okta

Identity-Sicherheit: Die unverzichtbare Checkliste zur Abwehr von Angriffen

14 Fragen, die Ihnen helfen, Ihr Unternehmen vor Identity-basierten Cyberangriffen zu schützen

Angreifern ist Ihre Firewall egal, ihnen geht es um Ihre Anmeldedaten. Sie nutzen Session-Token aus, umgehen schwache Multi-Faktor-Authentifizierung (MFA) mithilfe von AiTM-Proxies und missbrauchen nicht-menschliche Identitäten wie inaktive Service-Accounts, um sich unerkannt zu bewegen.

Mit dieser Checkliste können Sie Ihre Verteidigungsfähigkeiten im Hinblick auf die moderne Bedrohungslandschaft überprüfen.

Beachten Sie dabei, dass diese Checkliste nur als eine Komponente Ihres gesamten Sicherheitsprogramms gedacht ist.

okta

Vor einem Angriff: Proaktives Sicherheitsmanagement

In diesem Abschnitt geht es um die Beseitigung von Konfigurationsfehlern und die Reduzierung der Identity-Angriffsfläche, noch bevor es zu einer Attacke kommt.

1. Überprüfen Sie kontinuierlich die Identity-Sicherheitslage menschlicher und nicht-menschlicher Identitäten (z. B. Service-Accounts und API-Schlüssel)?
2. Können Sie automatisch das Least-Privilege-Prinzip durchsetzen und gewährleisten, dass es keine MFA-Umgehungen gibt?
3. Haben Sie eine Möglichkeit zum Identifizieren veralteter oder teilweise stillgelegter Accounts, die immer noch aktiven Zugriff haben?
4. Gibt es ein System zum Priorisieren und Beheben von Identity-Konfigurationsfehlern und übermäßigen Berechtigungen, um die potenziellen Auswirkungen einer Sicherheitsverletzung zu minimieren?
5. Versuchen Sie aus der Identity-Perspektive, einen ganzheitlichen Überblick darüber zu erhalten, wer Zugriff auf welche Ressourcen hat und wie diese Zugriffe authentifiziert werden, um so die Lücken von CSPM- und SSPM-Tools zu schließen?

Identity Security Posture Management

Kontinuierliche Erkennung und Behebung Identity-basierter Risiken und Konfigurationsfehler

Während des Angriffs: Kontinuierliche Erkennung und Abwehr von Bedrohungen

In diesem Abschnitt geht es um die notwendigen Fähigkeiten zur Erkennung und Abwehr aktiver Bedrohungen in Echtzeit.

6. Haben Sie Phishing-resistente Authentifizierung (z. B. Okta FastPass) implementiert, um Benutzer vor Phishing-Angriffen zu schützen?
7. Überwachen Sie kontinuierlich Session-Aktivitäten und das Benutzerverhalten nach der Erstauthentifizierung, um Anomalien und potenzielle laterale Bewegungen zu erkennen?
8. Können Sie Inline-Reaktionen automatisieren, um Vorfälle einzudämmen, z. B. durch Universal Logout bei allen Anwendungen und Geräten, durch Erzwingen von Step-up-MFA oder durch Auslösen benutzerdefinierter Workflows?
9. Verfügen Sie über KI-gestützten Bot-Schutz, der automatisierte Angriffe erkennen und abwehren kann, ohne dass Benutzereingaben wie bei klassischen CAPTCHAs erforderlich sind?
10. Bewertet Ihr System kontinuierlich Risikostufen sowie den Benutzer- und Gerätekontext, um Sicherheitsrichtlinien während einer Session dynamisch auszuwerten und durchzusetzen?

Identity Threat Protection

Automatische Erkennung und Abwehr Identity-bezogener Bedrohungen in Echtzeit

Okta Device Access

Sichere Geräteanmeldungen, die den Schutz stärken und Ressourcenzugriffe vereinfachen

Okta FastPass

Zero-Trust-Sicherheit mit Phishing-resistenter, passwortloser Authentifizierung

Nach dem Angriff: Stärkung der Identity-Resilienz

In diesem Abschnitt geht es um die Verbesserung der Sicherheitslage und die Maßnahmen nach einem Vorfall.

11. Verfügen Sie über Tools zum Anzeigen von Sicherheitsvorfällen und für forensische Analysen, mit denen sich der gesamte Pfad eines Identity-Angriffs aufdecken lässt?
12. Gibt es ein System zum Verbessern der Behebung sicherheitsrelevanter Vorfälle durch Identity-Ereignis-Korrelation und gemeinsam für alle Sicherheitstools verfügbare Informationen?
13. Können Sie die Einhaltung von Compliance-Vorschriften gewährleisten, indem Sie Identity-Kontrollen gängigen Frameworks wie NIST zuordnen?
14. Verfügen Sie über einen kontinuierlichen Feedback-Loop-Mechanismus, um Sicherheitsereignisse zu analysieren und die Reaktionen im Laufe der Zeit zu optimieren?

Die Vorteile von Okta

Dank Einblicken in 10 Milliarden weltweite Anmeldungen und 2 Milliarden blockierte Bedrohungen pro Monat erkennt Okta die TTPs (Taktiken, Techniken und Prozeduren), die anderen Anbietern entgehen. Durch das einheitliche Identity-Management ermöglicht Okta eine völlig neue Übersicht über die Indikatoren und Richtlinien in Ihren IT-, Sicherheits- und Kundenumgebungen. Dadurch stehen Ihren Teams leistungsstarke Möglichkeiten zur Echtzeit-Erkennung und -Abwehr von Bedrohungen zur Verfügung.

Okta implementiert einen Identity Security Fabric für orchestrierte End-to-End-Sicherheit vor, während und nach der Authentifizierung für alle digitalen Identitäten – menschliche und nicht-menschliche Identitäten sowie KI-Agenten – in allen Umgebungen.