Whitepaper

Die Anatomie Identity-basierter Angriffe

So stoppen Sie Bedrohungen für ihre Benutzer

Inhalt

Die Rolle der Identity in der Sicherheit

Bislang war Identity-Management im Rahmen einer unternehmensweiten Sicherheitsstrategie darauf beschränkt, die Identität des Benutzers zum Authentifizierungszeitpunkt zu überprüfen und den jeweils richtigen Zugriff zu gewähren. Da Angreifer jedoch zunehmend Benutzer und ihre Anmeldedaten ins Visier nehmen, decken die Sicherheitsfunktionen von Systemen zur Identitäts- und Zugriffsverwaltung (Identity and Access Management, IAM) mittlerweile auch diese Bedrohungen ab. Digitale Identitäten (Identities) sind auch ein zentraler Bestandteil von Zero-Trust-Strategien, mit denen Sicherheitsverantwortliche den Schutz ihrer Umgebungen stärken wollen.

Mittlerweile sind Identities zu einem Kernelement in der Cybersicherheitsstrategie aller Unternehmen geworden. Angesichts von Homeoffice-Arbeit, nicht verwalteten Geräten und Cloud- sowie SaaS-Umgebungen sind Identities das einzige Bindeglied zwischen Mitarbeitern und den für ihre Arbeit notwendigen Geräten, Anwendungen und Ressourcen. Die eigentliche Verbindung wird dabei von Identity-Anbietern bereitgestellt.

Identities sind die einzige Technologie, die IT-übergreifend integriert ist und einen kollaborativen IT-Sicherheitsansatz ermöglicht. Okta Workforce Identity Cloud kann mithilfe eigener und externer Sicherheitskontrollen Risiken bewerten, Bedrohungen abwehren und die Cybersicherheit verbessern. Dieser Identity-basierte Sicherheitsansatz bietet folgende Vorteile:

- Vereinheitlichung und Stärkung von Identity-Richtlinien, Transparenz und Kontrolle mit einer Plattform, die IAM, IGA (Identity Governance and Administration) und PAM (Privileged Access Management) zusammenführt
- Erkennung von unternehmensspezifischen Risiken, wobei die Lösung eigenständig agiert oder mit bereits vorhandenen Sicherheitsprodukten zusammenarbeitet
- Kontinuierliche Bewertung von Risiken vor, während und nach der Benutzerauthentifizierung
- Reaktion auf Bedrohungen auf Grundlage von Echtzeitinformationen

Dieses Whitepaper erläutert die folgenden aktuell wachsenden Bedrohungen für Unternehmen und zeigt, wie Okta diese Bedrohungen vor, während und nach der Authentifizierung erkennen und abwehren kann.

- Phishing
- Kompromittierung von Endbenutzergeräten
- Insider-Bedrohungen
- Bedrohungen nach der Authentifizierung
- Brute-Force-Angriffe

Statistiken zu Identity-Sicherheit

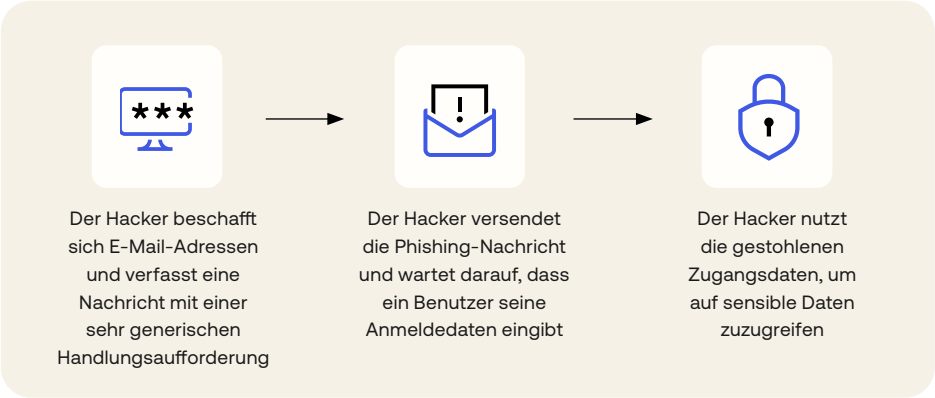
- Angreifer nutzten **2022** bei **45 %** aller Datensicherheitsverstöße gestohlene Anmeldedaten, während es im Jahr zuvor noch **42 %** waren.[1]
- **74 %** aller Sicherheitsverletzungen gehen mit einer menschlichen Komponente einher, seien es Fehler, Missbrauch von Berechtigungen, Nutzung gestohlener Anmeldedaten oder Social Engineering.[1]
- **86 %** aller Datenschutzverletzungen bei Web-Anwendungen gehen mit gestohlenen Anmeldedaten einher.[1]

[1] 2023 Verizon Data Breach Investigations Report

Phishing

Phishing-Betrug ist die häufigste Form von Cyberkriminalität in den USA und verursacht bei den Opfern die höchsten finanziellen Schäden.[2] Damit die Angreifer ihre Phishing-Attacken in großem Maßstab durchführen können, setzen sie auf KI und Automatisierung, was die Erkennung und Blockierung erschwert. Die meisten Phishing-Angriffe beginnen mit E-Mails, die Benutzer zum Eingeben ihrer Anmeldedaten auf einer gefälschten Website verleiten sollen. Dabei können diese E-Mails und Websites dank richtigem Branding und Sprachstil sehr überzeugend sein und E-Mail-Adressen nutzen, die den tatsächlichen Adressen sehr ähnlich sehen. Sobald dem Angreifer die Benutzeranmeldedaten in die Hände gefallen sind, kann er sich damit anmelden. Auf diese Weise öffnet sich eine Hintertür, durch die größere Angriffe gestartet werden können. Dazu gehören beispielsweise:

- Installieren von Ransomware in Unternehmenssystemen, um Lösegeldzahlungen zu erpressen
- Betrugsversuche mit Business Email Compromise (BEC), um Gelder an ein von den Angreifern kontrolliertes Bankkonto zu überweisen, z. B. durch die Änderung der Kontonummern für Gehaltszahlungen oder Rechnungen
- Durchsuchen von Anwendungen nach vertraulichen Daten, die sich im Dark Web verkaufen lassen



Unternehmen investieren viel Geld in Spam-Filter, E-Mail-Sicherheits-software, Virenschutz, Web-Filter und Benutzerschulungsprogramme, um sich vor den mehr als 156 Millionen Phishing-E-Mails zu schützen, die jeden Tag weltweit versendet werden. Die inzwischen immer raffinierteren Angriffe können diese klassischen Sicherheitsmaßnahmen jedoch zunehmend umgehen. Ebenso galt Multi-Faktor-Authentifizierung (MFA) bisher als Goldstandard zum Verhindern von Anmeldedaten-Diebstahl einschließlich Phishing. Doch aktuelle vielbeachtete Angriffe haben gezeigt, dass MFA allein nicht mehr alle Datensicherheitsverstöße verhindern kann, da diese Technik für AitM-Angriffe (Adversary-in-the-Middle), SIM-Kartentausch, Pass-the-Cookie, MFA Fatigue und MFA-Bombing-Angriffe (x-fach wiederholte MFA-Push-Benachrichtigungen) anfällig ist. MFA ist nur dann wirksam, wenn die eingesetzten Methoden zuverlässig vor Umgehungen und Hacking geschützt sind.

[2] Federal Bureau of Investigation Internet Crime Report 2022

Strategien zur Behebung

1. **Benutzertools und -schulungen:** Da Benutzer mit Phishing angegriffen werden können, müssen sie über Schutztools verfügen.

    a. Führen Sie mit Okta Workflows simulierte Phishing-Kampagnen durch, bei denen gefälschte MFA-Abfragen versendet werden, um die Benutzer zu MFA Fatigue zu schulen.

    b. Mit Okta HealthInsight können Sie Endbenutzer ganz einfach über Authentifizierungsänderungen in ihren Accounts informieren. Mit dieser Funktion ist es für Benutzer zudem einfacher, verdächtige Authentifizierungsereignisse zu melden.

2. **Zugriff nach dem Least-Privilege-Prinzip:** Okta Identity Governance (OIG) bietet Zugriffskontrollen, die Benutzerzugriffe auf die Ressourcen beschränken, die sie für ihre aktuelle Rolle bzw. ein laufendes Projekt benötigen. Dadurch wird das Risiko lateraler Bewegungen bei erfolgreichem Phishing oder Social Engineering verringert. Ebenso automatisiert und verwaltet OIG die Joiner-, Mover- und Leaver-Prozesse in Cloud- und On-Premise-Ressourcen und zertifiziert regelmäßig den Zugriff. Durch diese Automatisierung wird das Risiko minimiert, dass Angreifer inaktive Accounts für Phishing-Angriffe missbrauchen oder Zugriff erlangen.

3. **Step-up-Authentifizierung:** Die Verhaltenserkennung von Okta Adaptive MFA analysiert das Benutzerverhalten und erstellt basierend auf früheren Aktivitäten Profile typischer Verhaltensmuster. Sie können Richtlinien konfigurieren, die automatisch auf verändertes Benutzerverhalten reagieren und beispielsweise einen zusätzlichen Faktor anfordern, wenn ein Benutzer versucht, sich aus einem anderen Land oder mit einer anderen IP-Adresse anzumelden.

4. **Phishing-sichere Authentifizierung:** Bei der Phishing-resistenten Authentifizierung wird auf Shared Secrets wie Sicherheitsfragen verzichtet. Auf diese Weise soll die MFA-Umgehung verhindert und sichergestellt werden, dass Benutzer keine Anmeldedaten bei gefälschten Domänen eingeben können. Okta unterstützt dabei folgende Optionen:

    a. Alle wichtigen Phishing-resistenten Authentifizierungsverfahren, darunter alle FIDO 2-WebAuthn-Optionen und PIV/CAC-Smartcards

    b. Okta FastPass, eine Phishing-resistente und passwortlose Zero-Trust-Authentifizierungslösung für verwaltete und unverwaltete Geräte

5. **Bedrohungserkennung:** Security-Teams können Okta-Integrationen mit führenden E-Mail-Anbietern nutzen und risikobasierte adaptive Authentifizierungsrichtlinien einrichten. So ist es mit Okta-Richtlinien beispielsweise möglich, als Reaktion auf Bedrohungen auf E-Mail-Ebene die Authentifizierung zu verschärfen oder User Accounts zu sperren. Okta Identity Threat Protection mit Okta AI nutzt Sicherheitsinformationen aus verschiedenen Sicherheitslösungen, darunter auch E-Mail-Sicherheitsanbieter. Wenn diese Anbieter eingehende Phishing-E-Mails oder schädliche Links registrieren, können sie Okta warnen, damit die Risikostufe des betreffenden Benutzers erhöht und entsprechende Inline-Reaktionen ausgelöst werden.
6. **Bedrohungsabwehr:** Abgesehen von der Bedrohungserkennung koordiniert Okta Identity Threat Protection maßgeschneiderte Reaktionsmaßnahmen basierend auf konfigurierten Richtlinien und ermittelten Benutzerrisikostufen. Beispielsweise kann Identity Threat Protection bei einer mittleren Risikostufe das SIEM- oder Incident Response-Team benachrichtigen, während bei einem hohen Risiko die erneute Benutzerauthentifizierung ausgelöst, eine Benutzersitzung beendet oder Benutzer sogar von unterstützten Anwendungen abgemeldet werden.

Kompromittierung von Endbenutzer-geräten

Homeoffice-Arbeit und BYOD haben neuen Bedrohungen die Tür zu Benutzer-Smartphones, Laptops und anderen Geräten geöffnet. Da sich Phishing-resistente Authentifizierung immer weiter durchsetzt, können Angreifer kompromittierte Geräte als Zugang zu Ihrem Unternehmen wählen.

Cyberangriffe beginnen häufig mit der Kompromittierung eines Endbenutzergeräts, zum Beispiel nachdem der Benutzer zum Installieren einer Malware verleitet wurde. Diese Malware kann anschließend Anmeldedaten stehlen und dem Angreifer (ebenso wie beim Phishing) die Möglichkeit geben, sich lateral im Unternehmen zu bewegen und Ransomware zu verteilen, vertrauliche Daten zu exfiltrieren oder eine BEC-Attacke zu starten. Identity-Management kann die Prävention und Erkennung einiger Endpoint-Angriffe unterstützen, da zusätzliche Sicherheitsmaßnahmen für die Geräte implementiert und Geräte vor und nach der Authentifizierung überprüft werden.

Strategien zur Behebung

1. **Device Trust:** Mit Device Trust wird gewährleistet, dass nur Benutzer mit vertrauenswürdigen und verwalteten Geräten auf Ihre Umgebung zugreifen können. Bei Okta wird Device Trust dadurch sichergestellt, dass jedes verwaltete Gerät angemessen abgesichert ist, bevor Benutzer sich anmelden dürfen. Die Okta Verify-App integriert sich in Lösungen für Mobile Device Management (MDM) sowie Endpoint Detection and Response (EDR) und erfasst während der Anmeldung Informationen über das Gerät. Auf Grundlage dieser Indikatoren sowie Ihrer eigenen Richtlinien entscheidet Okta über die Gewährung des Zugriffs.
2. **Device Assurance:** Bei nicht verwalteten Geräten oder verwalteten Geräten ohne MDM oder EDR kann Okta Verify Statusprüfungen vornehmen und Zugriffsentscheidungen anhand Ihrer Richtlinien treffen. So könnten Sie beispielsweise Datenträgerverschlüsselung und eine aktuelle Betriebssystemversion vorschreiben oder Geräte mit Jailbreak verbieten. Nach der Authentifizierung kann FastPass im Hintergrund bei jedem Öffnen einer neuen Anwendung eine Geräteüberprüfung durchführen. Je nach Ergebnis kann FastPass eine erneute Authentifizierung anfordern oder den Zugriff auf die Anwendung sperren.
3. **Zugriffsschutz für Geräte:** Okta Device Access erweitert die sicheren MFA-Prozesse auf die Desktop-Anmeldung und bietet dadurch zusätzlichen Schutz für diese Geräte. Device Access kann die Benutzeridentität überprüfen und sogar ohne eine Internetverbindung Zugriffsentscheidungen treffen.

4. **Filter für vertrauenswürdige Anwendungen:** Administratoren können mit einer Allow-Liste verhindern, dass schädliche oder nicht überprüfte Anwendungen auf Benutzergeräten FastPass für unbefugten Zugriff missbrauchen.
5. **Erkennung und Abwehr von Bedrohungen:** Okta Identity Threat Protection integriert sich mit führenden EDR-Anbietern und ermöglicht Malware-Gerätescans und Abwehrmaßnahmen. Abhängig von der Echtzeit-Risikobewertung durch Identity Threat Protection können beispielsweise erneute Authentifizierungen erzwungen oder Benutzer mit kompromittierten Geräten abgemeldet werden, wobei diese Reaktionen automatisiert erfolgen.

Insider-Bedrohungen

Insider-Bedrohungen nehmen stetig zu und sind teilweise mit böswilligen Absichten verbunden, z. B. im Fall von Diebstahl von Informationen oder Sabotage. Fakt ist jedoch, dass 55 % aller Insider-Zwischenfälle durch fahrlässiges Verhalten von Mitarbeitern verursacht werden, sei es die fehlende Absicherung von Geräten, die fehlende Installation von Sicherheitsupdates oder Verstöße gegen Sicherheitsrichtlinien des Unternehmens. Andere Insider-Bedrohungen sind beispielsweise echte Versehen oder Vorfälle, bei denen Benutzer mit neuen Angriffstaktiken getäuscht wurden. Im vergangenen Jahr dauerte es im Schnitt 86 Tage, um einen Insider-Vorfall einzudämmen. Die durch Insider-Risiken entstehenden Kosten pro Unternehmen stiegen durchschnittlich auf 16,2 Millionen US-Dollar.[3]

Bei einem Insider-Risiko-Management-Programm spielt die Benutzeridentität eine wichtige Rolle. So nutzen beispielsweise 56 %[3] aller Unternehmen PAM-Lösungen (Privileged Access Management), um die Gefahr zu minimieren, dass Insider versehentlich oder mit böswilliger Absicht auf privilegierte Anmeldedaten und Accounts zugreifen können. Auch IGA-Systeme können die Schäden durch Insider-Bedrohungen für ein Unternehmen eindämmen.

[3] Cost of Insider Risks Global Report, 2023

Strategien zur Behebung

1. **Zugriffsschutz für Geräte:** Wenn ein Insider einen Laptop verliert oder an einer nicht gesicherten Stelle zurücklässt, verhindert Device Access auch ohne Internetverbindung, dass unbefugte Benutzer Zugriff auf die Gerätedaten erhalten.

2. **Zugriff nach dem Least-Privilege-Prinzip:** Mit Okta Identity Governance können Unternehmen gewährleisten, dass Insider nur auf die Anwendungen und Ressourcen zugreifen können, die für ihre Rolle und das aktuelle Projekt erforderlich sind. Dadurch wird das Risiko minimiert, dass Benutzer unbefugten Zugriff auf wertvolle Informationen erhalten. Administratoren können festlegen, dass Zugriffsrechte nach einer gewissen Zeit ablaufen, oder Zertifizierungskampagnen durchführen, um den zulässigen Zugriff sicherzustellen.

3. **Privileged Account Access:** Verhindern Sie, dass Insider unbefugt auf vertrauliche Daten zugreifen können. Okta Privileged Access schützt wichtige Ressourcen, indem dauerhafte Zugriffsrechte beseitigt, gemeinsam genutzte Accounts abgesichert und die Aktivitäten der Benutzer lückenlos dokumentiert werden. Okta verbindet wichtige PAM-Funktionen mit IAM und Identity Governance in einer einzigen Plattform. Dadurch wird die Transparenz verbessert und die Durchsetzung von Richtlinien für privilegierte Konten und Ressourcen vereinfacht. Dieser einheitliche Ansatz macht isolierte IAM-, IGA- und PAM-Tools überflüssig und stärkt die Sicherheit. Verhaltensweisen oder Signale, die zur Erhöhung der Benutzerrisikostufen in IAM führen, werden automatisch an Okta Privileged Access übertragen, damit die Lösung Maßnahmen ergreifen kann, die das Risiko durch böswillige oder fahrlässige Insider mit erweiterten Berechtigungen verringern.

4. **Bedrohungserkennung:** In manchen Fällen missbrauchen autorisierte Benutzer die Ressourcen des Unternehmens. Okta Identity Threat Protection mit Okta AI integriert sich mit anderen Sicherheitstools wie EDR-Lösungen, CASBs (Cloud Access Security Broker) und SIEM-Systemen. Diese Anwendungen identifizieren verdächtiges Verhalten (z. B. das Herunterladen zahlreicher Dateien aus einem Directory) und benachrichtigen Okta bei erhöhten Benutzerrisiken.

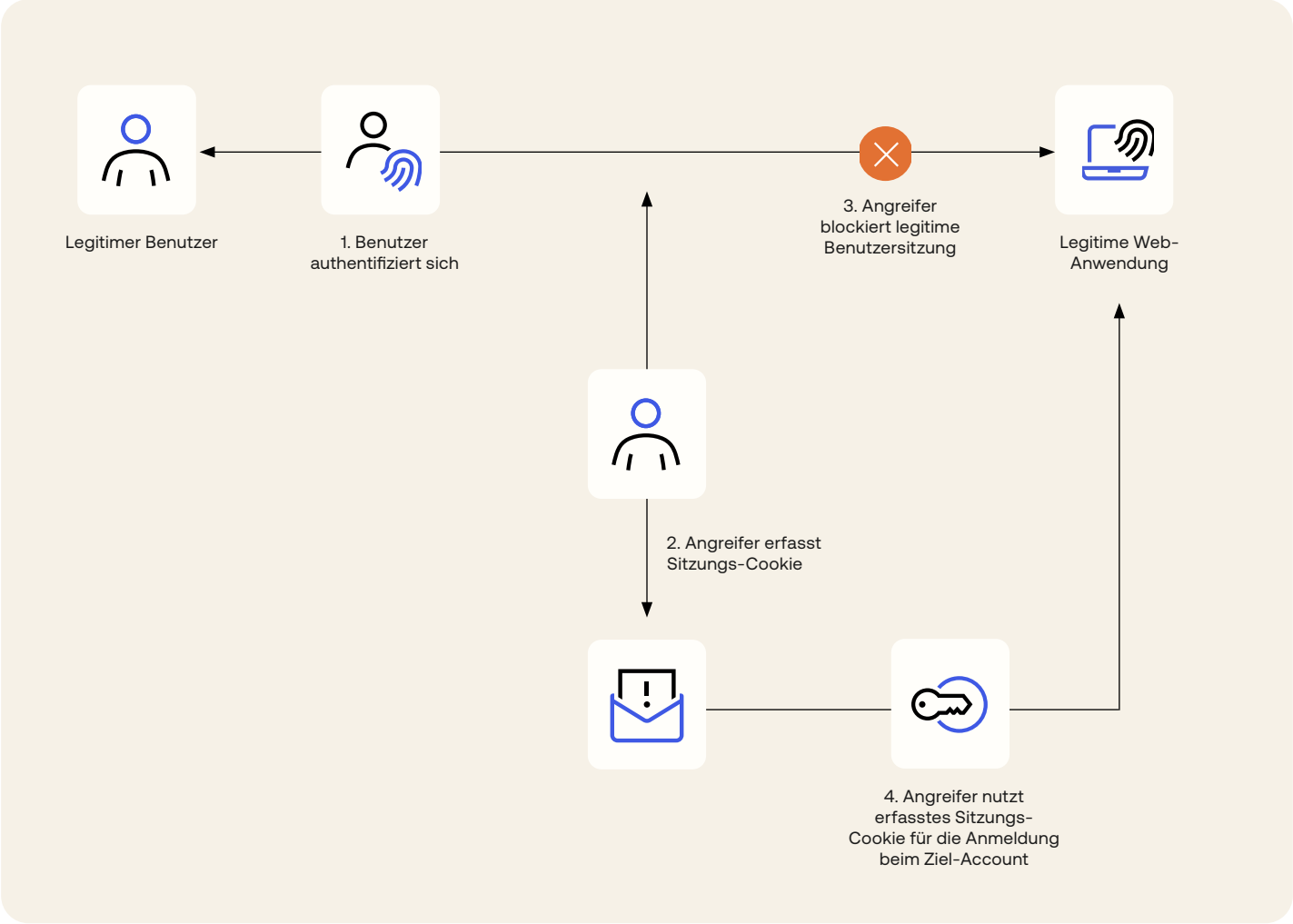
5. **Bedrohungsabwehr:** Wie bei anderen Angriffen auch kann Okta automatisch auf erhöhte Benutzerrisiken reagieren und eine erneute Authentifizierung anfordern, den Zugriff beschränken oder Benutzer von unterstützten Anwendungen abmelden.

Bedrohungen nach der Authentifizierung

Die Absicherung der ersten Anmeldung ist nicht mehr ausreichend. Der Diebstahl von Anmeldedaten zum Anmeldezeitpunkt wird durch die zunehmende Verbreitung von Multi-Faktor- und Phishing-resistenter Authentifizierung für Angreifer immer schwieriger. Das wird zunehmend dazu führen, dass Benutzer und ihre Geräte nach erfolgter Authentifizierung angegriffen werden. Mehrere bekannt gewordene Sicherheitsverletzungen haben die Möglichkeit solcher Angriffe demonstriert.

Session Hijacking

Nach erfolgreicher Authentifizierung eines Benutzers bei einem Anwendungsserver generiert dieser ein Sitzungs-Token oder Cookie, das im Browser des Benutzers gespeichert wird. Beim Session Hijacking kann dieses Sitzungs-Token mit Methoden wie Cross-Site-Scripting (XSS), Malware-Installation oder Session Sniffing gestohlen werden. Mit einem gültigen Sitzungs-Token verfügt der Angreifer in der Anwendung über die gleichen Möglichkeiten wie ein legitimer Benutzer.



Strategien zur Behebung

1. **Konfigurationen zur Risiko-Minimierung:** Okta erlaubt eine Reihe von Konfigurationen, mit denen das Risiko gestohlener Sessions minimiert wird:

    a. Sie können festlegen, dass Benutzersitzungen nach einer bestimmten Zeit oder nach einer bestimmten Phase der Inaktivität ablaufen, sodass für Angreifer die Zeit verkürzt wird, in der sie Sitzungs-Token stehlen oder gestohlene Token missbrauchen können.

    b. Okta Identity Governance kann Benutzern je nach ihren Rollen oder Projekten detaillierte Anwendungsberechtigungen zuweisen. Dadurch wird der Handlungsspielraum von Angreifern mit einer Anwendung begrenzt, was die potenziellen Risiken durch gestohlene Sitzungs-Cookies minimiert.

    c. Sie können mit einer Authentifizierungsrichtlinie festlegen, dass Benutzer sich bei jedem Zugriff auf eine neue Anwendung neu authentifizieren müssen. Passwortlose Authentifizierung per FastPass minimiert den Aufwand für Benutzer.

2. **Zusätzliche VPN-Sicherheit:** Virtuelle private Netzwerke (VPNs) verhindern zuverlässig Session Sniffing. VPNs erfordern jedoch oft Benutzernamen und Passwort, die sich leicht angreifen lassen. Daher integriert sich Okta mit vielen VPN-Anbietern und stellt eine zusätzliche Sicherheitsebene mit MFA oder Phishing-resistenter MFA bereit, um das Risiko erfolgreicher Sniffing-Angriffe in öffentlichen WLAN-Netzwerken zu minimieren.

3. **Session-Risikoanalyse:** Nach erfolgreicher Authentifizierung überwacht Okta Identity Threat Protection die Benutzersitzungen kontinuierlich auf verdächtiges oder ungewöhnliches Verhalten. Die Verhaltensanalysen werden von Analysesystemen bereitgestellt. Okta Identity Threat Protection erhält Sicherheitsindikatoren von Okta Verify und anderen externen Sicherheitstools und bietet so eine Echtzeit-Übersicht über alle Session-Risiken.

4. **Kontext-Neubewertung:** Bei Unternehmen mit einem heterogenen Gerätebestand führt FastPass im Hintergrund Statusprüfungen durch, sobald ein authentifizierter Benutzer eine neue Anwendung öffnet. Dadurch wird zusätzlich geprüft, dass das Gerät und seine Sicherheitseinstellungen vor der Zugriffsgewährung nicht verändert wurden, was die Gefahr von Session Hijacking minimiert.

5. **Privilegierte Accounts:** Okta Privileged Access minimiert die Angriffsfläche von Session-Attacken, da der Zugriff auf privilegierte Accounts nur berechtigten Personen mit einem legitimen Grund gewährt wird, was den Umfang der Berechtigungen während einer Session begrenzt.

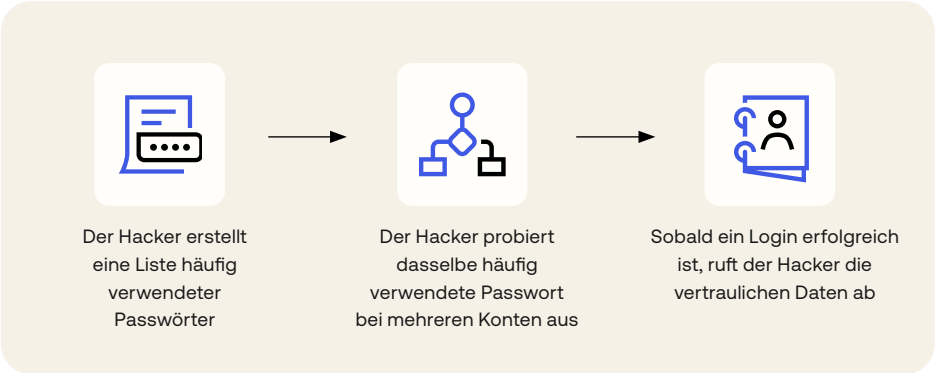
6. **Bedrohungsabwehr:** Okta kann flexibel auf Risiken in Benutzersitzungen reagieren und eine erneute Authentifizierung anfordern oder die Session komplett beenden. Umgekehrt kann Okta Identity Threat Protection die User Experience verbessern, indem die Sitzungslänge bei Benutzern mit geringem Risiko vergrößert wird.

Brute-Force-Angriffe

Brute-Force-Angriffe wird es so lange geben, wie Benutzer schwache Passwörter verwenden oder Passwörter mehrfach nutzen.

Password Spraying

Beim Password Spraying nehmen die Angreifer nicht bestimmte Benutzer oder Accounts ins Visier, sondern attackieren ungezielt Tausende potenzielle Opfer. Dabei probiert der Angreifer einfach eine Reihe bekannter Passwörter bei mehreren Accounts aus – in der Hoffnung, dass wenigstens ein Benutzer genau dieses Passwort für sein Konto gewählt hat. Weil die Angreifer dabei eine relativ kleine Zahl qualifizierter Passwörter auf sehr vielen Accounts testen, bleiben sie bei den fehlgeschlagenen Anmeldeversuchen in der Regel unter den Grenzwerten, die zu einer Sperrung eines Accounts führen würden. Um die Trefferwahrscheinlichkeit zu erhöhen, recherchieren Angreifer häufig die angegriffenen Unternehmen und versuchen zu ermitteln, ob deren System Passwörter mit einer bestimmten Länge oder Sonderzeichen verlangt.



Credential Stuffing

Beim Credential Stuffing versucht der Angreifer, gültige Zugangsdaten (oft in einem Online-Dump enthaltene Kombinationen) auf mehreren Websites einzugeben – in der Hoffnung, dass wenigstens ein Versuch erfolgreich ist. Bei diesen Angriffen machen sich die Cyberkriminellen zunutze, dass die meisten Benutzer ihre Passwörter mehrfach verwenden. Der Angreifer nutzt automatisierte Tools, um in kurzer Zeit eine Vielzahl von Systemen abdecken zu können. Diese Angriffe sind häufig erfolgreich, da gültige Anmeldedaten keine Account-Sperrung auslösen.

Strategien zur Behebung

1. **Benutzertools und -schulungen:** Bei Unternehmen, die immer noch Passwörter nutzen:

    a. Die weitgehende Vermeidung der Passwort-Wiederverwendung kann helfen, erfolgreiche Credential Stuffing-Angriffe zu verhindern. Um das zu erreichen, ist es sinnvoll, den Aufwand für die Erstellung starker Passwörter zu verringern. Okta bietet ein Browser-Plugin an, das Benutzern bei der Erstellung neuer Accounts sichere Passwörter vorschlägt und diese automatisch für sie speichert.

    b. Okta kann Ihr Unternehmen bei der Verhinderung häufiger Passwörter unterstützen, indem bei der Account-Erstellung höhere Anforderungen an Passwörter durchgesetzt werden, was Password Spraying-Angriffe wirkungslos macht.

2. **Erkennung gefährlicher IP-Adressen:** ThreatInsight nutzt aggregierte Daten aus dem gesamten Okta-Kundenstamm zur Erkennung gefährlicher IP-Adressen, von denen Anmeldedaten-basierte Angriffe ausgehen. Okta verhindert, dass diese IP-Adressen bis zur Authentifizierungsphase gelangen, und reduziert so das Risiko von ihren Accounts ausgesperrter legitimer Benutzer.

3. **Sichere Authentifizierungsmethoden:** Okta bietet mehrere Authentifizierungsverfahren an, die Brute-Force-Angriffe verhindern:

    a. FastPass ist eine Zero-Trust-Authentifizierungslösung, die Passwörter – einen gefährlichen Angriffsvektor – überflüssig macht. Dabei wird auch der Geräte- und Browser-Status überprüft und sichergestellt, dass nur vertrauenswürdige Benutzer und ihre Geräte auf Ihre Umgebung zugreifen können.

    b. Okta unterstützt eine Reihe weiterer Phishing-resistenter Authentifizierungsmethoden.

    c. Adaptive MFA gewährleistet, dass Angreifer den Authentifizierungsprozess nicht abschließen können, selbst wenn sie über kompromittierte Anmeldedaten verfügen. Okta erfasst Benutzerdaten wie Standort, IP-Adresse sowie andere Datenpunkte, erstellt daraus ein Basisprofil und ermittelt das Risiko des Login-Versuchs. Wenn sich MFA nicht für jeden Benutzer und jeden Login erzwingen lässt, können Sie diese Kontrolle parallel zu anderen Prüfungen wie Device Fingerprinting einsetzen. Außerdem können Sicherheitsadministratoren Captcha-Abfragen in den Login-Prozess integrieren und so die Authentifizierungsanfrage zusätzlich absichern.

Zusammen-fassung

Okta Workforce Identity Cloud bietet zahlreiche Funktionen für den Schutz von Benutzern, ihren Geräten sowie ihren Sessions vor Bedrohungen, die vor, während und nach der Authentifizierung ansetzen. Mit Verhaltensanalysen, Geräteprüfungen und standardmäßig enthaltenen Integrationen mit anderen Sicherheitstools überprüft Okta kontinuierlich Risiken, damit Ihr Unternehmen automatisch auf Identity-bezogene Bedrohungen reagieren kann, noch bevor diese zu einem echten Problem werden.

Weitere Informationen über Workforce Identity Cloud.