Whitepaper

Okta Secure Identity Commitment

Letzte Aktualisierung: 29. Mai 2024

Wir bieten marktführende Produkte und Services für den Schutz von Identities

Wir führen bei unseren Kunden Best Practices ein, die optimalen Schutz gewährleisten

Wir bringen unsere Branche aktiv voran – für besseren Schutz vor Identity-basierten Angriffen

Wir sichern die Infrastruktur unseres eigenen Unternehmens ab

Inhalt

Executive Summary

Identity ist heute der wichtigste Zugangsschlüssel für alle Mitarbeiter- und Kundenanwendungen. Gleichzeitig nimmt die Komplexität und Zahl der Angriffe gegen große und kleine Unternehmen immer mehr zu. Für Unternehmen ist es von größter Wichtigkeit, solche Attacken frühzeitig zu erkennen und zu stoppen.

Als ein führender, unabhängiger Identity-Anbieter steht Okta bei der Abwehr dieser Angriffe an vorderster Front. Dieser Rolle tragen wir jetzt Rechnung – mit dem Okta Secure Identity Commitment:

- Wir bieten marktführende Produkte und Services für den Schutz von Identities
- Wir führen bei unseren Kunden Best Practices ein, die optimalen Schutz gewährleisten
- Wir bringen unsere Branche aktiv voran – für besseren Schutz vor Identity-basierten Angriffen
- Wir sichern die Infrastruktur unseres eigenen Unternehmens ab

Im Rahmen dieses Programms haben wir bereits eine Reihe wichtiger Funktionalitäten und Upgrades umgesetzt bzw. angekündigt – sowohl in der Infrastruktur unseres Unternehmens als auch in unserem Produktportfolio. Eine Zusammenfassung dieser Updates finden Sie weiter unten.

Wir sind uns bewusst, dass unsere Arbeit nie zu Ende ist, und werden mit strategischen Investitionen weiterhin proaktiv Maßnahmen ergreifen, um der dynamischen Bedrohungslandschaft einen Schritt voraus zu bleiben.

Einführung

Als wir Okta im Jahr 2009 gründeten, konzentrierten wir uns in erster Linie auf das IT-Management – und konkret darauf, wie Identity and Access Management Mensch und Technologie verbinden kann.

Seitdem haben zwei wichtige Trends zu einer stark veränderten Wahrnehmung von Identities und damit auch zu einer veränderten Nachfrage nach Identity-Lösungen geführt:

1. **Identity ist heute der wichtigste Zugangsschlüssel** für alle Mitarbeiter- und Kundenanwendungen
2. **Volumen und Komplexität von Cyberangriffen haben zugenommen**, wobei zahlreiche Bedrohungsakteure (darunter Ransomware-Gruppen, staatliche Akteure und böswillige Insider) effektive Taktiken, Techniken und Prozesse (TTPs) entwickeln, um Schutzmaßnahmen zu umgehen und der Entdeckung zu entgehen

Diese Trends haben zu einem erheblichen Wandel in der Branche geführt. Dadurch agieren wir nicht mehr nur als Bindeglied zwischen Menschen und Technologie, sondern sind zudem als unermüdlicher Wächter für den Schutz der sensiblen Daten jedes Unternehmens verantwortlich.

Um dieser Verantwortung gerecht zu werden, verfolgen wir ***unser Ziel, jedem die Freiheit zu geben, jede Technologie sicher zu nutzen***.

Okta Secure Identity Commitment

Identities sind heute Teil der geschäftskritischen Sicherheitsinfrastruktur.

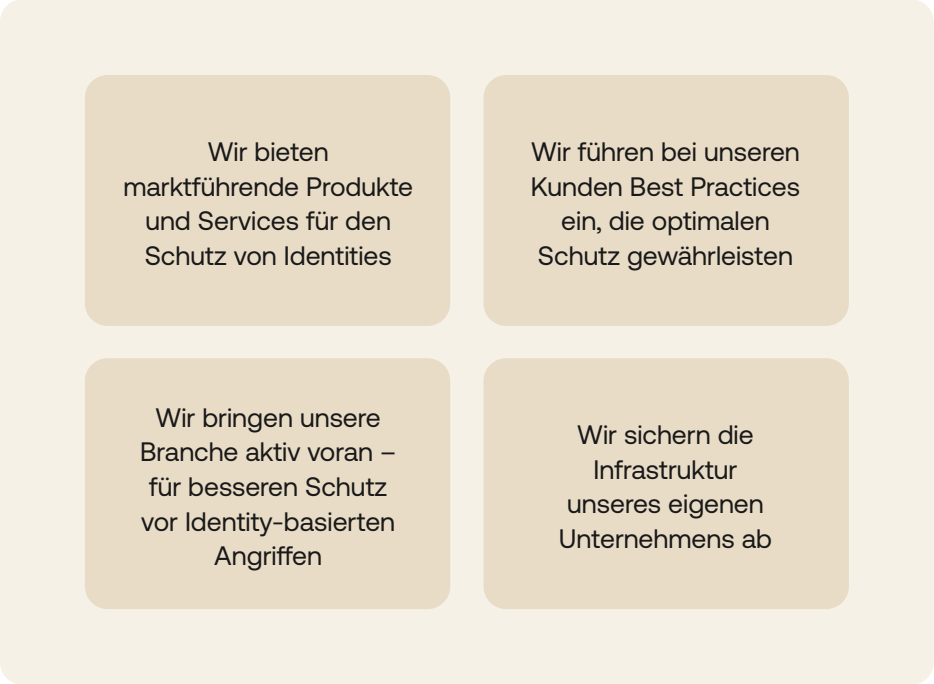
Als ein weltweit führender, unabhängiger Identity-Anbieter steht Okta bei der Abwehr von Identity-basierten Attacken an vorderster Front. Unsere Produkt-, Engineering-, Sicherheits- und Business-Technology-Teams entwickeln unsere Technologieplattform kontinuierlich weiter, um unsere mehr als 18.000 Kunden zu schützen. Zum Beispiel:

- Okta ThreatInsight ***erkennt und blockiert mehr als zwei Milliarden böswillige Anfragen*** innerhalb von 30 Tagen. (Quelle: interne Berichte für den Zeitraum vom 5. Dezember 2023 bis 4. Januar 2024)
- Bei einigen unserer größten Kunden konnten wir innerhalb von 90 Tagen ***Credential Stuffing-Angriffe und böswilligen Bot-Traffic um mehr als 90 Prozent reduzieren***. (Quelle: interne Berichte zu anonymisierten Daten von Enterprise-Kunden vom 5. Oktober 2023 bis 4. Januar 2024)

- Wir prägen die Best Practices der Branche – alle Okta-Mitarbeitende nutzen ***Okta FastPass mit Device Assurance sowie Adaptive MFA (AMFA) als Phishing-resistente Faktoren***.
  (Quelle: interne Berichte vom Februar 2024)

Wir haben uns das Ziel gesetzt, die IT Security-Branche voranzubringen und unsere Kunden sowie ihre wichtigsten Assets zuverlässig zu schützen. Dieser Aufgabe tragen wir jetzt Rechnung – mit dem Okta Secure Identity Commitment, unserer Initiative für sichere Identities.

Diese Initiative basiert auf vier Säulen, deren Umsetzung wir in diesem Dokument im Detail erläutern.



Wir bieten marktführende Produkte und Services für den Schutz von Identities

Wir sind uns bewusst, dass unsere Sicherheit auch Ihre Sicherheit ist. Aus diesem Grund entwickeln wir die Sicherheitsfunktionen unserer Identity-Produkte und -Services mit höchster Priorität weiter.

Durch diesen kontinuierlichen Fokus können wir die stärksten und innovativsten Schutzmaßnahmen bereitstellen und das Vertrauen weltweit bekannter Marken gewinnen.

Auf der Oktane 2023 haben wir eine Vielzahl von Funktionen angekündigt, die die Sicherheit unserer Kunden erhöhen – viele davon verwenden Okta AI.

Seither haben wir uns auf einige zentrale Bereiche konzentriert, um unsere Produkte und Services weiter auszubauen. Dazu gehören:

- Absicherung des Admin-Zugriffs auf Kundenverwaltungskonsolen
- Stärkung der Sicherheit für Sessions, Benutzer, Anwendungen und Geräte
- Bereitstellung von Security Best Practices für unsere Kunden

Kürzlich veröffentlicht oder angekündigt (für Ende Mai 2024)

Workforce Identity Cloud

- Identity Threat Protection mit Okta AI
- Kontrolle von Okta-Admin-Rollen
- Erzwingung von MFA für den Zugriff auf die Okta-Admin-Konsole
- Erzwingung von MFA für geschützte Aktivitäten in der Admin-Konsole
- Möglichkeit für Admins, Anfragen über Anonymisierungsdienste zu erkennen und zu stoppen
- Aktivierung von IP-Adressen- und ASN-Bindung an die Admin-Konsole
- Durchsetzung einer Allow-Listed-Netzwerkzone für APIs
- Durchsetzung von Token-Bindung für M2M-Application-Service-Integrationen
- Verhinderung von Account-Lockouts für Okta-Anwender

Geplante Features (für Ende Juli 2024)

Workforce Identity Cloud

- Identity Security Posture Management
- Ausbau der in den Produkten verankerten Best-Practice-Guidelines
- Erzwingung von MFA für den Zugriff auf First-Party-Admin-Anwendungen
- Sichere Agentenbereitstellung für Active Directory

Customer Identity Cloud

- Verbesserte Bot-Erkennung bei der Passwort-Wiederherstellung
- API für das Refresh Token-Management
- Von Kunden verwaltete Schlüssel
- Anpassung von Sessions durch erweiterbare Funktionen

Geplante Features (für Oktober 2024)

Workforce Identity Cloud

- Roll-out von FastPass ausschließlich auf verwalteten Geräten
- Step-up-Authentifizierung für sensible Tenant-Workflows
- Okta Privilege Access für Service-Accounts in SaaS

Customer Identity Cloud

- Kontrolle über gleichzeitige Sessions

Customer Identity Cloud

- Fine Grained Authorization
- Okta AI mit Bot-Erkennung der vierten Generation
- Authentifizierungsabfrage
- Erzwingung von MFA für alle Dashboard-Admins
- Erweiterung des OIDC Back-Channel-Logouts mit Initiatoren
- Durchsetzung von ASN-Bindung für Auth0-Admin-Sessions
- API für das Session- und Refresh-Token-Management
- Festlegung der progressiven Faktor-Registrierung für Endbenutzer
- Festlegung unternehmensweiter Session-Timeouts
- Absicherung der Zugriffskontrollen auf Tenant-Ebene

**Bitte beachten Sie, dass sich alle Roadmap-Elemente ändern können. Wir informieren unsere Kunden regelmäßig über den Status zuvor kommunizierter Projekte.*

Kürzlich veröffentlicht

Folgende Produkte und Features, die die Sicherheit unserer Kunden erhöhen, wurden in letzter Zeit veröffentlicht:

Workforce Identity Cloud

- **Identity Threat Protection mit Okta AI:** Stärken Sie die Resilienz Ihrer Identities nach der Authentifizierung, indem Sie die Risiken kontinuierlich neu bewerten. Nutzen Sie integrierte Indikatoren von First-Party- und Third-Party-Partnern, um neue, nach der Authentifizierung ansetzende Bedrohungen aus beliebigen Quellen proaktiv abzuwehren.
- **Kontrolle von Okta-Admin-Rollen:** Legen Sie für Ihre Okta-Admin-Konten Zero-Standing-Privilegien fest, mit befristeten Ad-hoc-Zugriffsrechten bei einzelnen Benutzern und Zugriffsüberprüfungen bei bestehenden Administratoren.

- **Erzwingung von MFA für den Zugriff auf die Admin-Konsole:** Verhindern Sie, dass Administratoren Authentifizierungsrichtlinien erstellen können, die nur einen Faktor erfordern. Außerdem kann der Ein-Faktor-Zugriff auf die Admin-Konsole optional deaktiviert werden.
- **Erzwingung von MFA für geschützte Aktivitäten in der Admin-Konsole:** Implementieren Sie eine zusätzliche Sicherheitsebene für wichtige Aktivitäten in Okta, indem Sie Step-up-Authentifizierung für Admins erzwingen.
- **Möglichkeit für Admins, Anfragen über Anonymisierungsdienste zu erkennen und zu stoppen:** Geben Sie Administratoren die Möglichkeit, den Zugriff basierend darauf zu erlauben oder zu verweigern, ob eine IP-Adresse mit Anonymisierungsdiensten verbunden ist. Dadurch kann das Unternehmen den unbefugten Zugriff über solche Quellen unterbinden.
- **Aktivierung von IP-Adressen- und ASN-Bindung an die Admin-Konsole:** Um potenzielle Session-Übernahmen wichtiger (First-Party-) Ressourcen zu verhindern, werden Sessions mit der Okta-Admin-Konsole automatisch beendet, wenn die ASN (Autonomous System Number) einer API- oder Web-Anfrage von der ASN abweicht, die zu Beginn der Session aufgezeichnet wurde. Bei folgenden Okta-Produkten haben Kundenadministratoren die Möglichkeit, Admin-Sessions automatisch zu beenden, wenn sich die beobachtete IP-Adresse während einer aktiven Session ändert: Workflows Admin, Okta Access Requests (Inbox), Okta Privileged Access (OPA), Okta-Admin-Konsole.
- **Durchsetzung einer Allow-Listed-Netzwerkzone für APIs:** Verhindern Sie, dass Angreifer und Malware SSWS-Token stehlen und außerhalb des spezifizierten IP-Bereichs wiederverwenden können, um sich unberechtigten Zugriff zu verschaffen.
- **Durchsetzung von Token-Bindung für M2M-Application-Service-Integrationen:** Okta erhöht die Sicherheit automatisierter Transaktionen, indem standardmäßig die Token-Bindung per Proof-of-Possession in M2M-Integrationen (Machine-to-Machine) erzwungen wird. Dadurch können nur authentifizierte Anwendungen Token für den Zugriff auf Okta-APIs verwenden.
- **Verhinderung von Account-Lockouts für Okta-Anwender:** Okta bietet schon länger die Möglichkeit, verdächtige Login-Versuche von unbekannten Geräten zu blockieren. Die neue Funktion verhindert, dass legitime Benutzer (einschließlich Admins) blockiert werden, wenn ein anderes, bisher unbekanntes Gerät eine Sperrung verursacht.

Customer Identity Cloud

- **Fine Grained Authorization:** Mit FGA lässt sich Autorisierungslogik stärker skalieren sowie besser einsetzen und auditieren als klassische Zugriffskontrollmethoden. Die Funktion ist für Workforce und Customer Identity Cloud verfügbar.
- **Okta AI mit Bot-Erkennung der vierten Generation:** Die neue Version der Bot Detection-Funktion nutzt Third-Party-Risikoindikatoren sowie ein neues ML-Modell (Machine Learning), um den Schutz vor betrügerischen Registrierungen zu optimieren.
- **Authentifizierungsabfrage:** Minimieren Sie Bot-Aktivitäten mit einer Authentifizierungsabfrage, die Browser- und Geräteindikatoren nutzt, um Bots größere Hindernisse als bei klassischen CAPTCHAs in den Weg zu legen.
- **Erzwingung von MFA für alle Dashboard-Admins:** Bisher wurde MFA für Auth0-Administratoren optional aktiviert. Nun wird jedoch für alle Admins mit Benutzername/Passwort-Anmeldung oder Third-Party-Social-Login die Authentifizierung per MFA erzwungen.
- **Erweiterung des OIDC Back-Channel-Logouts mit Initiatoren:** Fügt die Ereignisse „Konto gelöscht“ und „E-Mail-Adresse geändert“ zur Liste der Logout-Initiatoren hinzu (bisher: „Passwort geändert“, „Sitzung abgelaufen“ und verschiedene Logout-Ereignisse). Diese Ereignisse verbinden sich mit Session-Terminierungs-Ereignissen, um Anwendungen zur Abmeldung von Benutzern aufzufordern, sobald eine Benutzer-Session ungültig wird.
- **Durchsetzung von ASN-Bindung für Auth0-Admin-Sessions:** Sessions mit der Okta-Admin-Konsole werden automatisch beendet, wenn die ASN (Autonomous System Number) einer API- oder Web-Anfrage von der ASN abweicht, die zu Beginn der Session aufgezeichnet wurde.
- **API für das Session- und Refresh-Token-Management:** Gewährt zentralisierten Zugriff auf die Liste und ermöglicht das anwendungsübergreifende Management sowie den Widerruf von Benutzerrechten. Falls der Verdacht besteht, dass eine Sitzung gehackt wurde, kann sie präventiv beendet werden, um Kunden und Geschäftsbetrieb zu schützen.
- **Festlegung der progressiven Faktor-Registrierung für Endbenutzer:** Mit einer Post-Login Action können Unternehmen die sekundären Faktoren ihrer Endbenutzer für die MFA-Anmeldung definieren. Dadurch können Kunden ihre Authentifizierungsrichtlinien besser an ihre Sicherheitsziele anpassen.

Für Juli 2024 geplante Features

Workforce Identity Cloud

- **Identity Security Posture Management:** Minimieren Sie Ihre Identity-Angriffsfläche, indem Sie Risiken wie übermäßige Berechtigungen, Konfigurationsfehler und MFA-Lücken in Ihrer Identity-Infrastruktur, in der Cloud sowie in SaaS-Anwendungen identifizieren und priorisieren.
- **Ausbau der in den Produkten verankerten Best-Practice-Guidelines:** Okta wird zusätzliche produktinterne Empfehlungen bereitstellen, um Kunden bei der Implementierung von Best Practices zum Schutz ihrer Okta-Tenants zu unterstützen.
- **Erzwingung von MFA für den Zugriff von First-Party-Admin-Anwendungen:** Die Admin-Konsolenrichtlinie für First-Party-Admin-Anwendungen deckt Okta Access Certifications, Okta Entitlement Management und Okta Access Requests ab. Für den Admin-Zugriff auf diese Anwendungen wird MFA erzwungen.
- **Sichere Agentenbereitstellung für Active Directory:** Der aktualisierte AD-Agent nutzt einen OIDC-Proof-of-Possession-Ansatz für die Kommunikation mit Okta, der verhindert, dass nicht autorisierte Benutzer auf vertrauliche Informationen zugreifen können.

Customer Identity Cloud

- **Verbesserte Bot-Erkennung bei der Passwort-Wiederherstellung:** Kunden erhalten die Möglichkeit, die Funktion Bot Detection für Passwort-Wiederherstellungsprozesse (zusätzlich zu den bereits bestehenden Registrierungs- und Anmeldungsprozessen) zu aktivieren, um zusätzlichen Schutz vor Account-Hacking zu erhalten.
- **API für das Refresh Token-Management:** Entwickler erhalten mithilfe zusätzlicher Management-API-Endpoints die Möglichkeit, den Authentifizierungsstatus ihrer Benutzer per Fernzugriff zu überwachen.
- **Von Kunden verwaltete Schlüssel:** Bieten Sie Kunden die Möglichkeit, die wichtigsten Verschlüsselungsschlüssel ihrer Tenants auf sichere Weise zu ersetzen und zu verwalten, auch bei Bring Your Own Keys (BYOK)- und Control Your Own Keys (CYOK)-Szenarien.
- **Anpassen von Sessions durch erweiterbare Funktionen:** Nutzen Sie die Session-Management-API unserer Actions & Extensibility-Plattform, um basierend auf Risikoindikatoren konkrete Verhaltensweisen zu definieren, die zur Beendigung verdächtiger Sessions führen, und Richtlinien für die Erkennung und Reaktion auf Hacker-Angriffe festzulegen.

- **Festlegung unternehmensweiter Session-Timeouts:** Passen Sie Session-Timeouts mit zusätzlicher Logik an, einschließlich Organisation.
- **Absicherung der Zugriffskontrollen auf Tenant-Ebene:** Geben Sie Kunden die Möglichkeit, Traffic von konkreten IP-Adressen, CIDR-Blöcken (Classless Inter-Domain Routing) und Regionen zu blockieren, um DDoS-Angriffe abzuwehren, indem Anfragen direkt am Edge abgewiesen werden.

Für Oktober 2024 geplante Features

Workforce Identity Cloud

- **Roll-out von FastPass ausschließlich auf verwalteten Geräten:** Bei Okta können Administratoren mithilfe von Richtlinien festlegen, dass Benutzer bestimmte Voraussetzungen erfüllen müssen, damit für sie Authentifizierungsfaktoren registriert werden dürfen. In der ersten Phase können nur diejenigen Benutzer Okta Verify FastPass nutzen, die ein verwaltetes Gerät verwenden.
- **Step-up-Authentifizierung für sensible Tenant-Workflows:** Implementieren Sie eine zusätzliche Sicherheits- und Kontrollebene für die Benutzerauthentifizierungsprozesse.
- **Okta Privilege Access für Service-Accounts in SaaS:** Beschleunigen Sie Service-Accounts in SaaS- und Hyperscaler-Umgebungen, indem Sie sie in Okta Privileged Access als geschützte Ressource festlegen. Dadurch erhalten Kunden native Produktfunktionen, mit denen sie Transparenz erhalten und den Lebenszyklus von Service-Accounts verwalten können, darunter Erkennung, Verwaltung, Governance, Transparenz und Provisionierung.

Customer Identity Cloud

- **Kontrolle über gleichzeitige Sessions:** Mit Kontrollfunktionen für gleichzeitige Sessions können Ihre Tenants die Anzahl aktiver Geräte Ihrer Benutzer einschränken – und somit die Zahl der für mehrere Konten genutzten Anmeldedaten deckeln oder diese Zahl als Risikoindikator nutzen, sodass neue Logins oberhalb einer von Ihrem Unternehmen definierten Grenze abgelehnt werden.

Wir führen bei unseren Kunden Best Practices ein, die optimalen Schutz gewährleisten

Eine falsch konfigurierte Identity ist ein weiteres Einfallstor für einen böswilligen Akteur oder Insider. Mit 15 Jahren Erfahrung und mehr als 18.000 Kunden verfügen wir über das notwendige Know-how, um die richtigen Identity-Konfigurationen bei unseren Kunden zu implementieren.

Um sicherzustellen, dass unsere Kunden in vollem Umfang von unserer langjährigen Erfahrung profitieren, bauen wir unseren Kundenservice weiter aus.

Darüber hinaus setzen wir uns dafür ein, dass unsere Produkte mit den Security Best Practices von Okta implementiert werden, damit die Widerstandsfähigkeit unserer Kunden gegenüber Identity-basierten Sicherheitsverletzungen gestärkt wird.

Dazu stellen wir unseren Kunden und der gesamten Branche Best-Practice-Guides und weitere Schulungsmaterialien bereit, die aktuelle Bedrohungen thematisieren:

- **Actions Template Implementation Guides:** Sichere Konfigurationsvorlagen vereinfachen die Implementierung von Best Practices bei Kunden mit Okta Customer Identity Cloud.
- **Protecting Administrative Sessions in Okta:** Informieren Sie sich über empfohlene Konfigurationen in Okta, um Admin-Sessions und Konten mit privilegierten Zugriffsrechten zu schützen, die Angriffsfläche zu minimieren, Account-Hacking zu verhindern und die Auswirkungen gestohlener Sessions einzudämmen.
- **Customer Identity Cloud Enhancements to Prevent Account Takeover:** Dieser Blog stellt die die neuen Funktionen vor und erklärt, wie sie den Schutz vor gehackten Konten stärken.
- **Okta Device Access now supports passwordless login and FIDO2 Yubikeys for Desktop MFA:** (WIC): Okta ist für den Ansatz bekannt, dass bestmöglicher Schutz in Zukunft ohne Passwörter gewährleistet wird. Dies ist ein weiteres Beispiel dafür, wie wir das umsetzen.
- **Apply IP or ASN binding to Admin Console:** (WIC, standardmäßig aktivierte Funktion): Security-by-Default ist eine branchenweite Best Practice, sodass der Schutz durch IP-Adressenbindung für Kunden standardmäßig aktiv ist. Wenn also ein Admin plötzlich eine andere IP-Adresse nutzt als diejenige, mit der er sich ursprünglich angemeldet hat, wird er automatisch abgemeldet und zur Neuauthentifizierung aufgefordert.

Wir bringen unsere Branche aktiv voran – für besseren Schutz vor Identity-basierten Angriffen

Im Bereich Identity-Sicherheit führend zu sein, ist für Okta ein zentrales Ziel. Wir konzentrieren uns darauf, unsere Branche bei der Erkennung und Abwehr von Identity-Angriffen zu unterstützen, entwickeln deshalb unsere Möglichkeiten weiter und implementieren neue Technologien wie KI.

Darüber hinaus spielen wir eine proaktive Rolle bei der Gestaltung des Identity-Sicherheitsansatzes der Branche. Dazu reagieren wir mit führenden Präventions-, Erkennungs- sowie Schutzstrategien auf die rasant wachsenden und immer komplexeren Cyberbedrohungen und setzen damit einen hohen Standard in der Branche.

- **How to Secure the SaaS Apps of the Future:** Lernen Sie die grundsätzlichen Anforderungen an die Absicherung moderner SaaS-Anwendungen gegen Angriffe nach erfolgter Authentifizierung kennen und erfahren Sie, wie Cybersicherheitsstandards in der gesamten IT-Branche dank fortschrittlicher Sicherheitsfunktionen wie Proof-of-Possession, kontinuierlicher Evaluierung der Zugriffsrechte sowie Universal Logout-Funktionen vorangebracht werden.
- **Leveraging the Okta Identity Security Commitment to Enable Zero Trust:** Erfahren Sie, wie Okta-Sicherheitsfunktionen die Identity-basierten Zero Trust-Strategien unterstützen. Dabei wird für jede Funktion erläutert, wie sie basierend auf dem NIST Cybersecurity Framework den Zero Trust-Ansatz umsetzt.
- **Learning grants address the tech industry skills gap:** Okta-Bildungsstipendien unterstützen arbeitssuchende Techniker, einschließlich Veteranen und Ehepartner von Militärangehörigen. Dabei erhalten sie Zugang zum On-Demand-Kurskatalog von Okta, einem Premier Practice Exam, einem Okta-Voucher für Zertifizierungen und mehr.
- **Okta for Good hat 3,1 Millionen US-Dollar** für das eigene Wohltätigkeitsprogramm in Höhe von 50 Millionen US-Dollar bereitgestellt. Dies deckt auch zwei über 5 Jahre laufende Programme in Höhe von 1 Millionen US-Dollar für langjährige Partner und bekannte Fürsprecher für die digitale Transformation im Non-Profit-Sektor ab.
- **CISA's Secure by Design pledge:** Neben anderen weltweiten Unternehmen bekennt Okta sich zu CISA-Initiative „Secure by Design". Im Rahmen dieser Initiative verpflichtet sich unsere Branche, entscheidende Schritte zur Implementierung grundsätzlich sicherer Designprinzipien zu unternehmen.

Absicherung der Okta-Infrastruktur

Für alle unsere internen Mitarbeitenden, Prozesse und Technologien gelten die gleichen strengen Sicherheitsstandards wie für unsere kundenorientierten Produkte – im Sinne eines ganzheitlichen Sicherheitsansatzes.

Darüber hinaus investieren wir verstärkt in die Absicherung unserer sekundären (d. h. produktionsnahen) und unternehmenseigenen Systeme.

Kürzlich veröffentlicht/ angekündigt (für Ende Mai 202)	Geplante Updates (für Juli 2024)	Geplante Updates (für Oktober 2024)
• Verbesserung der Phishing-Resistenz bei neuen Mitarbeitenden • Durchführung eines internen Security-Assessments • Standardisiertes und zentralisiertes Reporting für das Sicherheitsrisiko-Management • Durchführung eines Security-Assessments für SaaS-Anwendungen **Verbesserte Erkennungs- und Reaktions-Funktionen:** • Neues Tool zur Verwaltung von Sicherheitsvorfällen • Neue Threat Intelligence-Plattform • Zusätzliche Dark Web-Überwachungsfunktionen	• Verbesserung der Phishing-Resistenz bei allen Mitarbeitenden • Verbesserter Schutz von Laptops • Automatisierte Erkennung und Meldung von M2M-Service-Accounts in SaaS-Anwendungen • Verbesserter Schutz mobiler Geräte	• Standardisiertes und zentralisiertes Management von Schwachstellen, Asset-Management und CSPM • Verbesserung bei der Protokolldatenerfassung und bei Analysetools • Erweiterte Scans von Open-Source-Software

**Bitte beachten Sie, dass sich alle Roadmap-Elemente ändern können. Wir informieren unsere Kunden regelmäßig über den Status zuvor kommunizierter Projekte.*

Kürzlich integriert

Zu den jüngsten Änderungen, Upgrades und Verbesserungen der Okta-Unternehmensinfrastruktur zählen:

- **Verbesserung der Phishing-Resistenz bei neuen Mitarbeitenden:** Wir haben schon vor längerer Zeit Okta FastPass für Phishing-resistentes MFA implementiert und vor kurzem Phishing-Schutz per YubiKeys für alle neuen Mitarbeitende bereitgestellt, sodass während der gesamten Mitarbeiterlaufbahn gänzlich auf Passwörter verzichtet werden kann.
- **Durchführung eines internen Security-Assessments:** In Partnerschaft mit einer führenden weltweiten Beratungsfirma haben wir eine umfassende Sicherheitsüberprüfung unserer Produkte, Infrastruktur und Unternehmenssysteme durchgeführt. Dazu gehört ein Security-Assessment unserer internen Systeme für Finanzen, Vertrieb, Data Warehouse, Marketing, IaaS und Integration.
- **Standardisiertes und zentralisiertes Reporting für das Sicherheitsrisiko-Management:** Wir haben eine Single-Vendor-Lösung implementiert, um das Risiko- und Vorfall-Management im Zusammenhang mit unserem Governance-, Risiko- und Compliance-Programm zu zentralisieren (einschließlich Third-Party-Risiko-Management).
- **Durchführung eines Security-Assessments für SaaS-Anwendungen:** Gemeinsam mit externen Sicherheitsexperten haben wir Security-Assessments unserer kritischen SaaS-Anwendungen durchgeführt, darunter das Okta Help Center sowie unsere Systeme für Finanzen, CRM (Customer Relationship Management), HCM (Human Capital Management), Vertrieb, Data Warehouse, Marketing, Infrastructure-as-a-Service (IaaS) und Integration.

Verbesserte Erkennungs- und Reaktions-Funktionen:

- **Neues Tool zur Verwaltung von Sicherheitsvorfällen:** Unsere neuen Tools bieten verbesserte Reaktionszeiten, Automatisierung und Zuverlässigkeit.
- **Neue Threat Intelligence-Plattform:** Unsere neue Plattform ermöglicht die Automatisierung und Korrelation von Threat Intelligence, wodurch die Bedrohungserkennung und -abwehr verbessert wird.
- **Zusätzliche Dark Web-Überwachungsfunktionen:** Wir können jetzt potenzielle Bedrohungen proaktiv identifizieren, indem wir regelmäßig das Dark Web nach Inhalten mit Bezug zu Okta scannen.

Für die Veröffentlichung im Juli 2024 geplante Updates:

- **Verbesserung der Phishing-Resistenz bei allen Mitarbeitenden:** Wir werden die Phishing-Resistenz durch YubiKeys für alle Mitarbeitende stärken.
- **Verbesserter Schutz von Laptops:** Wir werden weiter einschränken, welche Okta-Laptops verwendet werden können, und zudem auf Least Privilege-Prinzipien sowie klar definierte Rollen achten.
- **Automatisierte Erkennung und Meldung von M2M-Service-Accounts in SaaS-Anwendungen:** Wir werden ein Tool implementieren, das Transparenz für lokale Service-Accounts bietet, die innerhalb von SaaS-Anwendungen erstellt wurden, um die zur Authentifizierung verwendeten Secrets besser kontrollieren und rotieren zu können.
- **Verbesserter Schutz mobiler Geräte:** In puncto Mobilgerätesicherheit werden wir eine harte Linie fahren. Auch wenn unser Produkt Okta Verify bereits größere Sicherheit bietet (z. B. durch Vorschriften für PIN, Verschlüsselung und Betriebssystem), werden wir unsere MDM-Sicherheit (Mobile Device Management) durch zusätzliche Einschränkungen des privilegierten Zugriffs stärken.

Für die Veröffentlichung im Oktober 2024 geplante Updates:

- **Standardisiertes und zentralisiertes Reporting für Vulnerability Management, Asset Management und Cloud Security Posture Management (CSPM):** Wir werden eine Single-Vendor-Lösung einsetzen, um alle Schwachstellen-Informationen in unseren Produktions- und Unternehmensumgebungen zu bündeln.
- **Verbesserung bei der Protokolldatenerfassung und bei Analysetools:** Wir werden unsere Protokollierungsmöglichkeiten erweitern, um relevantere Warnungen sowie die schnellere Untersuchung von Zwischenfällen in unserer Protokollierungs-umgebung zu ermöglichen.
- **Erweiterte Scans von Open-Source-Software (OSS):** Zur Verbesserung der allgemeinen Sicherheit werden alle Sicherheitsbibliotheken auf Lieferkettenangriffe überprüft.

Fazit

Okta hat sich das Ziel gesetzt, branchenweit führenden Schutz vor Identity-basierten Angriffen bereitzustellen. Dazu haben wir das Okta Secure Identity Commitment verfasst, das auf vier tragenden Säulen basiert:

- Wir bieten marktführende Produkte und Services für den Schutz von Identities
- Wir führen bei unseren Kunden Best Practices ein, die optimalen Schutz gewährleisten
- Wir bringen unsere Branche aktiv voran – für besseren Schutz vor Identity-basierten Angriffen
- Wir sichern die Infrastruktur unseres eigenen Unternehmens ab

Dies ist ein langfristiges Bekenntnis zu Cybersicherheit, das wir kontinuierlich weiterentwickeln und bei dem wir aktuellen Technologie- und Bedrohungstrends berücksichtigen werden.

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.