Whitepaper

Okta Secure Identity Commitment

Wir bieten markt-führende Produkte und Services für den Schutz von Identitäten

Wir härten die Infrastruktur unseres eigenen Unternehmens

Wir geben unseren Kunden die Best Practices an die Hand, die sie für einen optimalen Schutz brauchen

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

okta

Inhalt

Executive Summary

Identity ist heute der wichtigste Schlüssel zur Absicherung aller Mitarbeiter- und Kundenanwendungen. Gleichzeitig nehmen die Komplexität und Zahl der Angriffe gegen große und kleine Unternehmen immer schneller zu. Diese Angriffe frühzeitig zu erkennen und zu stoppen, ist geschäftskritisch.

Als der weltweit führende, unabhängige Identity-Anbieter steht Okta bei der Abwehr dieser Attacken 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 Identitäten
- Wir härten die Infrastruktur unseres eigenen Unternehmens
- Wir geben unseren Kunden die Best Practices an die Hand, die sie für einen optimalen Schutz brauchen
- Wir bringen unsere Branche aktiv voran – für einen besseren Schutz vor Identity-basierten Angriffen

Im Rahmen dieses Programms haben wir bereits eine Reihe wichtiger Funktionalitäten und Upgrades umgesetzt oder 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 abgeschlossen ist, und werden weiterhin strategische Investments tätigen, um der dynamischen Bedrohungslandschaft proaktiv vorzugreifen und auf sie zu reagieren.

Einführung

Als wir Okta im Jahr 2009 gründeten, konzentrierten wir uns in erster Linie auf das Management der IT – konkret darauf, wie Identitäten Menschen und Technologie zusammenbringen können.

Seitdem haben zwei wichtige Trends zu einem dramatischen Wandel in der Wahrnehmung von Identitäten und damit auch in der Nachfrage nach Identitätslösungen geführt:

1. **Identity ist heute der wichtigste Schlüssel zur Absicherung** aller Mitarbeiter- und Kundenanwendungen

2. **Volumen und Komplexität von Cyberangriffen haben zugenommen**, wobei eine Reihe von Bedrohungsakteuren – darunter Ransomware-Gruppen, staatliche Akteure und böswillige Insider – leistungsfähige Taktiken, Techniken und Prozesse (TTPs) entwickeln, um Schutzmaßnahmen zu umgehen und der Entdeckung zu entgehen

Diese Trends haben zu einem bedeutenden Wandel in der Branche geführt und uns die Verantwortung auferlegt, nicht mehr nur Menschen mit Technologie zusammenzubringen, sondern als kritischer Kontrollpunkt für den Schutz der sensiblen Daten jedes Unternehmens zu fungieren.

Und diese Verantwortung ist verankert in ***unserer Vision, jedem die Freiheit zu geben, jede Technologie sicher zu nutzen.***

Okta Secure Identity Commitment

Identitäten sind Teil der geschäftskritischen Sicherheitsinfrastruktur.

Als der weltweit führende, unabhängige 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 bösartige Anfragen*** innerhalb von 30 Tagen (Quelle: Interne Quelle von Okta - Januar 2024)

- Bei einigen unserer größten Kunden konnten wir über einen Zeitraum von 90 Tagen ***Credential-Stuffing-Angriffe und bösartigen Bot-Traffic um mehr als 90 Prozent reduzieren*** (Quelle: Okta The State of Secure Identity Report 2023)

- Wir prägen die Best Practices der Branche – 100 Prozent der Okta Mitarbeitenden nutzen ***Okta FastPass und Adaptive MFA (AMFA) als Phishing-resistente Faktoren*** (Quelle: Interne Quelle von Okta - Februar 2024)

Als einer der Marktführer in diesem Bereich haben wir es uns auf die Fahne geschrieben, Kunden zuverlässig vor Identity-basierten Angriffen zu schützen. Dieser Rolle tragen wir jetzt Rechnung – mit dem Okta Secure Identity Commitment.

Dieses Commitment beruht auf vier Säulen:

- Wir bieten marktführende Produkte und Services für den Schutz von Identitäten
- Wir härten die Infrastruktur unseres eigenen Unternehmens
- Wir geben unseren Kunden die Best Practices an die Hand, die sie für einen optimalen Schutz brauchen
- Wir bringen unsere Branche aktiv voran – für einen besseren Schutz vor Identity-basierten Angriffen

Wir bieten marktführende Produkte und Services für den Schutz von Identitäten

Wir sind uns bewusst, dass unsere Security Posture auch Ihre Security Posture ist. Aus diesem Grund sind wir bestrebt, die Security-Features unserer Identity-Produkte und -Services weiterzuentwickeln und zu priorisieren.

Durch diesen kontinuierlichen Fokus können wir das Vertrauen, das Weltmarken in uns setzen, mit den stärksten und innovativsten Schutzmaßnahmen rechtfertigen.

Wir härten die Infrastruktur unseres eigenen Unternehmens

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 Härtung unserer sekundären (d. h. produktionsnahen) und unternehmenseigenen Systeme.

Wir geben unseren Kunden die Best Practices an die Hand, die sie für einen optimalen Schutz brauchen

Eine falsch konfigurierte Identität ist nur ein weiteres Einfallstor für einen böswilligen Akteur oder Insider. Mit 15 Jahren Erfahrung und mehr als 18.000 Kunden verfügen wir über das einzigartige Know-how, um sicherzustellen, dass unsere Kunden über die richtige Identitätskonfiguration verfügen.

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

Darüber hinaus haben wir uns dazu committet, sicherzustellen, dass unsere Produkte mit den Security Best Practices von Okta implementiert werden, um direkt dazu beizutragen, die Widerstandsfähigkeit unserer Kunden gegenüber Identity-basierten Breaches zu stärken.

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

Im Bereich Identitätssicherheit führend zu sein, ist für Okta eine Selbstverständlichkeit. Wir sind darauf fokussiert, Identity-basierte Attacken zu erkennen und zu vereiteln. Wir tun dies, indem wir unsere Funktionalitäten erweitern und neue Technologien wie KI nutzen. Darüber hinaus spielen wir eine proaktive Rolle bei der Gestaltung des Identitätssicherheitsansatzes der Branche. Dazu gehört auch die Unterstützung von Okta for Good, um die digitale Transformation von gemeinnützigen Organisationen zu finanzieren und inklusive Wege in die Tech-Branche zu fördern.

Im Folgenden wird erläutert, wie wir unsere Commitments in die Tat umsetzen.

Wir bieten marktführende Produkte und Services für den Schutz von Identitäten

Auf der Oktane 2023 haben wir eine Vielzahl von Funktionalitäten angekündigt, die die Sicherheit unserer Kunden erhöhen — viele davon mit Okta AI.

Mit Blick auf die Zukunft gibt es einige zentrale Ansatzpunkte, wenn es darum geht, unsere Produkte und Services weiter zu härten:

- Strengerer Administratorzugriff in Okta Unternehmen
- Stärkerer Schutz der Tenants
- Bereitstellung von Security Best Practices für unsere Kunden

Kürzlich integriert	Für Februar 2024 geplante Features	Für Juli 2024 geplante Features
• Okta Privileged Access • Entitlement Management • Passkeys • Highly Regulated Identity • Expert Assist • Spera-Übernahme • Veränderungen beim Case-Zugriff im Okta Help Center • Authentisierung von Admin-Sessions • Management APIs - Admin-Session erforderlich für Okta-API-Calls • Und mehr...	• MFA erforderlich für den Zugriff auf die Okta Admin-Konsole • MFA erforderlich für geschützte Aktivitäten in der Admin-Konsole • Admins erhalten die Möglichkeit, Anfragen über Anonymizer zu erkennen und zu stoppen • Aktivierung von IP-Bindung an die Okta Admin-Konsole und IP- oder ASN-Bindung an die Admin-Konsole • Durchsetzung einer Allow-Listed-Network-Zone für APIs • Bereitstellung von Zero Standing Privileges für Okta-Admin-Rollen • Durchsetzung von Token-Binding für M2M-Application-Service-Integrationen • Verhinderung von Account-Lockouts für Okta-Anwender • Aktivierung von IP-Bindung für Privileged Access Management (PAM) • Und mehr...	• Device-gebundene Session-Cookies für Okta-Anwendungen • Verbesserte Bot Detection • Stärkeres Default-CAPTCHA • Erweiterte Steuerungs-optionen für das Session Management und stärkere Token-Security • Schnellere Service-Accounts in SaaS- und Hyperscaler-Umgebungen als geschützte Ressource in Okta Privileged Access • Roll-out von FastPass ausschließlich auf gemanagten Devices • Ausbau der in den Produkten verankerten Best-Practice-Guidelines • Und mehr...

Kürzlich angekündigt/integriert

Zu den kürzlich gelaunchten Produkten und Features, die die Sicherheit der Kunden erhöhen, gehören:

- **Okta Privileged Access**, das Kunden bei der Implementierung von Zero Standing Privileges und der Risikominimierung unterstützt
- **Entitlement Management** zur Minimierung potenzieller Bedrohungen durch Fehlkonfigurationen dank automatischer Erkennung und Anpassung von Berechtigungen
- **Passkeys** für einen sicheren, passwortlosen Zugriff auf Verbraucheranwendungen
- **Highly Regulated Identity** für Financial-Grade Security in Identitäts-Workflows
- **Okta Expert Assist** unterstützt Kunden aufsetzend auf dem Security-Know-how von Okta, ihre Security Posture und Konfigurationen zu stärken
- **Die Akquisition von Spera**, um die identitätsbasierte Sicherheit voranzutreiben und Unternehmen dabei zu unterstützen, Risiken zu minimieren und die Fragmentierung der Unternehmens-IT sowie Kosten zu reduzieren
- **Identity Threat Protection mit Okta AI**, *demnächst im Early Access*, mit leistungsstarken Features wie Universal Logout (z. B. als Reaktion auf Bedrohungen im Kunden-Ökosystem)

Okta Expert Assist

Kunden können gemeinsam mit Okta ihre Security Posture und Konfigurationen schrittweise weiter stärken.

So funktioniert der Okta Expert-Assist-Service:

1. **Entdecken: Setzen Sie sich mit einem Identity-Security-Experten in Verbindung**. Ihr Okta Architect führt (über Workshops) innerhalb von 2 Wochen eine umfassende Sicherheitsüberprüfung Ihrer Okta Tenants durch.
2. **Analysieren: Ihr Security-Experte definiert konkrete Maßnahmen**. Ihr Okta Architect überprüft Ihre Einstellungen ganzheitlich – auf Basis von Best Practices, die die neuesten Okta Produkt-Features und die sich ständig verändernde Bedrohungslandschaft berücksichtigen.
3. **Planung:** Stärken Sie Ihre Security Posture – heute und in Zukunft. Ihr Okta Architect liefert Ihnen priorisierte, praxisrelevante und schrittweise Guidelines, um Ihre Security Posture zu stärken und Bedrohungen einen Schritt voraus zu sein.

→ **Mehr dazu unter**: https://www.okta.com/de/expert-assist/

Weitere kürzlich gelaunchte Updates:

- **Veränderungen beim Case-Zugriff im Okta Help Center:** Admins haben im Okta Help Center nur dann Zugriff auf Support Cases, wenn sie diese eröffnet haben.

- **Authentisierung von Admin-Sessions:** Die Standardeinstellungen der Admin-Konsole sind auf eine Sitzungsdauer von 12 Stunden und eine Leerlaufzeit von 15 Minuten eingestellt. Kunden können diese Einstellungen ändern.

- **Management APIs – Admin-Session erforderlich für Okta API-Calls:** Die Best Practices von Okta sehen vor, dass Kunden API-Tokens verwenden, wenn sie API Calls automatisiert oder mit Terraform durchführen. Die Produktänderung trägt dem Rechnung und erhöht die Sicherheit der Kundenadministratoren.

Für Februar 2024 geplante Features:

- **MFA erforderlich für den Zugriff auf die Okta Admin-Konsole:** Okta erzwingt MFA für alle Okta-Admin-Rollen und verbessert so den sicheren Zugriff auf die Okta Admin-Konsole. MFA für die Admin-Konsole bietet eine zusätzliche Sicherheitsebene, die die Wahrscheinlichkeit von Breaches reduziert. Wir verfolgen einen schrittweisen Ansatz, bei dem in der ersten Phase verhindert wird, dass neue Authentisierungsrichtlinien für Admin-Apps ohne MFA definiert werden.

- **MFA erforderlich für geschützte Aktivitäten in der Admin-Konsole:** Ziehen Sie eine zusätzliche Sicherheitsebene für kritische Aktionen in Okta ein, indem Sie eine Step-up-Authentisierung für Admins erzwingen.

- **Admins erhalten die Möglichkeit, Anfragen über Anonymizer zu erkennen und zu stoppen:** Okta wird Administratoren die Möglichkeit geben, den Zugriff basierend darauf zu erlauben oder zu verweigern, ob eine IP-Adresse mit Anonymizers assoziiert ist. Dies ermöglicht es Unternehmen, den unbefugten Zugriff über solche Quelle zu unterbinden.

- **Aktivierung von IP-Bindung an die Okta Admin-Konsole und IP- oder ASN-Bindung an die Admin-Konsole:** Um mögliche Session-Takeovers zu verhindern, wird Okta eine Okta Admin-Console-Session automatisch abbrechen, wenn die ASN (Autonomous System Number), die während einer API- oder Web-Anfrage beobachtet wird, von der ASN abweicht, die zu Beginn der Session aufgezeichnet wurde. Bei den folgenden Okta Produkten werden Kundenadministratoren in der Lage sein, eine Admin-Session automatisch abzubrechen, wenn sich die beobachtete IP-Adresse während einer aktiven Session ändert: Workflows Admin, Okta Access Requests (Inbox), Okta Privileged Access (OPA), Okta Admin Console.

- **Durchsetzung einer Allow-Listed-Network-Zone für APIs:** Verhindern Sie, dass Angreifer und Malware SSWS-Tokens stehlen und außerhalb des spezifizierten IP-Bereichs wiederverwenden, um sich unberechtigten Zugriff zu verschaffen.

- **Bereitstellung* von Zero Standing Privileges für Okta-Admin-Rollen:** Managen Sie Okta-Admin-Rollen mit Okta Identity Governance (OIG). Indem Okta Zugriffsanfragen und Zertifizierungen für Adminrechte erzwingt, schützen wir Kunden vor Insider-Bedrohungen und unberechtigtem Zugriff und ermöglichen Least Privilege Access.

* Early Access (EA) für OIG-Kunden ab Februar 2024 und EA für weitere Kunden ab März

Für Februar 2024 geplante Features:

- **Durchsetzung von Token-Binding für M2M-Application-Service-Integrationen:** Okta erhöht die Sicherheit von automatisierten Transaktionen und erzwingt standardmäßig Token-Bindung via Proof-of-Possession in Machine-to-Machine-Integrationen (M2M), um sicherzustellen, dass nur authentisierte Anwendungen Tokens für den Zugriff auf Okta APIs verwenden können.

- **Verhinderung von Account-Lockouts für Okta-Anwender**: Okta bietet die Möglichkeit, verdächtige Login-Versuche von unbekannten Geräten zu blockieren. Wenn das Feature aktiviert ist, verhindert es, dass legitime User (einschließlich Admins) blockiert werden, wenn ein anderes, Okta unbekanntes Gerät einen Lockout verursacht.

- **Aktivierung von IP-Bindung für Privileged Access Management (PAM):** Kundenadministratoren können eine Admin-PAM-Session automatisch abbrechen, wenn die IP-Adresse, die während einer API- oder Web-Anfrage beobachtet wird, von der IP-Adresse abweicht, die zu Beginn der Session aufgezeichnet wurde. Um diese Funktionalität zu deaktivieren, ist ein Support-Ticket notwendig.

Für Juli 2024 geplante Features:

- **Device-gebundene Session-Cookies für Okta-Anwendungen:** Device-gebundene Session-Cookies werden weiter dazu beitragen, das Replay von Okta Sessions zu verhindern, indem sie einen Proof-of-Possession für einen Private Key erzwingen, der auf dem Gerät des Users gespeichert ist. Diese Challenge schafft eine starke Verbindung zwischen Session und Gerät und reduziert das Risiko von Token-Diebstahl oder Replay-Angriffen.

- **Verbesserte Bot Detection:** Einführung einer zusätzlichen Bot-Detection- und Bot-Protection-Ebene unter Verwendung von Third-Party-Scores und Edge-basierten Komponentensignalen.

- **Stärkeres Default-CAPTCHA:** Standardmäßig führen Events, die ein CAPTCHA in der Okta Customer Identity Cloud auslösen, zu Challenges, deren Komplexität proportional zum beobachteten Risiko ist.

- **Erweiterte Steuerungsoptionen für das Session-Management und stärkere Token-Security:** Vollständige programmatische Steuerungsoptionen für das Session-Management ermöglichen es Kunden, ihre eigenen Session-Control-Dashboards zu erstellen und die User Experience maßzuschneidern.

- **Schnellere Service-Accounts in SaaS- und Hyperscaler-Umgebungen** als geschützte Ressource in Okta Privileged Access.

- **Roll-out von FastPass ausschließlich auf gemanagten Devices:** Okta bietet Administratoren mehr Kontrolle, indem es das Pre-Enrollment von Usern in Okta Verify und FastPass über eine Mobile-Device-Management-Lösung (MDM) ermöglicht. So können Kunden Authenticator Enrollments auf gemanagte Geräte beschränken.

- **Ausbau der in den Produkten verankerten Best-Practice-Guidelines:** Okta wird zusätzliche In-Product-Guidelines zur Verfügung stellen, um Kunden bei der Implementierung von Best Practices zum Schutz ihrer Okta Tenants zu unterstützen.

Wir härten die Infrastruktur unseres eigenen Unternehmens

Wir investieren verstärkt in die Härtung unserer sekundären (produktionsnahen) und unternehmenseigenen Systeme.

Kürzlich integriert	Für April 2024 geplante Updates	Für Juli 2024 geplante Updates
• Entziehen des persönlichen Zugriffs auf Google Chrome Accounts • Erhöhung des Monitoring- und Detection-Levels für alle Service-Accounts • Bereinigung von HAR-Dateien im Okta Help Center zur Erkennung sensibler Daten • Härtung des Quellcode-Managements und Datenbank-Monitorings	• Ausweitung der Phishing-Resistenz auf den gesamten Employee Lifecycle • Automatisiertes Erkennen und Reporten von M2M-Service-Accounts in SaaS-Anwendungen • Durchführung eines internen Security-Assessments • Durchführung eines Security-Assessments für SaaS-Anwendungen	• Verbesserte Detection-and-Response-Fähigkeiten • Standardisiertes und zentralisiertes Vulnerability Management, Asset Management und CSPM • Standardisiertes und zentralisiertes Reporting für das Security-Risk-Management • Verbesserter Schutz von Laptops • Verbesserter Schutz mobiler Geräte

Kürzlich integriert

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

- Entziehen des persönlichen Zugriffs auf Google Chrome Accounts
- Erhöhung des Monitoring- und Detection-Levels für alle Service-Accounts
- Bereinigung von HAR-Dateien (HTTP-Archive-Format) im Okta Help Center zur Erkennung sensibler Daten (z. B. Session-Tokens)
- Härtung des Quellcode-Managements und Datenbank-Monitorings

Für April 2024 geplante Updates:

- **Ausweitung der Phishing-Resistenz auf den gesamten Employee Lifecycle:** Wir setzen Okta FastPass seit langem für Phishing-resistente MFA ein – und werden Phishing-Resistenz über den gesamten Employee Lifecycle hinweg implementieren, vom Enrollment/Onboarding bis zur Recovery.
- **Automatisiertes Erkennen und Reporten von M2M-Service-Accounts in SaaS-Anwendungen:** Wir werden ein Tool implementieren, das Transparenz über lokale Service-Accounts bietet, die innerhalb von SaaS-Anwendungen erstellt wurden, um die zur Authentisierung verwendeten Secrets besser managen und rotieren zu können.
- **Durchführung eines internen Security-Assessments:** Wir arbeiten mit einem führenden globalen Beratungsunternehmen zusammen, um eine umfassende Sicherheitsüberprüfung unserer Produkte, Infrastruktur und Unternehmenssysteme durchzuführen.
- **Durchführung eines Security-Assessments für SaaS-Anwendungen:** Wir arbeiten mit Third-Party-Sicherheitsexperten zusammen, um Security-Assessments unserer kritischen SaaS-Anwendungen, einschließlich des Okta Help Centers, durchzuführen.

Für Juli 2024 geplante Updates:

- **Verbesserte Detection-and-Response-Fähigkeiten:** Wir werden Lösungen implementieren, um unsere Detection-and-Response-Fähigkeiten zu verbessern – darunter ein neues Security-Incident-Case-Management-Tool, eine neue Threat-Intelligence-Plattform und zusätzliches Dark-Web-Monitoring.
- **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.
- **Standardisiertes und zentralisiertes Reporting für das Security-Risk-Management:** Wir werden eine Single-Vendor-Lösung einsetzen, um das Risk-and-Issue-Management im Zusammenhang mit unserem Governance-, Risiko- und Compliance-Programm zu zentralisieren – einschließlich Third-Party-Risk-Management.
- **Verbesserter Schutz von Laptops:** Wir werden die Nutzung von Okta Laptops durch unsere Mitarbeitenden weiter einschränken: Wir haben allen Mitarbeitenden des Unternehmens den lokalen Admin-Zugriff entzogen und planen, diesen auch bis dato ausgenommenen Entwicklern und Ingenieuren zu entziehen.
- **Verbesserter Schutz mobiler Geräte:** In puncto Mobile Device Security werden wir eine harte Linie fahren. Während Okta Verify bereits für eine robuste Device Security Posture sorgt – z. B. durch PIN, Verschlüsselung und Checks der Betriebssystemversion – werden wir für den Zugriff auf unsere Unternehmensanwendungen zusätzlich MDM-Software einsetzen.

Wir geben unseren Kunden die Best Practices an die Hand, die sie für einen optimalen Schutz brauchen

Wir konzentrieren uns darauf, Best Practices für unsere Branche zu optimieren, um mit der Bedrohungslandschaft Schritt zu halten.

- **Phishing-resistente Faktoren:** 100 Prozent der Okta Mitarbeitenden nutzen Okta FastPass und AMFA als Phishing-resistente Faktoren. Wir empfehlen unseren Kunden, Phishing-resistente Faktoren nach Möglichkeit auch in ihren Identity Stack zu integrieren.
- **MFA-Enrollment und Self-Service:** Wir tragen der Bedeutung von MFA Rechnung und konzentrieren uns darauf, unseren Kunden Transparenz über alle MFA-Enrollments (Admins + User) sowie die Möglichkeit zum Self-Service-Enrollment zu bieten.
- **Maßgeschneiderte Expertenunterstützung:** Wir haben Okta Expert Assist gelauncht, um Kunden mit unserem Security-Know-how dabei zu unterstützen, ihre Security Posture und Konfigurationen zu stärken. Wir empfehlen unsere Kunden, dieses Angebot in Anspruch zu nehmen und sich maßgeschneiderte Empfehlungen einzuholen.
- **Awareness und Training:** Wir intensivieren das Phishing-Awareness-Training und setzen Phishing-resistente Authentisierungsmethoden ein.
- **Ausbau der in den Produkten verankerten Best-Practice-Guidelines:** Wir werden zusätzliche In-Product-Guidelines bereitstellen, um Kunden mit Best Practices für den Schutz ihrer Okta Tenants zu unterstützen.

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

Zu den jüngsten Okta for Good-Initiativen zur Förderung der Cybersecurity-Branche gehören:

- Das **NetHope Global Humanitarian Information Sharing & Analysis Center** (ISAC) wurde als öffentlich-private Partnerschaft zwischen NetHope, USAID und Okta ins Leben gerufen, um globale humanitäre NGOs im Kampf gegen die zunehmenden Cyberbedrohungen zu unterstützen
- **Cybersecurity Futures 2030:** Okta hat dieses globale Forschungsprojekt in Zusammenarbeit mit dem UC Berkeley Center for Long-Term Cybersecurity und dem Centre for Cybersecurity des Weltwirtschaftsforums finanziert. Ziel ist es, neu aufkommende Cybersecurity-Trends und -Risiken für Regierungen, Industrie und Zivilgesellschaft zu identifizieren und eine bessere Zusammenarbeit bei der Bewältigung dieser zukünftigen Herausforderungen zu ermöglichen
- Die **Cybersecurity Workforce Development Initiative** bietet philanthropische und bildungsbezogene Zuschüsse, um inklusive Wege in die Tech- und Cyber-Branche zu fördern und Qualifikationslücken zu schließen
- Das **Nonprofit Cybersecurity Grant Portfolio** hat über einen Zeitraum von zwei Jahren mehr als 1 Million US-Dollar zur Förderung besserer Cybersicherheitspraktiken in gemeinnützigen Organisationen bereitgestellt

Fazit

Okta hat es sich auf die Fahne geschrieben, Kunden zuverlässig vor Identity-basierten Angriffen zu schützen. Dem tragen wir mit dem Okta Secure Identity Commitment Rechnung. Es basiert auf vier tragenden Säulen:

- Wir bieten marktführende Produkte und Services für den Schutz von Identitäten
- Wir härten die Infrastruktur unseres eigenen Unternehmens
- Wir geben unseren Kunden die Best Practices an die Hand, die sie für einen optimalen Schutz brauchen
- Wir bringen unsere Branche aktiv voran – für einen besseren Schutz vor Identity-basierten Angriffen

Dies ist ein langfristiges Commitment – und wir werden es kontinuierlich weiterentwickeln und an aktuellen Technologien und Threat-Landschaften ausrichten.

Über Okta
Okta ist das weltweit führende Identity-Unternehmen. Als der führende unabhängige Identity-Partner ermöglichen wir es jedermann, jede Technologie sicher zu nutzen – überall, mit jedem Device und jeder App. Die weltweit renommiertesten Marken vertrauen beim Schutz von Zugriff, Authentisierung und Automatisierung auf Okta. Im Mittelpunkt unserer Okta Workforce Identity und Customer Identity Clouds stehen Flexibilität und Neutralität. Mit unseren individualisierbaren Lösungen und unseren über 7.000 schlüsselfertigen Integrationen können sich Business-Verantwortliche 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.