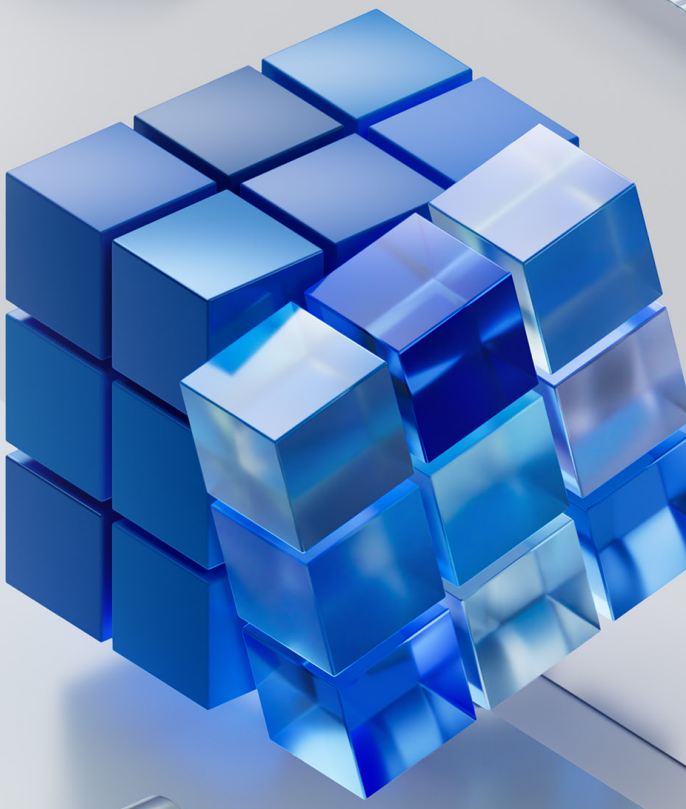
Acronis

Angriffe auf die Identitäts- und Kontrollebene von Microsoft 365



9 reale Bedrohungen, ausgenutzte Schwachstellen und wie MSPs diese mit Acronis SPM bewältigen können

Moderne Angriffe auf Microsoft 365 zielen inzwischen häufiger auf die Kontrollebene (Identitäten, OAuth-Apps, Berechtigungen, Sitzungen und Konfigurationen) als auf Endpunkte ab.

Bei den jüngsten Angriffen nutzten Cyberkriminelle legitime Authentifizierungsabläufe, übermäßige Berechtigungen, schwache Zugriffskontrollen und Fehlkonfigurationen, um sich dauerhaften Zugriff auf Microsoft 365-Mandanten zu verschaffen.

Diese Checkliste fasst Folgendes zusammen:

- Verwendete Angriffstechniken in realen Vorfällen
- Ausgenutzte Schwachstellen
- Empfohlene Microsoft 365-Kontrollen zur Risikominimierung
- Acronis SPM für die kontinuierliche, mandantenübergreifende Überwachung und Durchsetzung von Sicherheitsrichtlinien



Copyright © 2003–2026 Acronis International GmbH.

1. Password Spraying-Angriffe

Realer Vorfall

Midnight Blizzard (2024)

Angriffstechnik

Bei dem Angriff wurde Password Spraying eingesetzt, um Zugriff auf ein älteres Mandantenkonto zu erlangen, das nicht Teil der Produktionsumgebung war.

Ausgenutzte Schwachstellen

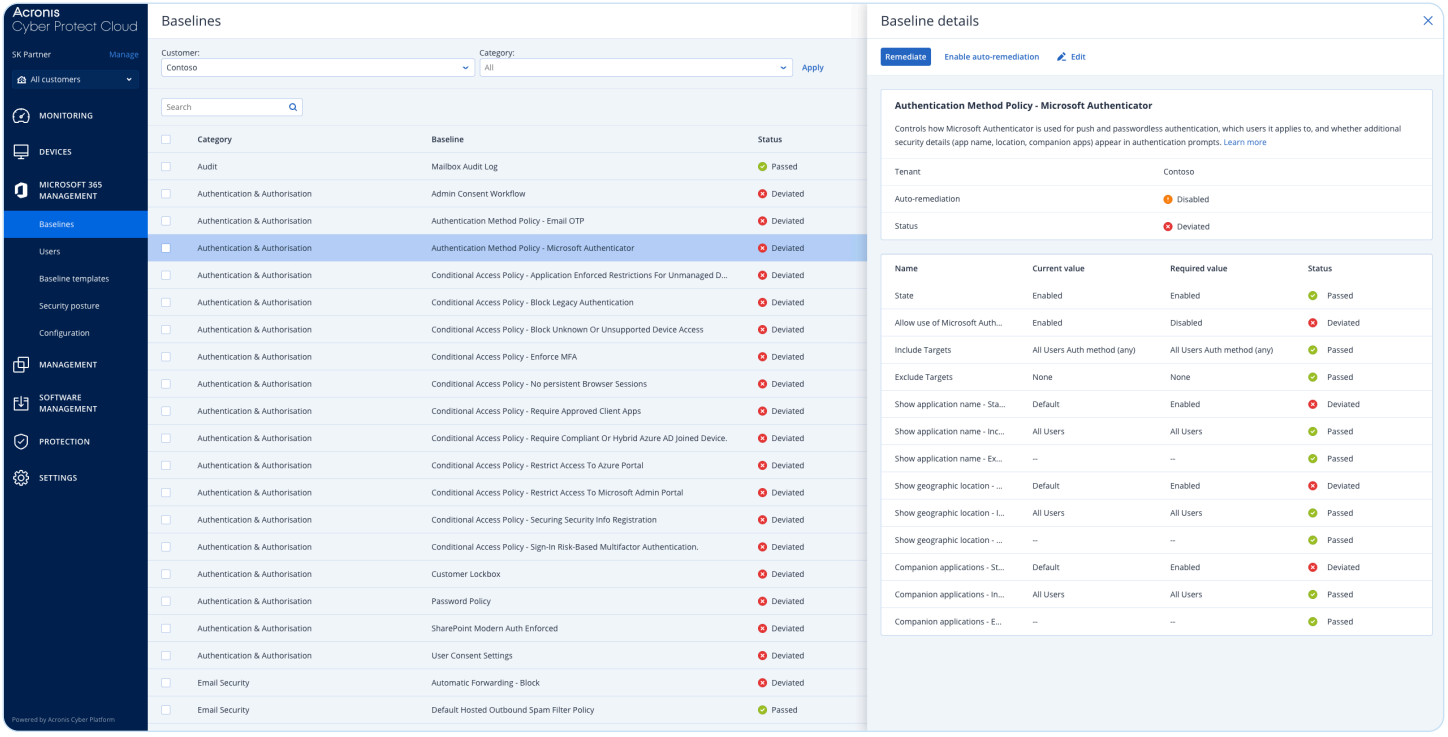
- Unsichere Anmeldedaten
- Keine Mehrfaktor-Authentifizierung (MFA) für ein altes Konto

Sicherheitsmaßnahmen zur Risikominimierung

- Durchsetzung von MFA
- Änderung unsicherer Passwörter
- Deaktivierung veralteter Authentifizierungsmethoden
- Überwachung auf ungewöhnliche Anmeldeversuche

Acronis SPM bietet MSPs folgende Vorteile

- Identifizierung von Konten ohne MFA
- Erkennung unsicherer Authentifizierungseinstellungen
- Überwachung aller Mandanten auf Abweichungen von Sicherheitsvorgaben
- Proaktive Behebung unsicherer Identitätskonfigurationen (bevor diese zu Angriffsflächen werden)



Copyright © 2003–2026 Acronis International GmbH.

2. Tokenfälschung und Sitzungsmissbrauch

Realer Vorfall

Storm-0558 (2023)

Angriffstechnik

Durch den Einsatz gefälschter Authentifizierungstoken gelang der Zugriff auf cloudbasierte E-Mail-Konten.

Ausgenutzte Schwachstellen

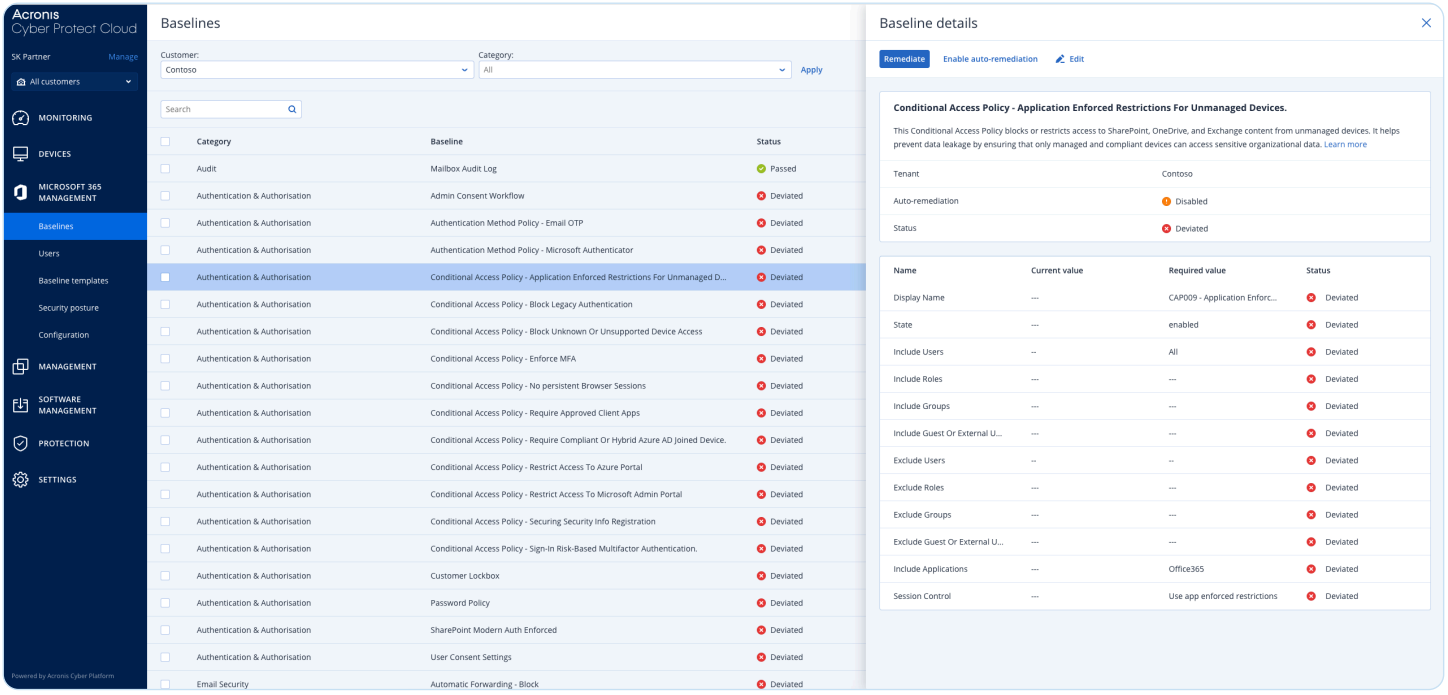
- Unsichere Token-Validierung
- Missbrauch von Signaturschlüsseln
- Mangelnde Transparenz bei der Nutzung ungewöhnlicher Token

Sicherheitsmaßnahmen zur Risikominimierung

- Verschärfte Sicherheitsmaßnahmen
- Durchsetzung von MFA und bedingtem Zugriff
- Beschränkung von App-Zustimmungen
- Schutz des privilegierten Zugriffs
- Überwachung von Token und Sitzungen auf ungewöhnliche Aktivitäten

Acronis SPM bietet MSPs folgende Vorteile

- Standardisierte Konfigurationen für MFA und bedingten Zugriff
- Erkennung von Abweichungen bei Identitätskonfigurationen
- Durchsetzung sicherer Baselines für den Administratorzugriff
- Verhinderung der Offenlegung von Identitätsdaten benachbarter Mandanten



Copyright © 2003–2026 Acronis International GmbH.

3. Sitzungsübernahme und AiTM-Phishing

Realer Vorfall

Mehrere gemeldete Vorfälle

Angriffstechnik

Diebstahl von Sitzungscookies durch Reverse-Proxy-Phishing

Ausgenutzte Schwachstellen

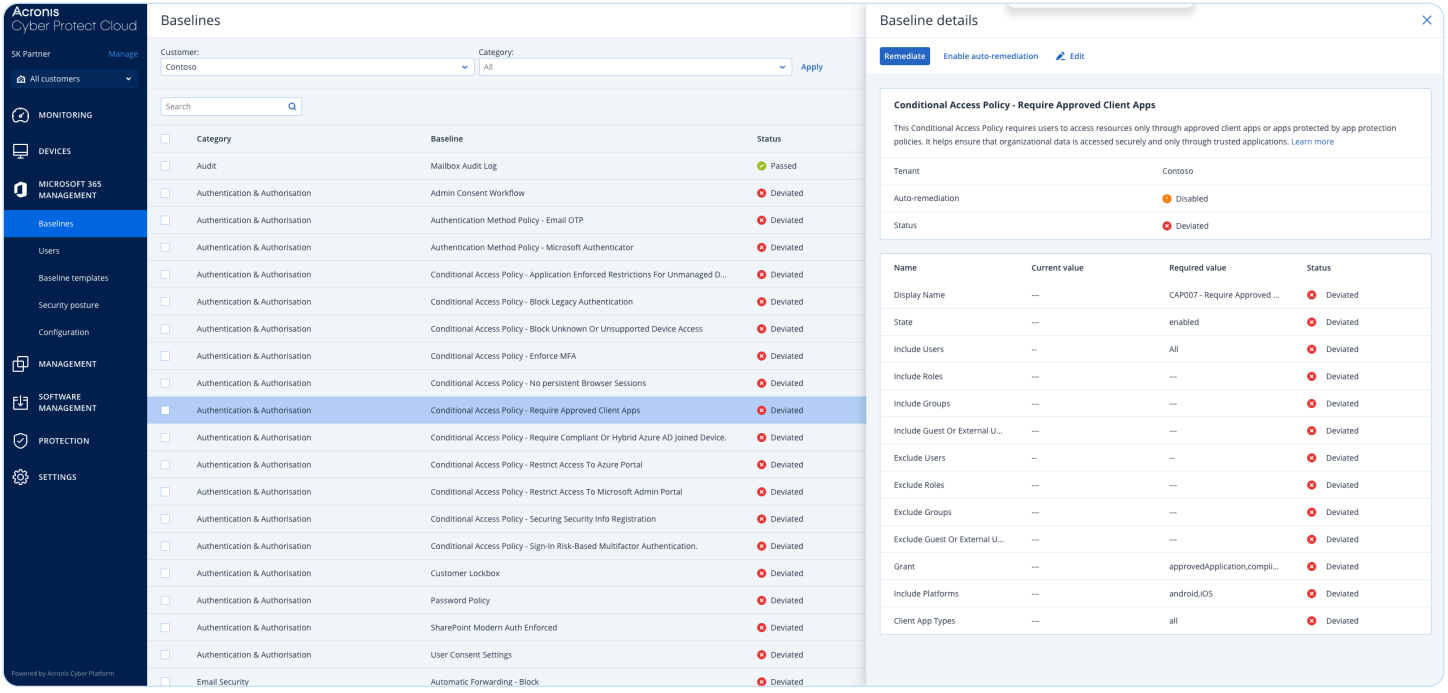
- Gestohlene authentifizierte Sitzungscookies
- Unzureichende Durchsetzung des bedingten Zugriffs
- Fehlende Zugriffsbeschränkungen auf Geräteebene

Sicherheitsmaßnahmen zur Risikominimierung

- Verbot von nicht konformen oder unverwalteten Geräten
- Umfassende Durchsetzung des bedingten Zugriffs
- Überwachung von Sitzungen auf ungewöhnliches Verhalten
- Kontinuierliche Zugriffsevaluierung, sofern verfügbar

Acronis SPM bietet MSPs folgende Vorteile

- Erkennung von Abweichungen von den Vorgaben für den bedingten Zugriff
- Langfristige Einhaltung der Basisrichtlinien für den sicheren Zugriff
- Mandantenübergreifende Standardisierung von Identitäts- und Gerätezugriffskontrollen



Copyright © 2003–2026 Acronis International GmbH.

4. Token-Replay-Angriffe

Realer Vorfall

Mehrere gemeldete Vorfälle

Angriffstechnik

Bei diesen Angriffen wurden gestohlene Primary Refresh Tokens (primäre Aktualisierungstoken) wiederverwendet.

Ausgenutzte Schwachstellen

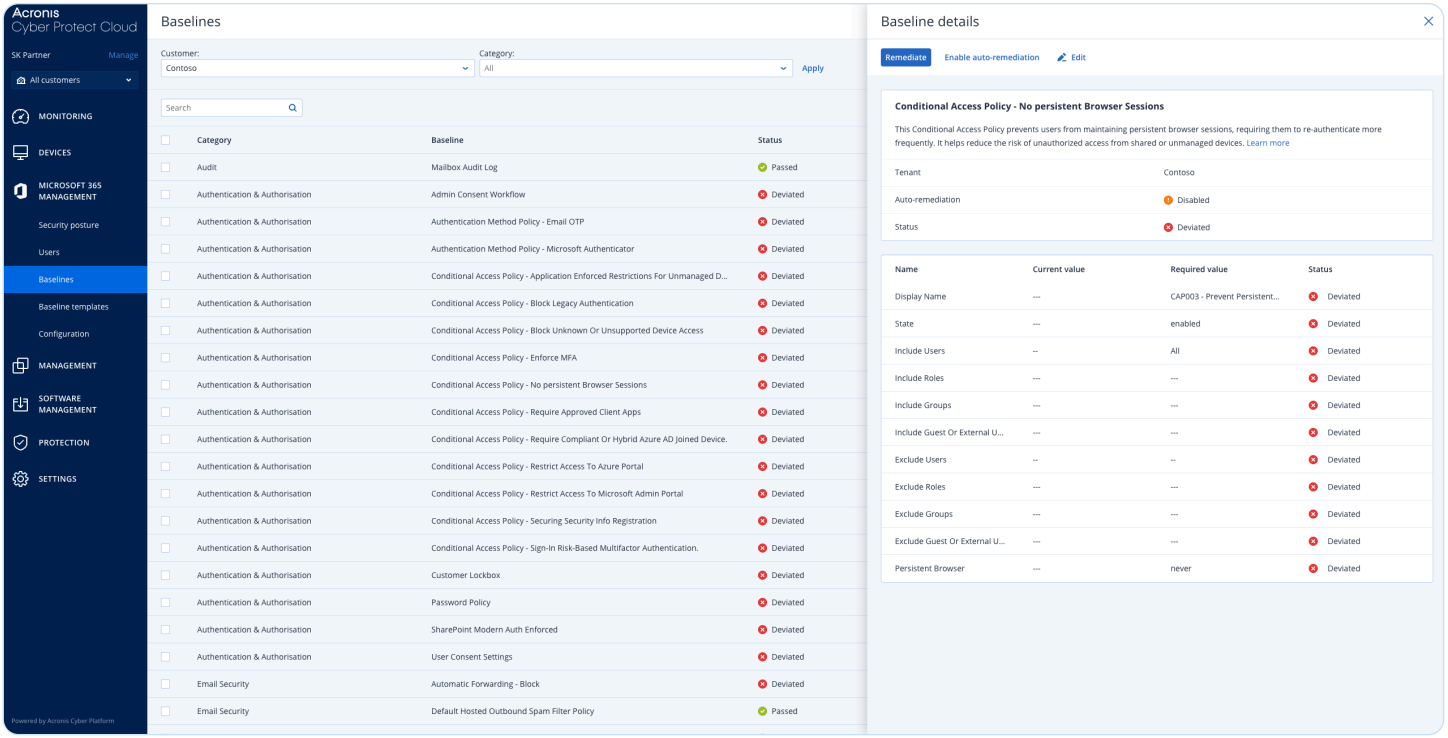
- Mangelnder Schutz für Token bzw. Sitzungen
- Unzureichende Durchsetzung von Sitzungsrichtlinien

Sicherheitsmaßnahmen zur Risikominimierung

- Durchsetzung des Token-Schutzes (wenn möglich)
- Ausweitung des bedingten Zugriffs auf Sitzungen
- Beschränkung des Zugriffs für nicht verwaltete Geräte

Acronis SPM bietet MSPs folgende Vorteile

- Kontinuierliche Überwachung der Authentifizierungsrichtlinien
- Erkennung von Abweichungen von den Sicherheitsvorgaben für den bedingten Zugriff und die Sitzungskonfiguration
- Durchsetzung sicherer Baselines für die Identitäts- und Zugriffsverwaltung



Copyright © 2003–2026 Acronis International GmbH.

5. OAuth-Consent-Phishing

Realer Vorfall

Mehrere gemeldete Vorfälle

Angriffstechnik

Zustimmungsfreigaben für böswillige Apps

Ausgenutzte Schwachstellen

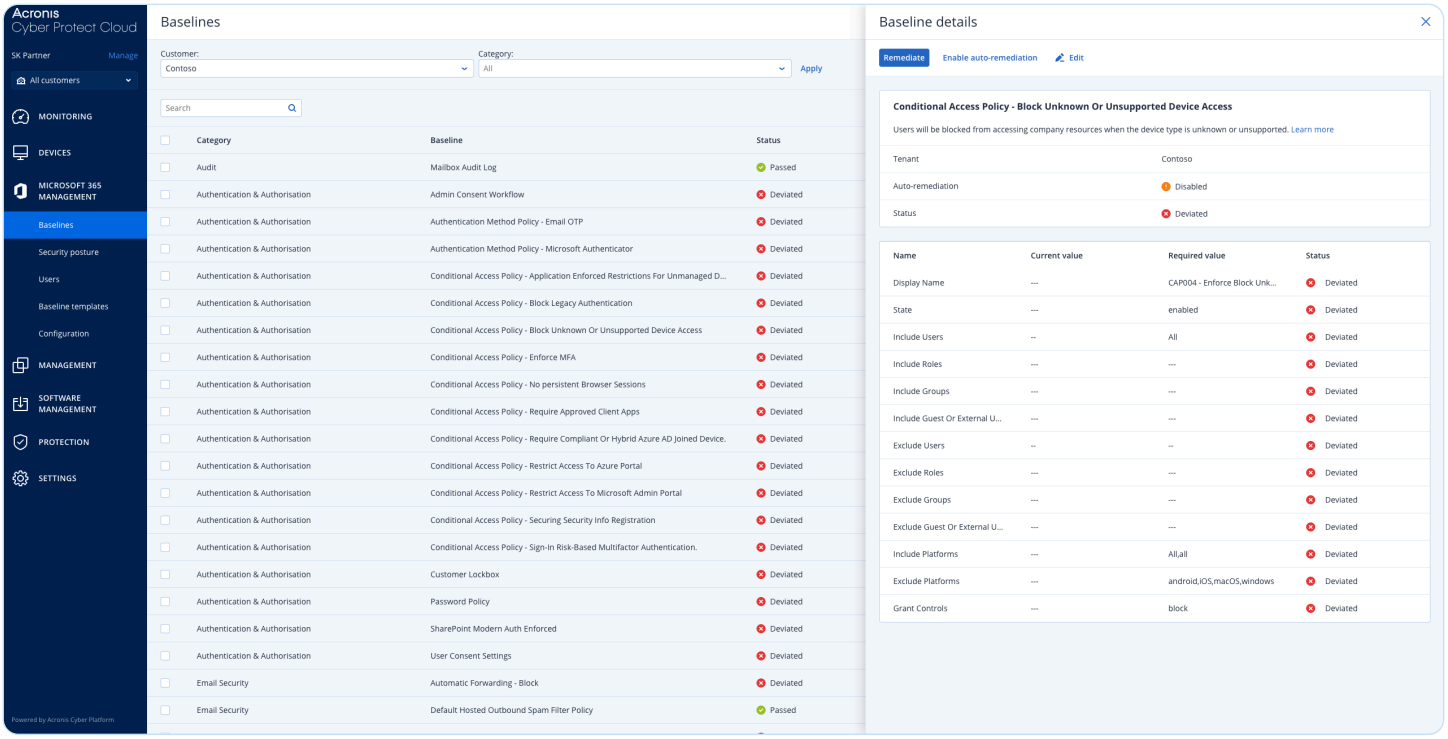
- Uneingeschränkte Benutzerzustimmung
- Unzureichende App-Kontrollen

Sicherheitsmaßnahmen zur Risikominimierung

- Einschränkung der Benutzerzustimmung
- Einführung von Administratorfreigaben für Apps
- Begrenzung der Apps auf verifizierte Anbieter und Durchsetzung minimaler Zugriffsrechte

Acronis SPM bietet MSPs folgende Vorteile

- Standardisierung autorisierungsbezogener Kontrollen
- Erkennung von Abweichungen von genehmigten App-Zustimmungsrichtlinien
- Gewährleistung sicherer Autorisierungsverfahren für alle Microsoft 365-Mandanten



Copyright © 2003–2026 Acronis International GmbH.

6. Missbrauch von OAuth-Apps und Datenexfiltration über die Graph API

Realer Vorfall

Mehrere gemeldete Vorfälle

Angriffstechnik

Es erfolgte ein API-basierter Datenzugriff und eine Datenexfiltration durch Apps mit zu vielen Berechtigungen.

Ausgenutzte Schwachstellen

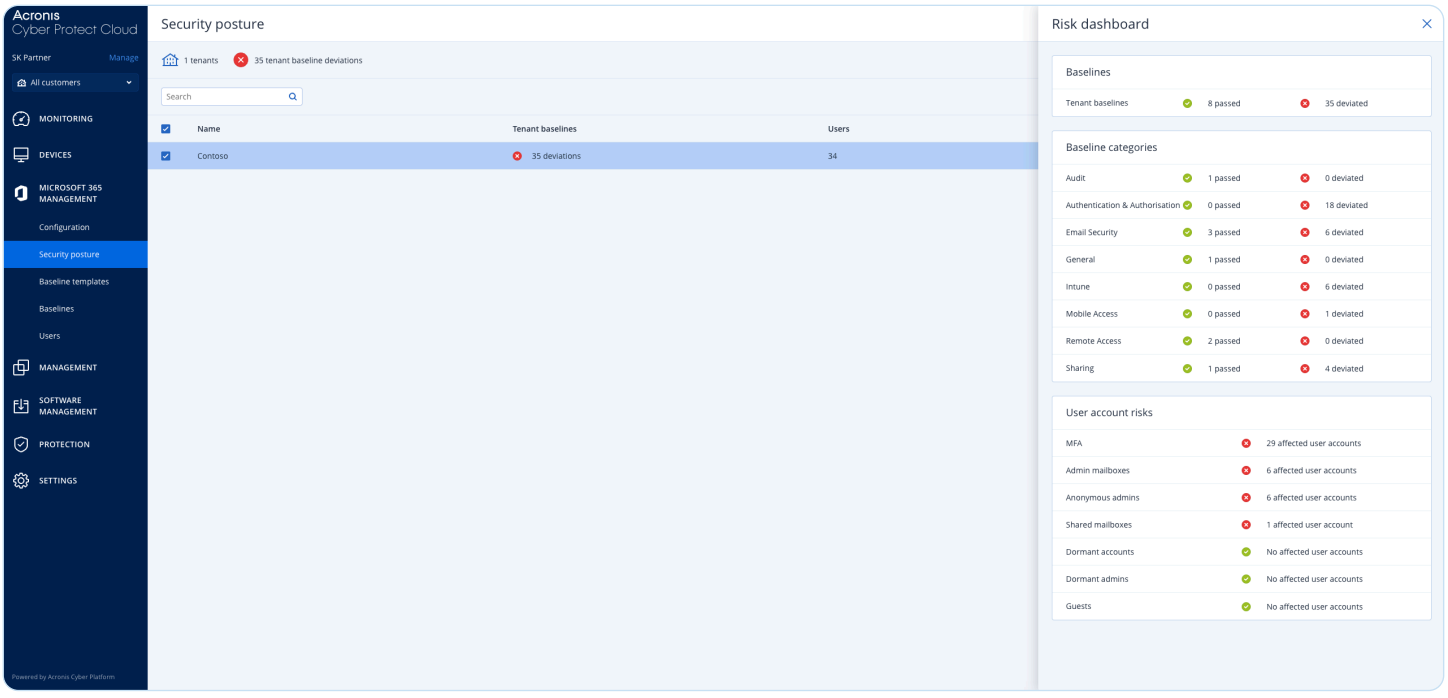
- Übermäßige Berechtigungen für Microsoft Graph
- Geringe Transparenz bezüglich des App-Verhaltens
- Nicht verwalteter App-Zugriff

Sicherheitsmaßnahmen zur Risikominimierung

- Regelmäßige Überprüfung von App-Berechtigungen
- Untersuchung ungewöhnlicher Aktivitäten in Graph
- Überprüfung der von externen Benutzer:innen autorisierten Apps

Acronis SPM bietet MSPs folgende Vorteile

- Gewährleistung der Kontrolle über App-Berechtigungen und Zustimmungsrichtlinien
- Erkennung von Abweichungen von Autorisierungsrichtlinien und von nicht verwalteten Apps
- Höhere Transparenz bei der Zugriffsverwaltung für Microsoft 365-Apps



Copyright © 2003–2026 Acronis International GmbH.

7. Rechteausweitung und Missbrauch von Rollen mit übermäßigen Berechtigungen

Realer Vorfall

Mehrere Vorfälle von Entra ID-Rechteausweitungen (Midnight Blizzard)

Angriffstechnik

Es wurden übermäßige Administratorrechte ausgenutzt, um die Rechte auszuweiten.

Ausgenutzte Schwachstellen

- Zu viele Administratorkonten mit globalen Berechtigungen
- Unbemerkte Ausweitung von Berechtigungen
- Schwache Kontrolle von Benutzerrollen

Sicherheitsmaßnahmen zur Risikominimierung

- Durchsetzung des Least-Privilege-Prinzips
- Einschränkung von Administratorkonten
- Kontinuierliche Überprüfung privilegierter Rollen

Acronis SPM bietet MSPs folgende Vorteile

- Erkennung übermäßiger Administratorkonten und Berechtigungen
- Mandantenübergreifende Standardisierung einer sicheren Rollenverwaltung
- Durchsetzung sicherer Identitäts- und Autorisierungsstandards

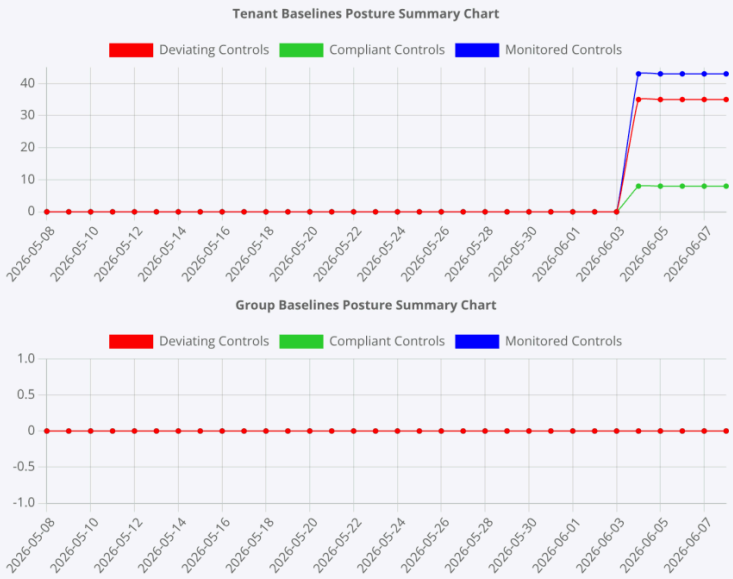
Compliance Posture Summary

Baselines

Current Posture Summary (All time)

Tenant		Group	
Passing:	8	Passing:	-
Deviating:	35	Deviating:	-

Posture Summary (In this period) *



Please noted that baseline created/passing were not recorded before 27/09/2022.
Only Deviations after this date will be accurate.

Copyright © 2003–2026 Acronis International GmbH.

8. Datenschutzverletzung über SharePoint und OneDrive

Realer Vorfall

Mehrere gemeldete Vorfälle

Angriffstechnik

Übermäßige oder versehentliche Freigabe von Daten

Ausgenutzte Schwachstellen

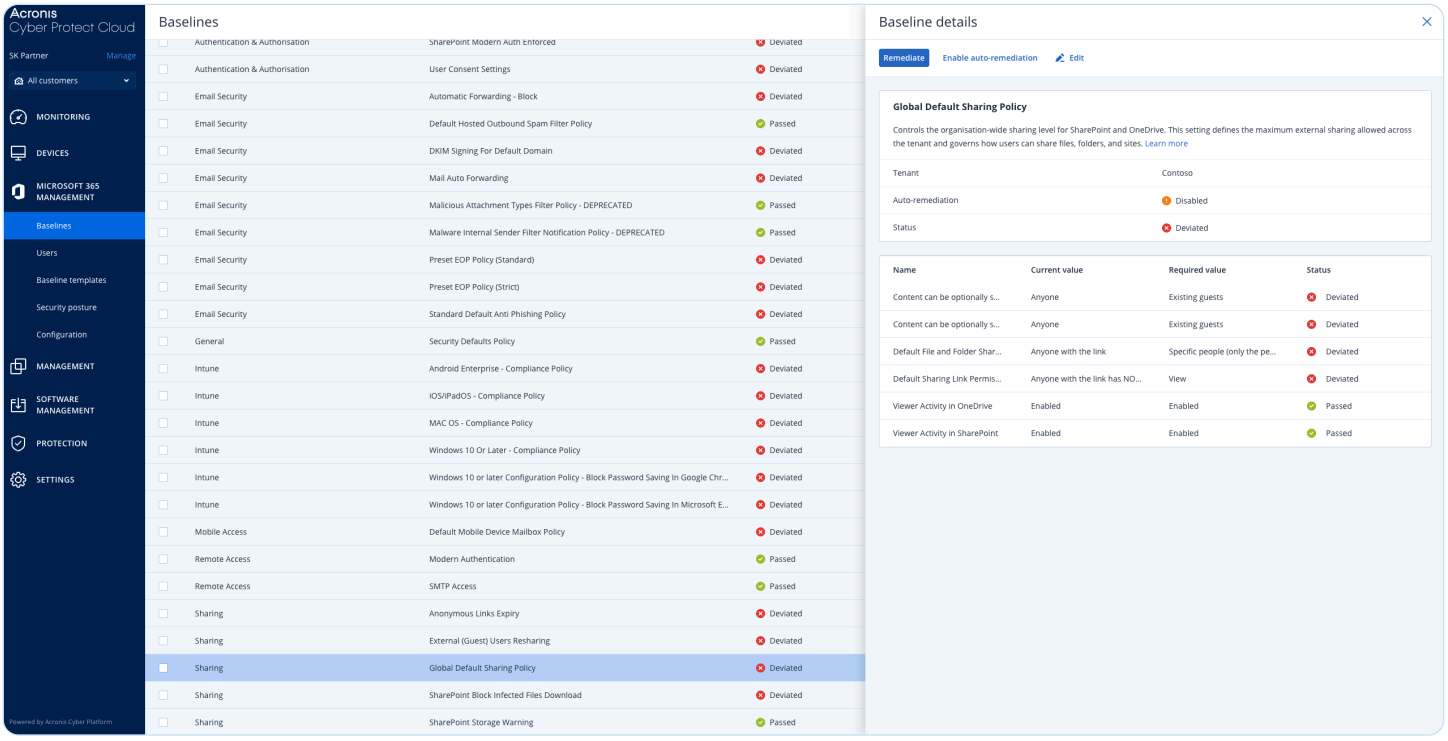
- Schwache Kontrollmechanismen für Freigaben
- Zu großzügige externe Zugriffseinstellungen

Sicherheitsmaßnahmen zur Risikominimierung

- Einrichtung unternehmensweiter Richtlinien für die externe Freigabe
- Einschränkung von Freigaben (falls erforderlich)
- Regelmäßige Überprüfung der Freigaberichtlinien

Acronis SPM bietet MSPs folgende Vorteile

- Kontinuierliche Validierung von Freigaberichtlinien gegenüber Baselines
- Erkennung riskanter Freigabekonfigurationen
- Langfristige Vermeidung von Konfigurationsabweichungen für alle Mandanten



Copyright © 2003–2026 Acronis International GmbH.

9. Lücken bei Audits und Untersuchungen

Realer Vorfall

Untersuchung von Sicherheitsvorfällen

Angriffstechnik

Bösartige Aktivitäten, die aufgrund unzureichender Audit-Maßnahmen nach einem Sicherheitsvorfall nicht erkannt wurden.

Ausgenutzte Schwachstellen

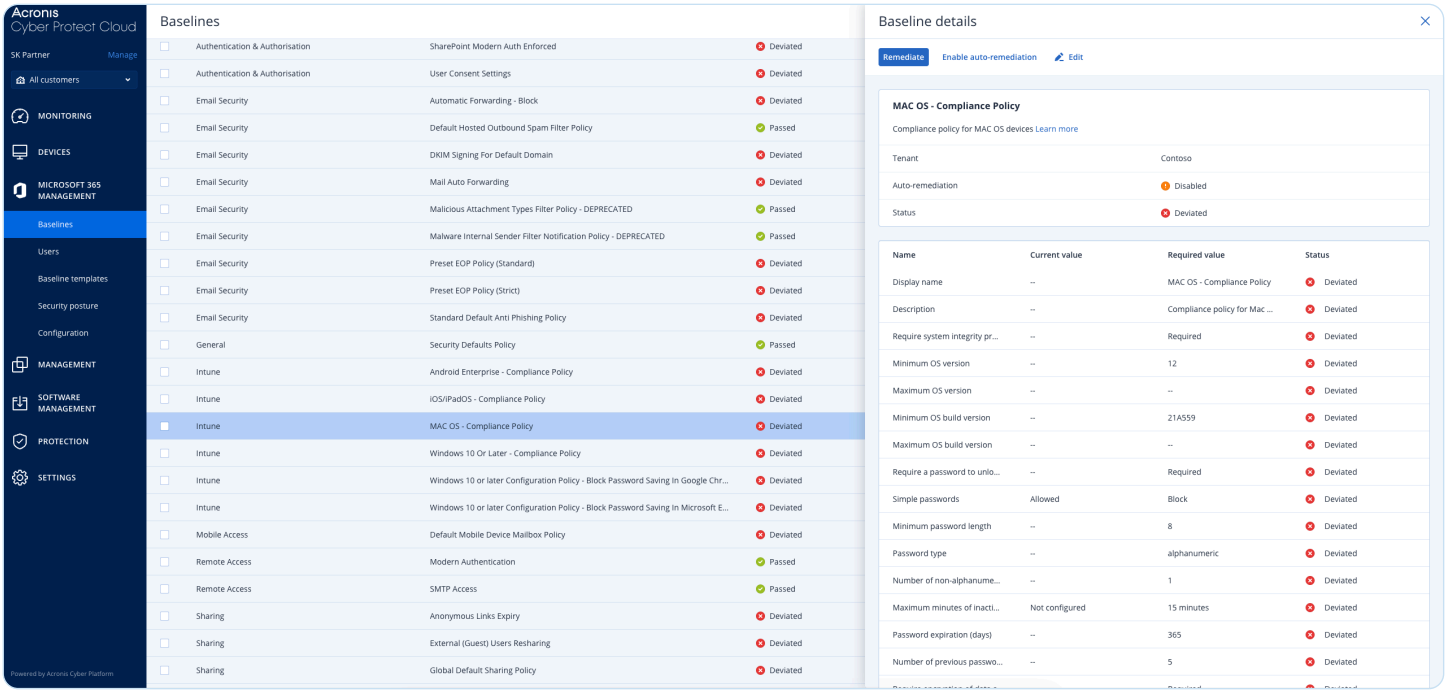
- Fehlende oder unvollständige Audit-Protokolle
- Mangelnde Audit-Bereitschaft

Sicherheitsmaßnahmen zur Risikominimierung

- Dauerhafte Aktivierung der Überwachung durch Microsoft Purview
- Erteilung der erforderlichen Zugriffsrechte an Audit-Teams
- Sicherstellung der Suchfunktionen für Audit-Bereitschaft

Acronis SPM bietet MSPs folgende Vorteile

- Überwachung auditrelevanter Konfigurationsrichtlinien
- Erkennung von Abweichungen in den Protokoll- und Audit-Einstellungen
- Unterstützung für laufende Untersuchungen und Compliance-Bereitschaft



Copyright © 2003–2026 Acronis International GmbH.

Was diese Angriffe gemeinsam haben

Alle Vorfälle weisen folgende Gemeinsamkeiten auf:

- Identitätsbasierte Infiltration
- Konfigurationsbasierte Persistenz
- Mandantenweite Auswirkungen
- Eingeschränkte Erkennung durch herkömmliche Endpunkt-Sicherheitstools

Warum ein kontinuierliches SPM wichtig ist

Moderne Microsoft 365-Angriffe sind aus den folgenden Gründen erfolgreich:

- Bestehende Fehlkonfigurationen
- Schleichende Verschlechterung der Sicherheitsstandards
- Vorhandensein unerkannter, mandantenübergreifender Sicherheitslücken

Wenn Prävention nicht ausreicht: Entra ID wiederherstellen

Mithilfe von Security Posture Management lassen sich Identitätsrisiken senken. Backups ermöglichen die Wiederherstellung der Identitätskontrollebene, sollte diese durch einen Angriff, versehentliches Löschen oder eine Fehlkonfiguration kompromittiert worden sein.

Warum die Wiederherstellbarkeit von Entra ID wichtig ist

Entra ID steuert den Zugriff auf Microsoft 365 und verbundene Apps. Erlangen Cyberkriminelle Zugriff auf Entra ID, können sie Benutzerkonten, Gruppen, Rollen, Richtlinien und Konfigurationen ändern oder löschen. Dadurch können sie ihre eigenen Berechtigungen erweitern, sich einen dauerhaften Zugriff sichern oder legitime Zugriffsversuche blockieren.

Werden nur die Microsoft 365-Daten und nicht auch die Entra ID-Daten wiederhergestellt, bleibt der Zugriff möglicherweise weiterhin kompromittiert. Unternehmen benötigen daher eine zuverlässige Wiederherstellungsmöglichkeit für die Identitäten, Einstellungen und Beziehungen, von denen ihre Umgebung abhängt.

Wie MSPs mit Acronis SPM Risiken reduzieren können

- Zentrale, mandantenübergreifende Verwaltung der Microsoft 365-Sicherheit
- Kontinuierliche Überwachung der Sicherheitsstandards im Vergleich zu Vorgaben
- Automatische Erkennung von neuen Risiken und Konfigurationsabweichungen
- Wiederverwendbare Baseline-Templates
- Automatisierung und Optimierung der Behebung
- Vereinfachte Onboarding- und Offboarding-Workflows
- Skalierbare Standardisierung der Sicherheitseinstellungen für Microsoft 365

Vorteile von Acronis Entra ID Backup

- Schutz wichtiger Entra ID-Daten wie Benutzerkonten, Gruppen, Rollen, Richtlinien und Konfigurationen
- Wiederherstellung gelöschter oder kompromittierter Identitätsobjekte und ihrer Beziehungen zueinander
- Unerwünschte Änderungen nach Angriffen oder Administratorfehler rückgängig machen
- Reduzierung von Ausfallzeiten und Unabhängigkeit von integrierten Aufbewahrungs- und Wiederherstellungsoptionen
- Zentrale Verwaltung des Schutzes von Microsoft 365-Daten und -Identitäten über die Acronis Plattform

Copyright © 2003–2026 Acronis International GmbH.

Resiliente Identitätsdaten

Kombinieren Sie proaktives Security Posture Management mit wiederherstellbaren Entra ID-Backups. So helfen Sie Ihren Kund:innen, identitätsbasierte Angriffe zu verhindern, deren Auswir-kungen zu begrenzen und sich schneller davon zu erholen.



Erfahren Sie mehr über Acronis Entra ID Backup

MEHR ERFAHREN

Möchten Sie erfahren, wie Acronis SPM den Schutz von Microsoft 365 skalierbar macht?

Dann scannen Sie jetzt den QR-Code und erleben Sie Acronis SPM in Aktion!



Copyright © 2003–2026 Acronis International GmbH. Alle Rechte vorbehalten. Acronis und das Acronis Logo sind eingetragene Markenzeichen der Acronis International GmbH in den Vereinigten Staaten und/oder in anderen Ländern. Alle anderen Marken oder eingetragenen Marken sind das Eigentum ihrer jeweiligen Inhaber. Technische Änderungen, Abweichungen bei den Abbildungen sowie Irrtümer sind vorbehalten. Oktober 2026