okta

Identity-Security-Checkliste

40 Fragen, die Ihnen helfen, Ihr Unternehmen vor Identity-basierten Angriffen zu schützen

Die Security-Breaches der vergangenen Jahre haben bewiesen, dass Identity ein gefährlicher Angriffsvektor ist – für Cyberkriminelle und staatliche Akteure gleichermaßen. Identity ist mehr als die Login-Box: Sie ist die erste und letzte Verteidigungslinie, die in den Unternehmen den Zugang zu den sensibelsten Daten und Infrastrukturen schützt. Identity ist Security.

Okta steht an vorderster Front, wenn es gilt, die Kunden und die IT-Branche zuverlässig vor Identity-basierten Angriffen zu schützen.

Wir managen weltweit mehr als 10 Milliarden Logins und schützen jeden Monat über 18.000 Kunden vor mehr als 2 Milliarden bösartiger Requests. Als einer der Marktführer haben wir es uns auf die Fahne geschrieben, unsere Kunden mit bewährten Best Practices, wie etwa der folgenden Checkliste, dabei zu helfen, ihr Security-Standing kontinuierlich zu verbessern. Bitte beachten Sie, dass diese Checkliste lediglich als eines von vielen Elementen Ihres Security-Programms dienen soll.

okta

Ganzheitliche Identity-Security- und Zero-Trust-Modelle

Grundlegende Anforderungen

1. Ist Ihre Identity Security integraler Bestandteil einer ***ganzheitlichen Cybersecurity-Strategie***, die auch Lösungen für das Identity & Access Management, die Incident Response und das Risikomanagement umfasst und kontinuierliche Verbesserungsprozesse vorsieht?
2. Haben Sie verbindliche Maßnahmen definiert, um ***Anwender, Devices und Anwendungen dynamisch zu authentisieren und zu autorisieren*** – und das im Kontext der jeweiligen Anfrage?
3. Gibt es etablierte Prozesse für ***Freigaben, Reviews und Updates privilegierter Zugänge***?
4. Haben Sie im Rahmen Ihrer Identity-Security-Lösung auch ***Least-Privilege Access*** implementiert, um die Angriffsfläche zu verringern? Und: Achten Sie darauf, Admin-Rechte so weit wie möglich zu beschränken oder aufzuheben?

Identity & Access Management

Grundlegende Anforderungen

10. Haben Sie ***Phishing-resistente Multi-Faktor-Authentisierung*** für alle Zugriffe auf sensible Ressourcen implementiert?
11. Stellen Sie ***über den gesamten Mitarbeiter-Lifecycle hinweg Phishing-resistente Prozesse sicher*** – vom Rollout und Onboarding bis hin zur Account-Recovery?
12. Müssen sich Ihre Administratoren mit ***Step-up-Authentisierung*** anmelden, bevor sie sensible Aktivitäten anstoßen können?
13. Werden ***Anwender automatisch über besonders riskante Events benachrichtigt – etwa, wenn alle MFA-Faktoren eines Accounts zurückgesetzt werden*** oder wenn ein Zugriff auf einen Account über ein neues Gerät erfolgt?
14. Ist das ***Management des Identity-Lifecycles automatisiert***, etwa mit Blick auf das Onboarding, das Offboarding und anstehende Access-Reviews, um ein Höchstmaß an Effizienz und Zuverlässigkeit sicherzustellen?
15. Nach welchen Kriterien werden in Ihrem Unternehmen ***Identity-Accounts als ‚Ruhend'*** eingestuft? Wie oft werden bei Ihnen ruhende Accounts überprüft?
16. Gibt es bei Ihnen Vorgaben für den Umgang mit Zugangsdaten für Service-Accounts – zum Beispiel ***regelmäßige Passwort-Rotationen oder Passwortwechsel nach jedem interaktiven Zugriff***?
17. Gibt es eine ***Identity-Governance-Strategie***? Orientiert sie sich an gängigen Branchenstandards und Best Practices?
18. Gibt es Mechanismen für ***die regelmäßige Bewertung und Zertifizierung der Zugriffsrechte*** Ihrer Benutzer?
19. Gibt es Mechanismen, um sicherzustellen, dass remote agierende Benutzer sicher und effizient auf benötigte Ressourcen zugreifen können – und das sowohl ***mit dienstlichen als auch mit privaten Devices*** (sowohl Notebook als auch Smartphone)?

Erweiterte Anforderungen

5. Gibt es eine robuste Strategie für die ***kontinuierliche Überwachung und Bewertung des User- und Device-Verhaltens***, um ungewöhnliche oder verdächtige Aktivitäten proaktiv zu erkennen?
6. ***Beschränken Sie die Berechtigungen der IT-Support-Mitarbeiter***, um zu verhindern, dass diese auf hochgradig privilegierte Accounts zugreifen? Werden für diese Anwender beispielsweise eigene Administrator-Rollen definiert und vorgehalten?
7. Gibt es Mechanismen für eine ***besonders strenge Verifizierung der Identitäten privilegierter Helpdesk-Mitarbeiter***, etwa den Einsatz von visueller Verifizierung?
8. Haben Sie Maßnahmen definiert, um ***die Identität von Anwendern kontinuierlich zu verifizieren***, während diese mit Ihren kritischsten Ressourcen interagieren?
9. Verpflichten Sie ***3rd-Party-Anbieter, die auf Ihre IT-Umgebung zugreifen, Zero Trust Security zu implementieren***? Konkret: Verifizieren und auditieren Sie das Security-Standing dieser Drittanbieter, oder vertrauen Sie implizit auf deren Fähigkeit, den eigenen Netzwerk-Perimeter zu schützen?

Erweiterte Anforderungen

20. Unterstützt Ihre Identity-Governance-Lösung die ***Segregation of Duties***, um toxische Access-Kombinationen zu verhindern?
21. Sind Ihre privilegierten Accounts durch eine robuste ***und Phishing-resistente Multi-Faktor-Authentisierung*** geschützt, um höchsten Sicherheitsstandards zu genügen?
22. Haben Sie eine ***unternehmensweite Lösung für das Privileged Access Management*** (PAM) im Einsatz, um Zugriffe auf privilegierte Accounts zu erkennen, zu sichern, zu dokumentieren und zu überwachen?
23. Verpflichten Sie ***3rd-Party-Anbieter, die auf Ihre IT-Umgebung zugreifen, sich beim Zugriff auf Workplace-Anwendungen stets über ein IAM*** anzumelden?
24. Nutzen Sie ***IP-Bindung, um Anwender an kritischen Ressourcen zu authentisieren***? Haben Ihre Administratoren die Möglichkeit, eine Admin-Session automatisch abzubrechen, wenn die IP-Adresse, die an einer API oder bei einem Web-Request registriert wird, von der IP-Adresse abweicht, die zu Beginn der Session aufgezeichnet wurde?
25. ***Blockieren Sie Requests an Ihrer Identity-Lösung nach Netzwerktyp*** (z. B. bei Einsatz eines Anonymisierungs-Proxys)?

okta

Strategien zur Behebung und Minimierung von Risiken

Grundlegende Anforderungen

26. Welche bestehenden Verfahren und Tools helfen Ihnen, ***das Monitoring privilegierter Accounts zu verbessern***?
27. Welche Rolle kommt ***Analysen des Benutzerverhaltens*** in Ihrer Identity-Security-Strategie zu – insbesondere mit Blick auf Detection & Response?
28. Nutzen Sie ***automatische Benachrichtigungen***, wenn auf Ihren On-Premises betriebenen AD-Agents Änderungen vorgenommen werden?
29. Unterstützt Ihre Identity-Plattform einen ***„Infrastructure-as-Code"***-Ansatz zur Entwicklung und Wartung der Systeme?
30. Erkennt Ihre Identity-Lösung Zugriffe über bekannte Devices, um ***Account-Lockouts*** bei einem Brute-Force-Angriff zu vermeiden?

Erweiterte Anforderungen

31. Können Sie ***Standort-abhängige Zugriffsbeschränkungen*** für Anwender und Machine-to-Machine-Zugriffe durchsetzen?
32. ***Gestatten Sie es Ihren Admins, Zugriffe über Anonymisierer zu identifizieren und zu unterbinden***, indem sie evaluieren, ob eine IP-Adresse einem bekannten Anonymisierer zugewiesen ist?
33. ***Setzen Sie Token-Bindung für Machine-to-Machine-Integrationen durch*** und nutzen Sie den Proof-of-Possession, um zu gewährleisten, dass ausschließlich authentisierte Anwendungen mithilfe von Tokens auf APIs zugreifen können?
34. ***Verwenden Sie leistungsfähige Bot-Detection- und Bot-Protection-Funktionalitäten*** mit 3rd-Party-Scores und Edge-basierten Komponenten-Signalen?
35. ***Implementieren Sie bei der Anwendungsentwicklung starke Session-Management-Funktionalitäten und robuste Token-Security***? Konkret: Entwickeln Sie eigene Session-Control-Dashboards, um eine maßgeschneiderte User Experience sicherzustellen?

Trainings und Awareness-Schulungen für Mitarbeiter

Grundlegende Anforderungen

36. Führen Sie ***regelmäßige Trainings zur Schärfung der Phishing-Awareness*** sowie allgemeine Cybersecurity-Trainings durch, um Ihre Mitarbeiter über aktuelle Bedrohungen und Best Practices zu informieren?
37. Wissen Ihre Mitarbeiter um die Rolle und die Bedeutung starker Passwort-Policies und ***passwortloser Authentisierungs***-Optionen?
38. Führen Sie ***simulierte Phishing-Übungen*** durch, um zu testen, wie resilient Ihre Mitarbeiter gegen Phishing-Angriffe sind? Gibt es dedizierte Trainings für Mitarbeiter, die Opfer eines solchen Angriffs waren?
39. Gibt es einen ***Mechanismus für Mitarbeiter, die Security-Verdachtsfälle melden möchten*** oder Fragen zur Security haben?
40. Wurden Ihre Mitarbeiter darüber aufgeklärt, ***warum es wichtig ist, Software und Devices stets up-to-date zu halten*** und die aktuellen Security-Patches einzuspielen?