen, Services, Use Cases und Benutzer abzudecken.

Hochentwickelt
Die Automatisierung und Integration wird verstärkt, um Experiences, Flexibilität und Sicherheit zu verbessern.

Strategisch
Strategische Wettbewerbsvorteile werden durch Initiativen erzielt, die die Belegschaft unterstützen, die Effizienz optimieren sowie die Identity-gestützte Erkennung und Abwehr von Bedrohungen in Echtzeit ermöglichen.

In der Tabelle auf der nächsten Folie wird gezeigt, wie die Steigerung des Reifegrads relevante, messbare Vorteile in den wichtigen Bereichen Sicherheit und Compliance, operative Flexibilität und User Experiences für Endbenutzer bietet.

okta

Bereich	Beispiele für Ergebnisse	Stufe 1: Einfach	Stufe 2: Eingeschränkt	Stufe 3: Hochentwickelt	Stufe 4: Strategisch
		Unternehmen fällt es oft schwer, Anwendungen und Benutzer zu unterstützen und gleichzeitig Identity-basierte Angriffe zu verhindern. Um den Reifegrad zu steigern, müssen sie ihre Identity-Infrastruktur konsolidieren und vereinfachen.	Wenn grundlegende Identity-Funktionen implementiert wurden, verschiebt sich der Fokus auf Verbesserungen, die zugrundeliegende Abläufe im großen Maßstab optimieren. Dazu sind mehrschichtige Schutzebenen und erweiterte Automatisierung erforderlich.	Unternehmen haben verschiedene Identity-Systeme aufgebaut und konzentrieren sich nun auf die Erweiterung hochwirksamer, leicht umsetzbarer Kontroll-maßnahmen mithilfe von Automatisierung oder stärkeren Sicherheitsrichtlinien.	In dieser finalen, kontinuierlichen Stufe geht es vor allem um die Erweiterung der Kontrollen und der Automatisierung auf möglichst viele Unternehmensbereiche sowie um Verbesserungen und Optimierungen.
Sicherheit und Compliance	• Proaktive Minimierung und Behebung von Identity-bezogenen Bedrohungen • Erzielung und Beibehaltung kritischer Compliance-Zertifizierungen • Optimierung und Absicherung des Endbenutzer-Zugriffs nach dem Least-Privilege-Prinzip	Der Schutz vor Identity-basierten Angriffen wird verbessert, indem grundlegende Funktionen für Single Sign-On (SSO) und Multi-Faktor-Authentifizierung (MFA) implementiert werden, die Richtlinien für rollenbasierte Zugriffskontrollen (Role Based Access Control, RBAC) nutzen.	Es werden dynamische Zugriffsrichtlinien definiert, um eine grundlegende Zero-Trust-Architektur einzurichten.	Risikobasierte und Phishing-resistente Authentifizierung und Autorisierung werden implementiert.	Intelligente, kontextbezogene sowie kontinuierliche Authentifizierung und Autorisierung werden verwendet, um mit modernen Angriffen Schritt zu halten.
Operative Flexibilität	• Steigerung der operativen Effizienz und Senkung der laufenden Kosten • Steigerung der Effizienz von Mitarbeitern • Vereinfachung der Integration nach Mergern und Akquisitionen	Die manuelle Verwaltung von Benutzern und Anwendungen wird nach und nach automatisiert.	Die Lebenszyklusverwaltung und Provisionierung von Benutzern wird automatisiert.	Hochentwickelte Funktionen zur Lebenszyklusverwaltung werden verwendet, wobei übliche Aufgaben wie Zugriffs-Anfragen/-Genehmigungen und App-Provisionierung automatisiert erfolgen.	Abläufe für Richtlinien, Benutzer-Lebenszyklusverwaltung sowie Identity-bezogene IT- und Sicherheitsabläufe für Cloud-Anwendungen und -Services erfolgen vollständig automatisiert.
User Experiences für Endbenutzer	• Bessere digitale Experiences für Endbenutzer • Steigerung der Konversionsrate bei Registrierung/Anmeldung	Es wird ein Inventar aller Anwendungen definiert. Außerdem werden sichere Login-Prozesse festgelegt, die grundlegende Schutzfunktionen wie MFA, Bot-Erkennung sowie starke Passwortrichtlinien verwenden.	SSO und MFA werden für alle Benutzertypen erweitert. Anfängliche passwortlose Optionen wie FastPass und Passkeys werden eingeführt. Self-Service-Zugriff für typische Einsatzbereiche wird standardisiert.	Passwortlose Zugriffe werden für Geräte und Kanäle erweitert. Nahtlose Self-Service-Optionen werden unterstützt. Zur Personalisierung des Zugriffs in Echtzeit werden Identity-Indikatoren verwendet.	Auf allen Touchpoints wird vollständig passwortloser Zugriff bereitgestellt. Dabei werden erweiterte Funktionen wie verifizierbare Anmeldedaten, adaptive Richtlinien und Session-Kontrollen in Echtzeit verwendet.

Hinweis: Diese Tabelle ist nicht dazu gedacht, die volle Bandbreite des Identity-Managements wiederzugeben.
Sie berücksichtigt nicht alle Eigenschaften und Verhaltensweisen, die in jeder Stufe bzw. bei den jeweiligen Geschäftsergebnissen relevant sein können.

okta

Über dieses Dokument

Wir haben das Identity-Reifegradmodell von Okta erstellt, um Unternehmen einen praktischen Mehrwert- und Ergebnis-orientierten Ratgeber für den Aufbau und zur Verbesserung der eigenen Identity-Strategie bereitzustellen.

Dieser Ansatz unterscheidet sich stark von technologiebasierten Frameworks und Reifegrad-Checklisten, die tendenziell Funktionen beschreiben und Technologien vorschreiben, ohne Mehrwert und Ergebnisse detailliert zu untersuchen.

Das Reifegradmodell unterscheidet sich auch dadurch von anderen Ressourcen, dass es nicht nur Sicherheit (und Compliance) berücksichtigt.

Der Leitfaden erkennt an, dass Sicherheit häufig der Anlass für die Implementierung von Identity-Projekten ist, bewertet den Identity-Reifegrad jedoch anhand der bekannten vier Identity-Funktionen und drei bereichsübergreifenden Funktionen, die beim bekannten CISA Zero Trust Maturity Model (ZTMM) verwendet werden:

Authentifizierung	Identity Stores	Risikobewertungen	Zugriffsmanagement
Transparenz und Analysen	Automatisierung und Orchestrierung	Governance	

Sie erhalten außerdem folgende Informationen:

- Einblicke und Kontext zu Beispielen aus der Praxis
- Vergleiche und Abgrenzungen zu ZTMM
- Empfehlungen zu Okta-Lösungen, mit denen Ihr Unternehmen die Identity-Reifegrad-Ziele erreichen kann

Identity-Reifegrad und Zero Trust

Die „digitale Identität“ (Identity) ist die erste von fünf Säulen im Zero Trust Maturity Model (ZTMM), das von der Cybersecurity and Infrastructure Security Agency (CISA) entwickelt wurde.

Im CISA ZTMM wird US-Behörden in Bezug auf die digitale Identität Folgendes empfohlen:

- Behörden sollen gewährleisten und durchsetzen, dass Benutzer und Entitäten zum richtigen Zeitpunkt für den richtigen Zweck auf die richtigen Ressourcen zugreifen können, ohne übermäßige Zugriffsrechte einzuräumen.
- Behörden sollen Lösungen zur Verwaltung von Identities, Anmeldedaten und Zugriffsrechten in der gesamten Umgebung integrieren (sofern möglich), um starke Authentifizierung durchzusetzen, maßgeschneiderte kontextbasierte Autorisierung sicherzustellen und Identity-Risiken für Behördenmitarbeiter und Entitäten zu bewerten.
- Behörden sollen ihre Identity Stores und Verwaltungssysteme integrieren (sofern möglich), um den Überblick über die verwendeten Identities und deren Aufgaben und Befugnisse zu verbessern.

Auch wenn das technologiebasierte ZTMM für US-Behörden entwickelt wurde, wird es von zahlreichen Unternehmen aus dem öffentlichen Sektor eingesetzt. Das CISA-Modell ergänzt das Architekturkonzept von NIST Zero Trust Architecture (SP 800-207), in dem Grundsätze wie kontinuierliche Verifizierung und das Least-Privilege-Prinzip erläutert werden. Das Modell ist jedoch eher deskriptiv als präskriptiv, sodass uns viele Okta-Kunden fragen, wie sie ihre Identity-Umgebung entsprechend dem CISA ZTMM optimieren können.

Deshalb verweisen wir in diesem Leitfaden auf konkrete Aspekte im CISA ZTMM, um zu verdeutlichen, wie das Okta IMM und das CISA-Modell aufeinander abgestimmt sind.

Erfahren Sie mehr darüber, wie das Identity-Reifegradmodell von Okta den Zero-Trust-Ansatz für regulierte Branchen unterstützt.

okta

Authentifizierung

Authentifizierung bestätigt die Identität eines Benutzers oder einer Entität, der bzw. die auf eine Anwendung, einen Service oder eine andere Ressource zuzugreifen versucht. Damit wird sichergestellt, dass es sich tatsächlich um die Person oder Entität handelt, für die er oder sie sich ausgibt.

Zur Umgehung der Authentifizierung setzen Angreifer häufig auf diese (und andere) Methoden:

- Brute-Force-Angriffe, bei denen unzählige Kombinationen von Anmeldedaten ausprobiert werden
- Social Engineering, um Benutzer zur Weitergabe von Anmeldedaten zu verleiten
- Infostealer-Malware, die Anmeldedaten, Cookies und Token stiehlt
- SIM-Swapping (SIM-Kartentausch) und AitM-Angriffe (Adversary-in-the-Middle), um anfällige MFA-Formen zu umgehen

Authentifizierung ist für die Gewährleistung der Sicherheit ganz klar unverzichtbar, doch sie hat auch Einfluss auf die User Experience und Produktivität der Benutzer – mit potenziell erheblichen Folgen.

So hat zum Beispiel der Auth0 Customer Identity Trends Report 2025 gezeigt, dass fast ein Viertel der Benutzer Online-Käufe bei Problemen mit dem Registrierungs- oder Login-Prozess immer (6 %), häufig (17 %) oder manchmal (40 %) abbricht. Bei Mitarbeitern führen Zugriffsprobleme auf Anwendungen oder Informationen dazu, dass sie ihre Arbeit nicht erledigen können.

Wenn der Bereich Authentifizierung ausgereift ist, kombiniert er starke, Phishing-resistente Sicherheit (die auch Risikoindikatoren berücksichtigt) mit Bedienfreundlichkeit. Sie stellt sicher, dass Angreifer nur mit größter Mühe und hohem finanziellem Aufwand Zugriff erlangen können, und bietet legitimen Benutzern dennoch komfortablen Zugriff.

Bei ausgereifter Authentifizierung wird das Risiko zudem nicht nur einmal (z. B. beim Login), sondern kontinuierlich bewertet, um vor Session Hijacking und anderen Bedrohungen nach dem Login zu schützen.

Autorisierung

Authentifizierung verifiziert die Identität einer Entität, während Autorisierung je nach Systemeinstellungen entscheidet, auf welche Informationen die Entität anschließend zugreifen kann.

CISA ZTMM geht im Zusammenhang mit anderen Funktionen auf Autorisierung ein (z. B. im Abschnitt zu Authentifizierung, hier wird auf „Zugriffsrechte“ verwiesen). Wir haben uns jedoch entschieden, hier auf Autorisierung einzugehen.

Bei einer nicht ausgereiften Identity-Implementierung sind diese Rechte nicht detailliert definiert und werden von statischen Faktoren wie dem Anmeldezeitpunkt bestimmt.

Eine ausgereifte Identity-Implementierung:

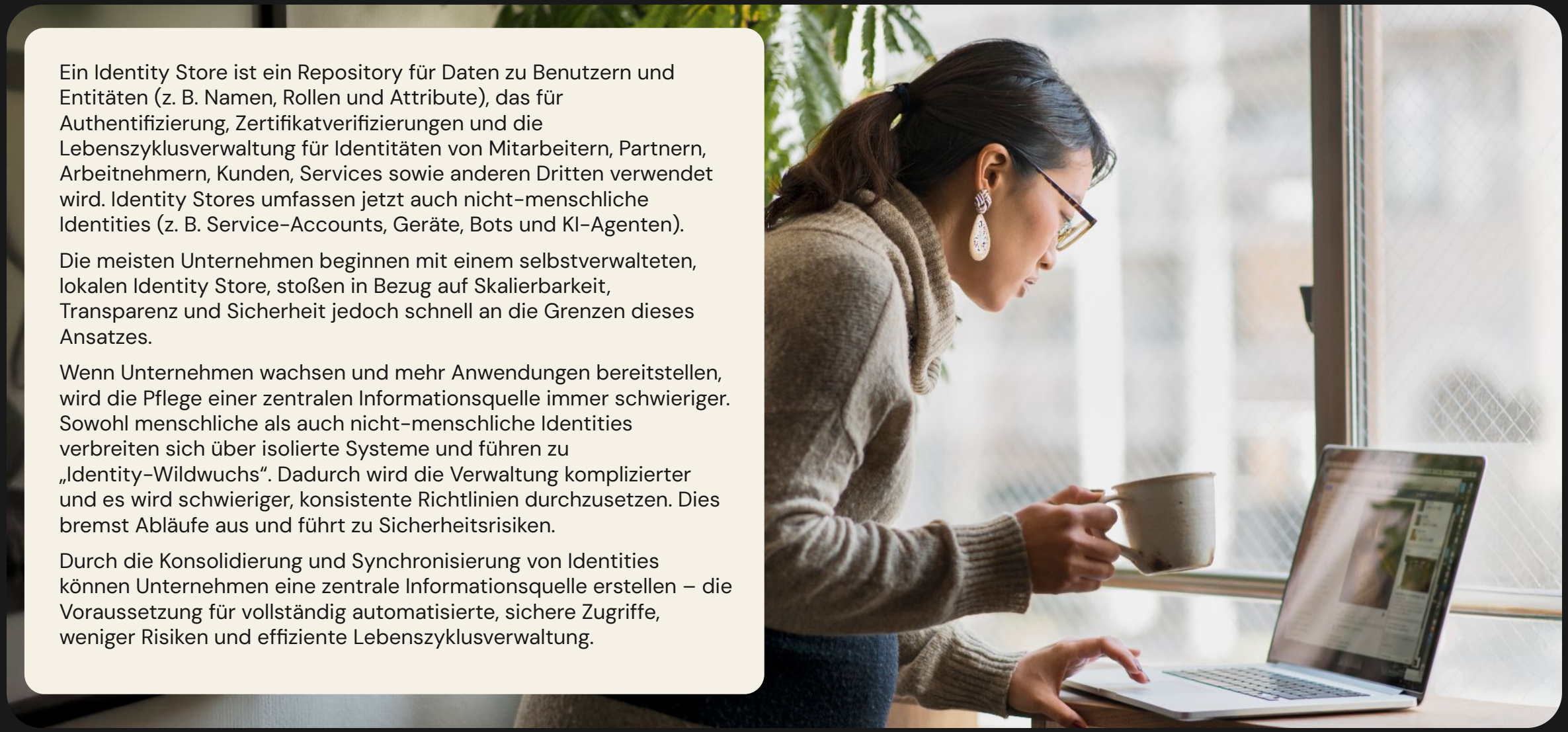
- verwendet dynamische Attribute,
- nutzt kontextbezogene Evaluierungen (z. B. Standort, Gerätestatus) und
- weist Zugriffsrechte feingranular zu.

okta

Stufe	Beschreibung	Relevante Okta-Lösungen
 **Einfach**	In dieser hochriskanten Stufe werden zur Authentifizierung primär Benutzername-Passwort-Paare verwendet. MFA wird zwar teilweise eingesetzt, allerdings nicht für die gesamte Belegschaft vorgeschrieben und kann Techniken involvieren, die für Phishing anfällig sind (z. B. SMS, E-Mail). Zudem ist Autorisierung vorab definiert sowie festgeschrieben und berücksichtigt keine kontextbezogenen Bedingungen (z. B. Zeitpunkt).	• Multi-Factor Authentication • Adaptive Multi-Factor Authentication • Single Sign-On • Universal Directory
 **Eingeschränkt**	Unternehmen setzen MFA für alle Entitäten durch, wobei die Sicherheit mit Besitz- und Inhärenzfaktoren gestärkt wird, die potenziell Phishing-resistent sind. In Kombination mit Single Sign-On (SSO) ist Authentifizierung jetzt sicherer und komfortabler. Vereinfachte und zentrale User Stores ermöglichen eine effizientere und effektivere Autorisierungsverwaltung. Rollenbasierte oder attributbasierte Zugriffskontrollen (RBAC oder ABAC) sind implementiert und verwenden dynamische Faktoren, mit deren Hilfe sich Risiken (z. B. Standort der Entität, lokale Uhrzeit und Gerätetyp) bewerten lassen.	• Adaptive Multi-Factor Authentication • Single Sign-On • Universal Directory • Fine-Grained Authorization
 **Hochentwickelt**	Unternehmen beginnen damit, Passwörter, Einmal-Passwörter/Passcodes (OTPs), Sicherheitsfragen und Push-Benachrichtigungen auslaufen zu lassen. Phishing-resistente MFA wird für das gesamte Unternehmen eingeführt und nutzt passwortlose MFA per FIDO2 oder (sofern anwendbar) sichere behördliche Anmeldedaten wie PIV-Karten (Personal Identity Verification). Beziehungsbasierte Zugriffskontrolle (ReBAC) ermöglicht präzise und dynamische Autorisierung. Zugriffsmanagement und MFA berücksichtigen, wie sich Benutzer über Computer anmelden. Authentifizierungsabläufe sind zur sicheren und passwortlosen Aktivierung durch vertrauenswürdige Systeme (z. B. Callcenter, Selbstbedienungskioske oder KI-gestützte Agenten) entkoppelt, sodass keine Sicherheitsfragen, OPTs oder PINs mehr erforderlich sind.	• Adaptive Multi-Factor Authentication • Single Sign-On • Universal Directory • Identity Threat Protection • Okta FastPass • Fine-Grained Authorization • Okta Device Access • Client-Initiated Backchannel Authentication (CIBA)
 **Strategisch**	Alle Identities werden mit Phishing-resistenter und passwortloser Authentifizierung validiert. Zugriffskontrollen decken Geräte-Logins bis hin zu Anwendungsanmeldungen ab, um integrierte Sicherheit zu unterstützen. Gleichzeitig wird die User Experience vereinfacht. Zugriffsrechte werden jetzt kontinuierlich mithilfe dynamischer Variablen evaluiert, um Bedrohungen nach der Authentifizierung zu erkennen. Sensible Kundenaktivitäten (z. B. hochriskante Transaktionen oder Profiländerungen) werden authentifiziert und über Echtzeit-Bestätigungsmechnismen geschützt, die zusätzliche Sicherheit bieten, ohne die Abläufe zu stören. Im Hintergrund werden Kundenkommunikationskanäle sowie Datenweitergaben mit Financial Grade Identity-Standards geschützt, um während der gesamten Customer Journey Manipulationen oder MitM-Zugriffe zu verhindern.	• Adaptive Multi-Factor Authentication • Single Sign-On • Universal Directory • Identity Threat Protection • Okta FastPass • Fine-Grained Authorization • Okta Device Access • Strong Customer Authentication • Financial-Grade APIs (FAPI)

okta

Identity Stores



Ein Identity Store ist ein Repository für Daten zu Benutzern und Entitäten (z. B. Namen, Rollen und Attribute), das für Authentifizierung, Zertifikatverifizierungen und die Lebenszyklusverwaltung für Identitäten von Mitarbeitern, Partnern, Arbeitnehmern, Kunden, Services sowie anderen Dritten verwendet wird. Identity Stores umfassen jetzt auch nicht-menschliche Identities (z. B. Service-Accounts, Geräte, Bots und KI-Agenten).

Die meisten Unternehmen beginnen mit einem selbstverwalteten, lokalen Identity Store, stoßen in Bezug auf Skalierbarkeit, Transparenz und Sicherheit jedoch schnell an die Grenzen dieses Ansatzes.

Wenn Unternehmen wachsen und mehr Anwendungen bereitstellen, wird die Pflege einer zentralen Informationsquelle immer schwieriger. Sowohl menschliche als auch nicht-menschliche Identities verbreiten sich über isolierte Systeme und führen zu „Identity-Wildwuchs“. Dadurch wird die Verwaltung komplizierter und es wird schwieriger, konsistente Richtlinien durchzusetzen. Dies bremst Abläufe aus und führt zu Sicherheitsrisiken.

Durch die Konsolidierung und Synchronisierung von Identities können Unternehmen eine zentrale Informationsquelle erstellen – die Voraussetzung für vollständig automatisierte, sichere Zugriffe, weniger Risiken und effiziente Lebenszyklusverwaltung.

okta

Stufe	Beschreibung	Relevante Okta-Lösungen
 **Einfach**	Unternehmen verwenden selbstverwaltete (z. B. selbst geplante, bereitgestellte und gepflegte) Identity Stores wie Active Directory oder LDAP. Diese konzentrieren sich meist auf menschliche Benutzer, sodass nicht-menschliche Identities wie Service-Accounts häufig nicht verwaltet oder informell nachverfolgt werden.	• Single Sign-On • Universal Directory
 **Eingeschränkt**	Unternehmen beginnen, ihre selbstverwalteten und in der Cloud gehosteten Identity Stores zu vereinheitlichen, um den Identity-Wildwuchs und die verbundenen Risiken zu reduzieren. Gleichzeitig wenden sie Governance-Kontrollen auf menschliche und nicht-menschliche Identities an, die per Automatisierung und Infrastructure-as-Code erstellt wurden. Unternehmen synchronisieren zudem ihre Directories, standardisieren Prozesse zur Lebenszyklusverwaltung und beginnen mit der formellen Nachverfolgung von nicht-menschlichen Identities. Diese Schritte legen die Grundlage für die Reduzierung von Duplikaten. Gleichzeitig werden die Transparenz verbessert und automatisierte Workflows im großen Maßstab eingerichtet.	• Single Sign-On • Universal Directory • Lifecycle Management • Workflows
 **Hochentwickelt**	Identity Stores werden konsolidiert und Governance-Richtlinien werden auf alle menschlichen und nicht-menschlichen Identities angewendet. Dadurch wird der Identity-Wildwuchs reduziert und Identity-Abläufe (z. B. SSO) sowie Verwaltung (z. B. Provisionierung, LCM) werden sicherer und effizienter. Service-Accounts, APIs und Bots werden zur Verwaltung hinzugefügt und formeller nachverfolgt. Die Transparenz wird verbessert und Identity-Lebenszyklusereignisse werden zentraler verwaltet.	• Universal Directory • Single Sign-On • Lifecycle Management • Workflows • Okta Identity Governance • Okta Privileged Access
 **Strategisch**	Identity Stores werden für alle Umgebungen vereinheitlicht, sodass die Zahl der verwendeten Identity Stores minimiert wird und Store-übergreifende automatisierte Lebenszyklusverwaltung möglich wird. Nicht-menschliche Identities (jetzt einschließlich neuer KI-Agenten) werden parallel mit menschlichen Benutzern kontrolliert. Unternehmen führen adaptive Richtlinien, automatisierte Lebenszyklusverwaltung und Posture Management für einen einheitlichen Identity Security Fabric ein.	• Universal Directory • Single Sign-On • Lifecycle Management • Workflows • Okta Identity Governance • Okta Privileged Access • Identity Security Posture Management

Risikobewertungen

Okta definiert ein Identity-Risiko sehr allgemein als *„jede Schwachstelle in den IAM-Prozessen (Identity and Access Management) eines Unternehmens“*.

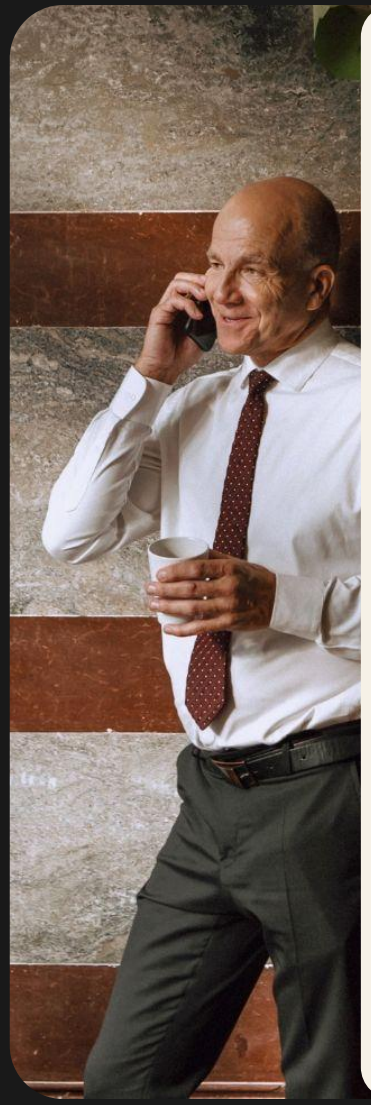
Diese breit gefasste Definition deckt sowohl Risiken individueller Identities als auch Risiken durch folgende Probleme ab:

- Schwache IAM-Hygiene (z. B. verwaiste Accounts, Überprovisionierung)
- Konfigurationsfehler, die zu Sicherheitslücken führen
- Verwendung veralteter Technologien

Für den Wechsel in die Stufe „Strategisch“ müssen Unternehmen sich auf Funktionen konzentrieren, die ihre Gesamtsicherheit stärken und Identity-Risiken dynamisch reduzieren. Dazu müssen sie Sicherheitsindikatoren aus ihrer Umgebung erfassen und analysieren, z. B. zur Sicherheit von Identities, Endpoints, Netzwerken und Geräten.

Diese Echtzeitindikatoren können als Grundlage für adaptive Richtlinien dienen und bieten folgende Vorteile, die die Identity-bezogene Angriffsfläche reduzieren und die Sicherheit stärken:

- **Erkennung:** Identifizierung verborgener Bedrohungen und Konfigurationsfehler bei Identity-Anbietern, SaaS und Cloud-Infrastrukturen (IaaS)
- **Priorisierung:** Erkennung und Priorisierung von Schwachstellen wie MFA-Umgehung, Benutzern mit zu umfangreichen Zugriffsrechten und fehlerhaftem Offboarding
- **Behebung:** Gewinnung entscheidungsrelevanter Sicherheitseinblicke, die eine schnelle Behebung ermöglichen
- **Kontinuierliche Überwachung:** Durchführung kontinuierlicher Analysen zur Identity-Sicherheit des Unternehmens mit schnellen Maßnahmen und risikobasierte Überwachung der Einhaltung von Sicherheits-, IAM- und Compliance-Standards (z. B. NIST, CIS, ISO, SOX und PCI DSS)



Identity-Risiko

Das CISA ZTMM *beschränkt die Definition von „Identity-Risiko“ auf die „Wahrscheinlichkeit*, dass eine Identity kompromittiert wurde“ und ist damit enger gefasst als bei Okta.[1]

Daher konzentriert sich das Modell darauf, Unternehmen bei der schnellen und zuverlässigen Erkennung kompromittierter Identities zu unterstützen. Es erkennt zum Beispiel ungewöhnliches Verhalten (z. B. Service-Accounts, die auf sensible Ressourcen zugreifen, mit denen sie zuvor noch nie interagiert haben) und kennzeichnet es zur genaueren Untersuchung.

CISA ZTMM stellt keine direkte Verbindung zwischen den Bereichen Risikobewertung und Authentifizierung her. Diese Bereiche sind jedoch eng miteinander verknüpft – und Okta hilft beim Schließen dieser Lücke. Beispiele:

- Wenn ein Prozess mit hoher Wahrscheinlichkeit feststellt, dass eine Identity kompromittiert wurde, kann dieser Entität die Authentifizierung verweigert werden.
- Wenn das Verhalten einer Entität während der Authentifizierung verdächtig ist, kann diese Beobachtung bei der Risikobewertung berücksichtigt werden.

Okta weitet diese Beziehung aus, indem das Risiko während des gesamten Identity-Lebenszyklus (nicht nur beim Login) kontinuierlich bewertet wird. Dazu werden Echtzeitsignale zum Verhalten und Kontext von anderen Bedrohungsbereichen überwacht. Dies ermöglicht schnelle Reaktionen (z. B. richtlinienbasierte Beendigung/Abmeldung von Sessions oder adaptive Step-up-Authentifizierung) und die rechtzeitige Eindämmung von Bedrohungen.

[1] CISA: Zero Trust Maturity Model, Version 2.0, April 2023, S. 14, abgerufen am 9. Juni 2025, https://www.cisa.gov/sites/default/files/2023-04/zero_trust_maturity_model_v2_508.pdf.

okta

Diese Bereiche überschneiden sich mit dem im CISA ZTMM beschriebenen Bereich Zugriffsmanagement und den drei bereichsübergreifenden Bereichen (Transparenz und Analysen, Automatisierung und Orchestrierung sowie Governance).

Stufe	Beschreibung	Relevante Okta-Lösungen
 **Einfach**	In dieser Stufe verfügen Unternehmen nur über sehr begrenzte Möglichkeiten zur Bewertung und Einbeziehung von Identity-Risiken in ihren Zugriffsrichtlinien. Alle vorhandenen Bewertungen basieren wahrscheinlich auf statischen Attributen und die entsprechenden Richtlinien sind sehr einfach (z. B. binär).	• Multi-Factor Authentication • Adaptive Multi-Factor Authentication
 **Eingeschränkt**	Richtlinien sind etwas komplexer und Bewertungen berücksichtigen Authentifizierungstelemetrie beim Login. Die Bewertungen sind jedoch relativ einfach und für Identity-basierte Angriffe anfällig, da sie weiterhin auf manuellen Methoden und statischen Regeln basieren.	• Adaptive Multi-Factor Authentication
 **Hochentwickelt**	Bewertungen nutzen Automatisierung sowie dynamische Regeln und treffen Zugriffsentscheidungen basierend auf zahlreichen Authentifizierungsindikatoren (z. B. von Device Assurance- und Management-Lösungen). Die Bewertungen erfolgen jedoch weiterhin vor allem beim Login und werden während einer Benutzer-Session nicht wiederholt.	• Adaptive Multi-Factor Authentication • Identity Threat Protection • Identity Security Posture Management
 **Strategisch**	Risikobewertungen werden kontinuierlich und in Echtzeit durchgeführt und nutzen dynamischen Kontext sowie eine Vielzahl von Signalen aus der Identity-Infrastruktur und von unterstützenden Sicherheits- und IT-Systemen. Automatisierung und Integration ermöglichen zudem die Durchsetzung geeigneter Richtlinien bzw. angemessene Reaktionen, z. B. die sofortige Abmeldung und Aktivierung von Sicherheits- oder IT-Workflows zum Schutz des Unternehmens und der kompromittierten Benutzer.	• Adaptive Multi-Factor Authentication • Identity Threat Protection • Identity Security Posture Management • Workflows

Zugriffsmanagement

Da sich das CISA ZTMM im Bereich Zugriffsmanagement auf Identity Governance and Administration (IGA) konzentriert, beschreiben die vier Stufen die Implementierung und den Prozessreifegrad statt technischer Lösungen. Nichtsdestotrotz benötigen Unternehmen zur Implementierung von IGA-Richtlinien entsprechende Funktionen.

Allgemein ausgedrückt, nutzen Unternehmen mit geringem Reifegrad manuelle Zugriffsprüfungsprozesse, sehr langlebige Zugriffsrechte sowie wenig differenzierte Autorisierungen. Diese Kombination führt häufig zu erheblich überprovisionierten Zugriffen sowie gefährlichen Kombinationen (z. B. kann ein einzelner Benutzer eine Berechtigungsausweitung anfordern UND genehmigen), was eine Vielzahl von Missbrauchsmöglichkeiten schafft. Gleichzeitig lässt sich ein solches System nicht skalieren.

Im Gegensatz dazu nutzen Unternehmen mit hohem Reifegrad sämtliche Automatisierungsmöglichkeiten und wenden das Least-Privilege-Prinzip an, wobei äußerst präzise Zero-Standing-Privilegien gewährt werden.

Identity Governance and Administration

Der Bereich Zugriffsmanagement innerhalb des CISA ZTMM bezieht sich auf das, was als Identity Governance and Administration bezeichnet wird, d. h. auf einen richtlinienbasierten Ansatz für Identity-Management und Zugriffskontrollen, der Folgendes kombiniert:

- **Identity Governance:** Prozesse und Richtlinien für die Trennung von Aufgabenbereichen, das Management unterschiedlicher Rollen sowie für Protokollierung, Zugriffsprüfungen, Analysen und Reporting
- **Identity Administration:** Umfasst die Verwaltung von Accounts und Anmeldedaten, die Provisionierung und Deprovisionierung von Benutzern und Geräten, das Management von Zugriffsrechten sowie weitere Maßnahmen

okta

Stufe	Beschreibung	Relevante Okta-Lösungen
 **Einfach**	In dieser Stufe autorisieren kleinere Unternehmen den Zugriff für privilegierte und standardmäßige Accounts häufig permanent und überprüfen ihn nur gelegentlich. Zugriffskontrollen sind nicht kontextbezogen, die Durchsetzung ist begrenzt und der Zugriff wird wahrscheinlich manuell überwacht (z. B. in einer Tabelle).	• Okta Identity Governance • Identity Security Posture Management
 **Eingeschränkt**	Der Zugriff für privilegierte und standardmäßige Accounts wird mithilfe automatisierter Überprüfungen nachverfolgt. Der wichtigste Unterschied besteht in dieser Stufe darin, dass die Zugriffsrechte mit der automatisierten Überprüfung ablaufen, sofern sie nicht anderweitig verlängert werden. Die für Zugriffsentscheidungen verfügbaren Informationen sind jedoch begrenzt und basieren eher auf der Rolle als auf dem Bedarf oder früheren Zugriffsprotokollen, was zu langlebigen und übermäßig privilegierten Zugriffsrechten führt. Aufgrund begrenzter Granularität der Zugriffskontrollen können Entitäten zu viele Zugriffsrechte erhalten.	• Okta Identity Governance • Identity Security Posture Management • Okta Privileged Access • Fine-Grained Authorization
 **Hochentwickelt**	Zugriffsrechte werden nach Bedarf und pro Session verwaltet, für konkrete Aktionen und Ressourcen maßgeschneidert und automatisch widerrufen. Dabei wird das Least-Privilege-Prinzip mit zeitgebundenen, passwortlosen Just-in-Time-Zugriffen angewendet. Das gilt besonders für kritische Infrastruktur wie Server. Auch die Verwaltung der Zugriffe für Geräte-Logins erfolgt risikobasiert und richtliniengestützt. Bei der Durchsetzung werden granulare Bedingungen wie Risikoindikatoren zu Gerätestatus, Netzwerk und Verhalten berücksichtigt.	• Okta Identity Governance • Identity Security Posture Management • Okta Privileged Access • Fine-Grained Authorization • Workflows • Okta Device Access
 **Strategisch**	Die Durchsetzung des Least-Privilege-Prinzips und der Just-in-Time-Zugriffsrichtlinien erfolgt jetzt automatisiert. Dabei werden die Zugriffsrechte für einzelne Aktionen und Ressourcen maßgeschneidert, sodass keine Standing-Privilegien entstehen. Die Zugriffsdurchsetzung ist vollständig adaptiv und reagiert auf Echtzeitsignale aus dem gesamten Tech-Stack. Authentifizierungs- und Session-Entscheidungen basieren auf kontinuierlichen Evaluierungen. Risikobasierte Step-up-Authentifizierung und andere Aktionen erfolgen automatisiert und in Echtzeit, wodurch die User Experience verbessert und gleichzeitig die Gesamtsicherheit gestärkt wird.	• Okta Identity Governance • Identity Security Posture Management • Okta Privileged Access • Fine-Grained Authorization • Workflows • Okta Device Access

Transparenz und Analysen

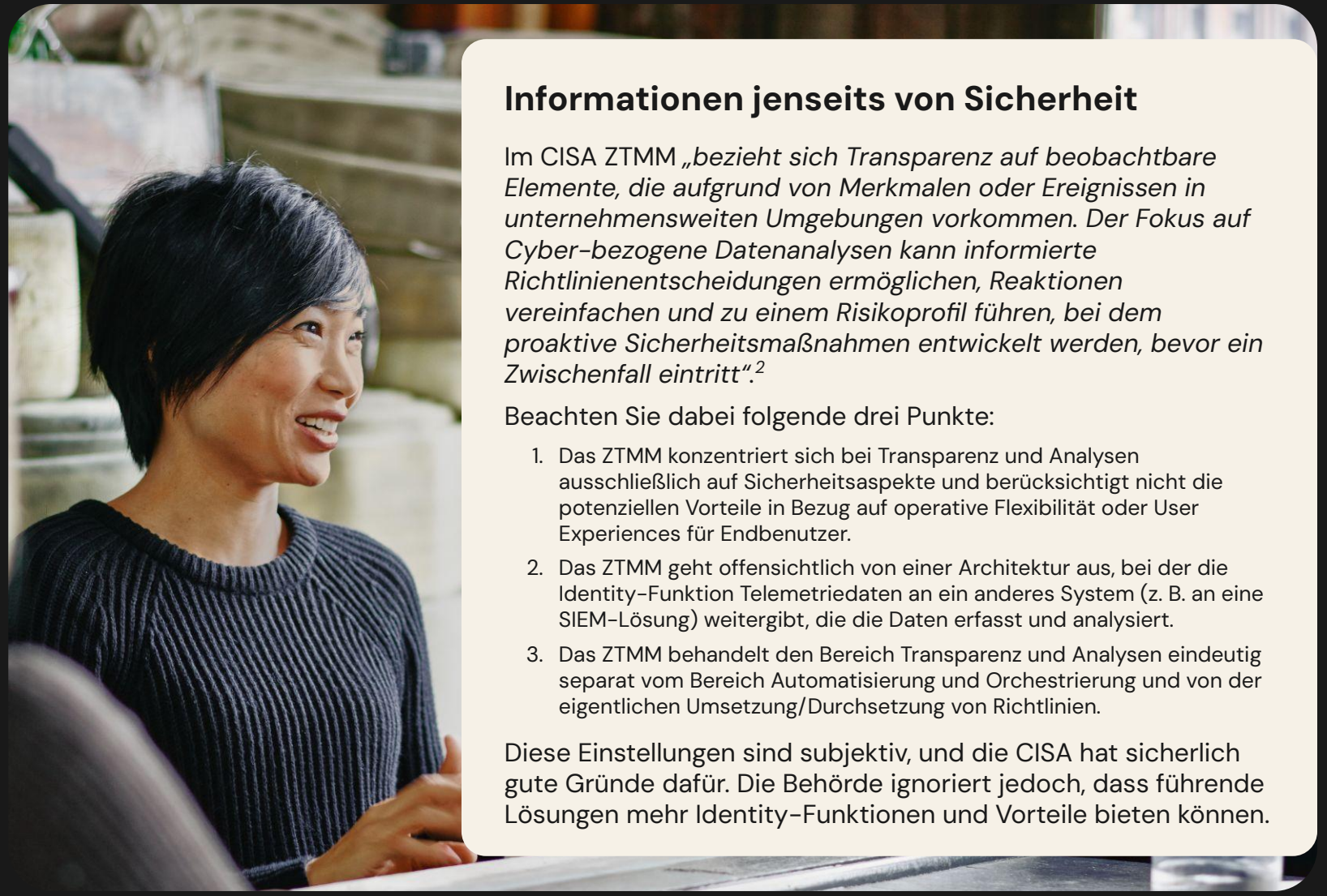
Je besser Unternehmen verstehen, wie Entitäten Identity-Systeme verwenden, desto eher können sie Folgendes erreichen:

- Verbesserte operative Flexibilität (z. B. durch automatisierte Workflows)
- Optimierte User Experiences (z. B. durch verbesserte Zugriffsmanagement-Richtlinien)
- Stärkere Sicherheit (z. B. durch die Implementierung von Funktionen für Prävention, Erkennung und Reaktion)

Einige Identity-Lösungen können Risiken in Echtzeit erkennen – häufig sogar schneller und zuverlässiger als generische Sicherheitstools – und müssen dazu noch nicht einmal Daten an ein SIEM-System senden. Wichtig dabei: Lokale Analysen können externe Systeme ergänzen.

Bestimmte Identity-Lösungen können Richtlinien als Reaktion auf Bedrohungen direkt durchsetzen und zum Beispiel die Authentifizierung verhindern oder kompromittierte Benutzer abmelden. Wenn dieselbe Lösung Echtzeiterkennung bietet, können Unternehmen Bedrohungen schnell beheben und ihre Gesamtsicherheit stärken.

Die erzielbaren Ergebnisse hängen jedoch von der Identity-Plattform und ihren Telemetrie-Funktionen ab.



Informationen jenseits von Sicherheit

Im CISA ZTMM *„bezieht sich Transparenz auf beobachtbare Elemente, die aufgrund von Merkmalen oder Ereignissen in unternehmensweiten Umgebungen vorkommen. Der Fokus auf Cyber-bezogene Datenanalysen kann informierte Richtlinienentscheidungen ermöglichen, Reaktionen vereinfachen und zu einem Risikoprofil führen, bei dem proaktive Sicherheitsmaßnahmen entwickelt werden, bevor ein Zwischenfall eintritt“.*[2]

Beachten Sie dabei folgende drei Punkte:

1. Das ZTMM konzentriert sich bei Transparenz und Analysen ausschließlich auf Sicherheitsaspekte und berücksichtigt nicht die potenziellen Vorteile in Bezug auf operative Flexibilität oder User Experiences für Endbenutzer.
2. Das ZTMM geht offensichtlich von einer Architektur aus, bei der die Identity-Funktion Telemetriedaten an ein anderes System (z. B. an eine SIEM-Lösung) weitergibt, die die Daten erfasst und analysiert.
3. Das ZTMM behandelt den Bereich Transparenz und Analysen eindeutig separat vom Bereich Automatisierung und Orchestrierung und von der eigentlichen Umsetzung/Durchsetzung von Richtlinien.

Diese Einstellungen sind subjektiv, und die CISA hat sicherlich gute Gründe dafür. Die Behörde ignoriert jedoch, dass führende Lösungen mehr Identity-Funktionen und Vorteile bieten können.

[2] CISA: Zero Trust Maturity Model, Version 2.0, April 2023, S. 11, abgerufen am 9. Juni 2025, https://www.cisa.gov/sites/default/files/2023-04/zero_trust_maturity_model_v2_508.pdf.

okta

Stufe	Beschreibung	Relevante Okta-Lösungen
 **Einfach**	In dieser Stufe erfassen Unternehmen Aktivitätenprotokolle und konzentrieren sich besonders auf privilegierte Anmeldedaten. Protokollanalysen werden routinemäßig (jedoch manuell) durchgeführt, sodass es kaum möglich ist, Risiken zeitnah zu identifizieren oder erweiterte Bedrohungen zu erkennen.	• Universal Directory
 **Eingeschränkt**	Zusätzlich zu manuellen Protokollanalysen führen Unternehmen einige automatisierte Analysen durch. Auch wenn Unternehmen durch die automatisierten Analysen Bedrohungen besser zeitnah erkennen können, behindert die begrenzte Korrelation zwischen den Protokolltypen dennoch die Erkennung erweiterter Bedrohungen.	• Universal Directory • Workflows
 **Hochentwickelt**	Analysen erfolgen jetzt vollständig (oder fast vollständig) automatisiert, einschließlich Korrelation zwischen Protokolltypen. Allerdings werden noch nicht alle Protokolltypen zu allen Benutzern und Entitäten einbezogen. Identity-Protokolle sind zudem mit anderen Quellen verknüpft. Auf diese Weise schließen sie die Transparenzlücken und bieten umfassendere Bedrohungserkennung.	• Universal Directory • Workflows • Identity Threat Protection
 **Strategisch**	Unternehmen erreichen und gewährleisten umfassende Transparenz durch automatisierte Analysen aller Protokolltypen zu allen Benutzern und Entitäten, wobei die Protokolle mit anderen Quellen verbunden sind.	• Universal Directory • Workflows • Identity Threat Protection

okta

Automatisierung und Orchestrierung

Der Umfang, mit dem ein Unternehmen den Bereich Automatisierung und Orchestrierung für Identities ausbauen kann, hängt stark von den Identity-Plattformen und den eingesetzten Produkten ab.

Die leistungsstärksten Identity-Lösungen unterstützen Automatisierung und Orchestrierung nicht nur durch Integration mit dem allgemeinen Tech-Stack, sondern enthalten auch selbst entsprechende Funktionen.

Diese integrierten Funktionen ermöglichen die Erstellung von Workflows für die Verwaltung von Identity-Lebenszyklen (inkl. JML-Prozesse (Joiner, Mover, Leaver)) und damit auch die Unterstützung starker Governance, die sorgfältige Kontrolle privilegierter Zugriffe, die Stärkung der Gesamtsicherheit usw., ohne dass dazu ein allgemeines Tool für Automatisierung und Orchestrierung benötigt wird.

Zero-Trust-Kontext

Das CISA ZTMM erklärt, dass „Zero Trust automatisierte Tools und Workflows vollständig nutzt, die in der Lage sind, die Sicherheitsreaktionen für Produkte und Services zu unterstützen und gleichzeitig Überwachung, Sicherheit und Interaktionen der Entwicklungsprozesse für diese Funktionen, Produkte und Services zu gewährleisten“.[3]

Der Bereich Automatisierung und Orchestrierung fasst also zusammen, *wie* Identity-Prozesse und -Funktionen aus anderen Bereichen implementiert sind und nicht, *was* diese Prozesse und Funktionen tatsächlich sind. Daher gibt es erhebliche Überschneidungen zwischen den Bereichen Automatisierung und Orchestrierung, Authentifizierung, Risikobewertungen und Zugriffsmanagement.

[3] CISA: Zero Trust Maturity Model, Version 2.0, April 2023, S. 11, abgerufen am 9. Juni 2025, https://www.cisa.gov/sites/default/files/2023-04/zero_trust_maturity_model_v2_508.pdf.

okta

Stufe	Beschreibung	Relevante Okta-Lösungen
 **Einfach**	In dieser Stufe arbeiten Unternehmen fast ausschließlich mit selbstverwalteten Identities und führen Lebenszyklusverwaltungsprozesse (inkl. Onboarding und Offboarding) manuell durch. Dazu verwenden sie v. a. E-Mails, Collaboration-Apps, Servicedesk-Tickets und ähnliche Hilfsmittel. Es gibt kaum Integrationen zwischen den verschiedenen Systemen und Überprüfungen (z. B. der Zugriffsrechte) erfolgen manuell in einem festgelegten Rhythmus.	• Lifecycle Management • Workflows
 **Eingeschränkt**	In dieser Stufe beginnen Unternehmen mit der Implementierung einiger Automatisierungs- und Orchestrierungsprozesse in Bezug auf nicht-privilegierte Benutzer und selbstverwaltete Identities. Die Provisionierung und Deprovisionierung von Benutzern erfolgt zunehmend automatisiert. Unternehmen orchestrieren privilegierte Identities weiterhin manuell, verwalten jetzt allerdings auch externe Identities.	• Lifecycle Management • Workflows • Okta Identity Governance • Okta Privileged Access
 **Hochentwickelt**	In dieser Stufe verfügen Unternehmen über ausreichend Integrationen in allen Umgebungen, um Automatisierung und Orchestrierung für interne und externe Identities zu ermöglichen. Privilegierte Identities werden weiterhin manuell orchestriert. Die Erkennung und Behebung von Identity-Risiken erfolgt automatisiert und umfasst Funktionen zur proaktiven Erkennung und Behebung potenzieller Bedrohungen.	• Lifecycle Management • Workflows • Okta Identity Governance • Okta Privileged Access
 **Strategisch**	In dieser Stufe sind alle Identity-Orchestrierungsprozesse automatisiert. Sie umfassen alle Identities sowie Umgebungen und basieren auf Verhaltensweisen, Registrierungen und Bereitstellungsanforderungen. Unternehmen können Behebungsreaktionen flexibel automatisieren, indem sie nachgelagerte Prozesse auslösen, die für die konkreten Anforderungen bei erkannten Risiken maßgeschneidert sind.	• Lifecycle Management • Workflows • Okta Identity Governance • Okta Privileged Access

Governance

Identity Governance bezieht sich auf die Definition und Durchsetzung von Richtlinien, Prozeduren und Prozessen, die für das Erreichen von Unternehmenszielen (z. B. Implementierung von Zero-Trust-Prinzipien, Verbesserung der Effizienz, Steigerung der Produktivität) und die Einhaltung von Vorschriften, Frameworks, Standards und vertraglichen Verpflichtungen erforderlich sind.

In Bezug auf Governance erhöht sich der Reifegrad, wenn isolierte und manuelle Ansätze schrittweise durch umfassende und automatisierte Ansätze ersetzt werden. Dazu gehören das Vereinheitlichen von Richtlinien für menschliche und nicht-menschliche Identities, das Anwenden rollen- und risikobasierter Zugriffskontrollen sowie das Skalieren der Lebenszyklusverwaltung und der Zertifizierungsprozesse.

Mit zunehmendem Reifegrad werden die Governance-Maßnahmen von Ad-hoc-Kontrollen hin zu kontinuierlicher und intelligenter Automatisierung für APIs, Service-Accounts und robotergestützten Prozessen erweitert. Nicht-menschliche Identities werden in Bezug auf Governance gleichberechtigt behandelt und unterliegen in jeder Phase des Identity-Lebenszyklus Least-Privilege-Prinzipien, Zugriffsprüfungen und Compliance-Kontrollen.

Stufe	Beschreibung	Relevante Okta-Lösungen
 **Einfach**	In dieser Stufe sind nur wenige Identity Governance-Maßnahmen integriert. Die vorhandenen Programme sind meist isoliert (und nicht auf gemeinsame geschäftliche und Governance-Ziele abgestimmt) oder separat und konzentrieren sich lediglich auf menschliche Identities. Es gibt keine zentralen Kontrollen für nicht-menschliche Identities, sodass deren Zahl häufig ungehindert steigt, was zu größeren Risiken führt.	• Lifecycle Management • Workflows
 **Eingeschränkt**	Unternehmen haben Governance und Compliance durch automatisierte Zugriffsprüfungen und Zugriffsanfragen vereinfacht. Governance wird durch rollenbasierte Modelle stärker strukturiert. Provisionierung und Deprovisionierung werden basierend auf Lebenszyklusereignissen automatisiert und es werden regelmäßige Zugriffszertifizierungen durchgeführt. Basale Kontrollen für nicht-menschliche Identities werden eingeführt und bestehen typischerweise aus grundlegender Lebenszyklusautomatisierung für Service-Accounts und Bots.	• Lifecycle Management • Workflows • Okta Identity Governance • Okta Privileged Access
 **Hochentwickelt**	Unternehmen nutzen erweiterte Prozesse für Governance und operative Abläufe, mit denen sichergestellt ist, dass das Identity-Management sich kontinuierlich weiterentwickeln kann und Mehrwert bietet. Der Zugriff wird durch dynamische und richtlinienbasierte Kontrollen überwacht, die Benutzerattribute, Risikostufen und Geschäftsregeln berücksichtigen. Just-in-Time- und zeitgebundener Zugriff wird implementiert. Riskante Abfragen lösen die Anforderung von Human-in-the-Loop-Genehmigungen aus. Zudem wird Aufgabentrennung durchgesetzt, um Konflikte bei Zugriffsrechten zu vermeiden. Governance für nicht-menschliche Identities wird systematisch implementiert, einschließlich Least-Privilege-Prinzip, Überprüfungen sowie Lebenszykluskontrollen ähnlich wie bei menschlichen Benutzern.	• Lifecycle Management • Workflows • Okta Identity Governance • Okta Privileged Access
 **Strategisch**	Unternehmen nutzen KI zur Verbesserung von Identity-Sicherheit, Governance und User Experiences sowie zur Vereinfachung von Konfigurationen und Entwicklung. Die Governance erfolgt nun kontinuierlich und proaktiv. Zugriffsentscheidungen sind autonom und erfolgen risikobasiert anhand prädiktiver Analysen und einheitlicher Richtlinien für alle Cloud-, Hybrid- und On-Premise-Umgebungen. Zertifizierungen erfolgen nicht mehr nach Zeitplan, sondern ereignisbasiert, wobei nicht-menschliche Identities vollständig in adaptive Governance-Prozesse integriert sind. Human-in-the-Loop-Kontrollen werden nur für hochriskante Szenarien angewendet und gewährleisten adaptive Governance, die ein Gleichgewicht zwischen Automatisierung und intelligenten Interventionen bietet. Autonome Governance für nicht-menschliche Identities (einschließlich Risikobewertungen, Zugriffsautomatisierung und intelligente Behebung) wird zu einer Kernfunktion.	• Lifecycle Management • Workflows • Okta Identity Governance • Okta Privileged Access

okta

Fazit

Auch wenn die Identity-Journey jedes Unternehmens individuell ist, gibt es ganz klar typische Muster. Und durch den Fokus auf den Identity-Reifegrad können Unternehmen von einer gestärkten Sicherheitslage, einer produktiveren Belegschaft, verbesserter betrieblicher Effizienz und kontinuierlichem geschäftlichem Wachstum profitieren.

okta