

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



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)

Acronis Cyber Protect Cloud

SK Partner

Manage

All customers

MONITORING

DEVICES

MICROSOFT 365 MANAGEMENT

Baselines

Users

Baseline templates

Security posture

Configuration

MANAGEMENT

SOFTWARE MANAGEMENT

PROTECTION

SETTINGS

Customer: Contoso

Category: All

Apply

Search

Category	Baseline	Status	
☐	Audit	Mailbox Audit Log	Passed
☐	Authentication & Authorisation	Admin Consent Workflow	Deviated
☐	Authentication & Authorisation	Authentication Method Policy - Email OTP	Deviated
☒	Authentication & Authorisation	Authentication Method Policy - Microsoft Authenticator	Deviated
☐	Authentication & Authorisation	Conditional Access Policy - Application Enforced Restrictions For Unmanaged D...	Deviated
☐	Authentication & Authorisation	Conditional Access Policy - Block Legacy Authentication	Deviated
☐	Authentication & Authorisation	Conditional Access Policy - Block Unknown Or Unsupported Device Access	Deviated
☐	Authentication & Authorisation	Conditional Access Policy - Enforce MFA	Deviated
☐	Authentication & Authorisation	Conditional Access Policy - No persistent Browser Sessions	Deviated
☐	Authentication & Authorisation	Conditional Access Policy - Require Approved Client Apps	Deviated
☐	Authentication & Authorisation	Conditional Access Policy - Require Compliant Or Hybrid Azure AD joined Device.	Deviated
☐	Authentication & Authorisation	Conditional Access Policy - Restrict Access To Azure Portal	Deviated
☐	Authentication & Authorisation	Conditional Access Policy - Restrict Access To Microsoft Admin Portal	Deviated
☐	Authentication & Authorisation	Conditional Access Policy - Securing Security Info Registration	Deviated
☐	Authentication & Authorisation	Conditional Access Policy - Sign-In Risk-Based Multifactor Authentication.	Deviated
☐	Authentication & Authorisation	Customer Lockbox	Deviated
☐	Authentication & Authorisation	Password Policy	Deviated
☐	Authentication & Authorisation	SharePoint Modern Auth Enforced	Deviated
☐	Authentication & Authorisation	User Consent Settings	Deviated
☐	Email Security	Automatic Forwarding - Block	Deviated
☐	Email Security	Default Hosted Outbound Spam Filter Policy	Passed

Baseline details

Remediate Enable auto-remediation Edit

Authentication Method Policy - Microsoft Authenticator

Controls how Microsoft Authenticator is used for push and passwordless authentication, which users it applies to, and whether additional security details (app name, location, companion apps) appear in authentication prompts. [Learn more](#)

Tenant

Contoso

Auto-remediation

Disabled

Status

Deviated

Name	Current value	Required value	Status
State	Enabled	Enabled	Passed
Allow use of Microsoft Auth...	Enabled	Disabled	Deviated
Include Targets	All Users Auth method (any)	All Users Auth method (any)	Passed
Exclude Targets	None	None	Passed
Show application name - Sta...	Default	Enabled	Deviated
Show application name - Inc...	All Users	All Users	Passed
Show application name - Ex...	--	--	Passed
Show geographic location - ...	Default	Enabled	Deviated
Show geographic location - L...	All Users	All Users	Passed
Show geographic location - ...	--	--	Passed
Companion applications - St...	Default	Enabled	Deviated
Companion applications - In...	All Users	All Users	Passed
Companion applications - E...	--	--	Passed

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

Acronis
Cyber Protect Cloud

SK Partner

MONITORING

DEVICES

MICROSOFT 365
MANAGEMENT

Baselines

Users

Baseline templates

Security posture

Configuration

MANAGEMENT

SOFTWARE
MANAGEMENT

PROTECTION

SETTINGS

Baselines

Customer: Contoso Category: All

Search

	Category	Baseline	Status
☐	Audit	Mailbox Audit Log	Passed
☐	Authentication & Authorisation	Admin Consent Workflow	Deviated
☐	Authentication & Authorisation	Authentication Method Policy - Email OTP	Deviated
☐	Authentication & Authorisation	Authentication Method Policy - Microsoft Authenticator	Deviated
☒	Authentication & Authorisation	Conditional Access Policy - Application Enforced Restrictions For Unmanaged D...	Deviated
☐	Authentication & Authorisation	Conditional Access Policy - Block Legacy Authentication	Deviated
☐	Authentication & Authorisation	Conditional Access Policy - Block Unknown Or Unsupported Device Access	Deviated
☐	Authentication & Authorisation	Conditional Access Policy - Enforce MFA	Deviated
☐	Authentication & Authorisation	Conditional Access Policy - No persistent Browser Sessions	Deviated
☐	Authentication & Authorisation	Conditional Access Policy - Require Approved Client Apps	Deviated
☐	Authentication & Authorisation	Conditional Access Policy - Require Compliant Or Hybrid Azure AD joined Device	Deviated
☐	Authentication & Authorisation	Conditional Access Policy - Restrict Access To Azure Portal	Deviated
☐	Authentication & Authorisation	Conditional Access Policy - Restrict Access To Microsoft Admin Portal	Deviated
☐	Authentication & Authorisation	Conditional Access Policy - Securing Security Info Registration	Deviated
☐	Authentication & Authorisation	Conditional Access Policy - Sign-In Risk-Based Multifactor Authentication	Deviated
☐	Authentication & Authorisation	Customer Lockbox	Deviated
☐	Authentication & Authorisation	Password Policy	Deviated
☐	Authentication & Authorisation	SharePoint Modern Auth Enforced	Deviated
☐	Authentication & Authorisation	User Consent Settings	Deviated
☐	Email Security	Automatic Forwarding - Block	Deviated

Baseline details

Remediate Enable auto-remediation Edit

Conditional Access Policy - Application Enforced Restrictions For Unmanaged Devices.

This Conditional Access Policy blocks or restricts access to SharePoint, OneDrive, and Exchange content from unmanaged devices. It helps prevent data leakage by ensuring that only managed and compliant devices can access sensitive organizational data. [Learn more](#)

Tenant	Contoso
Auto-remediation	Disabled
Status	Deviated

Name	Current value	Required value	Status
Display Name	---	CAP009 - Application Enforc...	Deviated
State	---	enabled	Deviated
Include Users	---	All	Deviated
Include Roles	---	---	Deviated
Include Groups	---	---	Deviated
Include Guest Or External U...	---	---	Deviated
Exclude Users	---	---	Deviated
Exclude Roles	---	---	Deviated
Exclude Groups	---	---	Deviated
Exclude Guest Or External U...	---	---	Deviated
Include Applications	---	Office365	Deviated
Session Control	---	Use app enforced restrictions	Deviated

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 Geräteebe



Sicherheitsmaßnahmen zur Risikominimierung

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

Acronis Cyber Protect Cloud

5K Partner

Manage

All customers

MONITORING

DEVICES

MICROSOFT 365 MANAGEMENT

Baselines

Users

Baseline templates

Security posture

Configuration

MANAGEMENT

SOFTWARE MANAGEMENT

PROTECTION

SETTINGS

Baselines

Customer: Contoso

Category: All

Apply

Search

Category	Baseline	Status
☐ Audit	Mailbox Audit Log	Passed
☐ Authentication & Authorisation	Admin Consent Workflow	Deviated
☐ Authentication & Authorisation	Authentication Method Policy - Email OTP	Deviated
☐ Authentication & Authorisation	Authentication Method Policy - Microsoft Authenticator	Deviated
☐ Authentication & Authorisation	Conditional Access Policy - Application Enforced Restrictions For Unmanaged D...	Deviated
☐ Authentication & Authorisation	Conditional Access Policy - Block Legacy Authentication	Deviated
☐ Authentication & Authorisation	Conditional Access Policy - Block Unknown Or Unsupported Device Access	Deviated
☐ Authentication & Authorisation	Conditional Access Policy - Enforce MFA	Deviated
☐ Authentication & Authorisation	Conditional Access Policy - No persistent Browser Sessions	Deviated
☒ Authentication & Authorisation	Conditional Access Policy - Require Approved Client Apps	Deviated
☐ Authentication & Authorisation	Conditional Access Policy - Require Compliant Or Hybrid Azure AD joined Device	Deviated
☐ Authentication & Authorisation	Conditional Access Policy - Restrict Access To Azure Portal	Deviated
☐ Authentication & Authorisation	Conditional Access Policy - Restrict Access To Microsoft Admin Portal	Deviated
☐ Authentication & Authorisation	Conditional Access Policy - Securing Security Info Registration	Deviated
☐ Authentication & Authorisation	Conditional Access Policy - Sign-In Risk-Based Multifactor Authentication	Deviated
☐ Authentication & Authorisation	Customer Lockbox	Deviated
☐ Authentication & Authorisation	Password Policy	Deviated
☐ Authentication & Authorisation	SharePoint Modern Auth Enforced	Deviated
☐ Authentication & Authorisation	User Consent Settings	Deviated
☐ Email Security	Automatic Forwarding - Block	Deviated

Baseline details

Remediate

Enable auto-remediation

Edit

Conditional Access Policy - Require Approved Client Apps

This Conditional Access Policy requires users to access resources only through approved client apps or apps protected by app protection policies. It helps ensure that organizational data is accessed securely and only through trusted applications. [Learn more](#)

Tenant	Contoso
Auto-remediation	Disabled
Status	Deviated

Name	Current value	Required value	Status
Display Name	---	CA007 - Require Approved ...	Deviated
State	---	enabled	Deviated
Include Users	---	All	Deviated
Include Roles	---	---	Deviated
Include Groups	---	---	Deviated
Include Guest Or External U...	---	---	Deviated
Exclude Users	---	---	Deviated
Exclude Roles	---	---	Deviated
Exclude Groups	---	---	Deviated
Exclude Guest Or External U...	---	---	Deviated
Grant	---	approvedApplication,compl...	Deviated
Include Platforms	---	android,iOS	Deviated
Client App Types	---	all	Deviated

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

Acronis Cyber Protect Cloud

SK Partner

Manage

All customers

MONITORING

DEVICES

MICROSOFT 365 MANAGEMENT

Security posture

Users

Baselines

Baseline templates

Configuration

MANAGEMENT

SOFTWARE MANAGEMENT

PROTECTION

SETTINGS

Baselines

Customer: Contoso

Category: All

Apply

Search

Category	Baseline	Status
☐ Audit	Mailbox Audit Log	Passed
☐ Authentication & Authorisation	Admin Consent Workflow	Deviated
☐ Authentication & Authorisation	Authentication Method Policy - Email OTP	Deviated
☐ Authentication & Authorisation	Authentication Method Policy - Microsoft Authenticator	Deviated
☐ Authentication & Authorisation	Conditional Access Policy - Application Enforced Restrictions For Unmanaged D...	Deviated
☐ Authentication & Authorisation	Conditional Access Policy - Block Legacy Authentication	Deviated
☐ Authentication & Authorisation	Conditional Access Policy - Block Unknown Or Unsupported Device Access	Deviated
☐ Authentication & Authorisation	Conditional Access Policy - Enforce MFA	Deviated
☐ Authentication & Authorisation	Conditional Access Policy - No persistent Browser Sessions	Deviated
☐ Authentication & Authorisation	Conditional Access Policy - Require Approved Client Apps	Deviated
☐ Authentication & Authorisation	Conditional Access Policy - Require Compliant Or Hybrid Azure AD joined Device	Deviated
☐ Authentication & Authorisation	Conditional Access Policy - Restrict Access To Azure Portal	Deviated
☐ Authentication & Authorisation	Conditional Access Policy - Restrict Access To Microsoft Admin Portal	Deviated
☐ Authentication & Authorisation	Conditional Access Policy - Securing Security Info Registration	Deviated
☐ Authentication & Authorisation	Conditional Access Policy - Sign-In Risk-Based Multifactor Authentication	Deviated
☐ Authentication & Authorisation	Customer Lockbox	Deviated
☐ Authentication & Authorisation	Password Policy	Deviated
☐ Authentication & Authorisation	SharePoint Modern Auth Enforced	Deviated
☐ Authentication & Authorisation	User Consent Settings	Deviated
☐ Email Security	Automatic Forwarding - Block	Deviated
☐ Email Security	Default Hosted Outbound Spam Filter Policy	Passed

Baseline details

Remediate

Enable auto-remediation

Edit

Conditional Access Policy - No persistent Browser Sessions

This Conditional Access Policy prevents users from maintaining persistent browser sessions, requiring them to re-authenticate more frequently. It helps reduce the risk of unauthorized access from shared or unmanaged devices. [Learn more](#)

Tenant

Contoso

Auto-remediation

Disabled

Status

Deviated

Name	Current value	Required value	Status
Display Name	---	CAPO03 - Prevent Persistent...	Deviated
State	---	enabled	Deviated
Include Users	---	All	Deviated
Include Roles	---	---	Deviated
Include Groups	---	---	Deviated
Include Guest Or External U...	---	---	Deviated
Exclude Users	---	---	Deviated
Exclude Roles	---	---	Deviated
Exclude Groups	---	---	Deviated
Exclude Guest Or External U...	---	---	Deviated
Persistent Browser	---	never	Deviated

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

Acronis Cyber Protect Cloud

SK Partner

Manage

All customers

MONITORING

DEVICES

MICROSOFT 365 MANAGEMENT

Baselines

Security posture

Users

Baseline templates

Configuration

MANAGEMENT

SOFTWARE MANAGEMENT

PROTECTION

SETTINGS

Baselines

Customer: Contoso

Category: All

Apply

Search

Category	Baseline	Status	
☐	Audit	Mailbox Audit Log	Passed
☐	Authentication & Authorisation	Admin Consent Workflow	Deviated
☐	Authentication & Authorisation	Authentication Method Policy - Email OTP	Deviated
☐	Authentication & Authorisation	Authentication Method Policy - Microsoft Authenticator	Deviated
☐	Authentication & Authorisation	Conditional Access Policy - Application Enforced Restrictions For Unmanaged D...	Deviated
☐	Authentication & Authorisation	Conditional Access Policy - Block Legacy Authentication	Deviated
☐	Authentication & Authorisation	Conditional Access Policy - Block Unknown Or Unsupported Device Access	Deviated
☐	Authentication & Authorisation	Conditional Access Policy - Enforce MFA	Deviated
☐	Authentication & Authorisation	Conditional Access Policy - No persistent Browser Sessions	Deviated
☐	Authentication & Authorisation	Conditional Access Policy - Require Approved Client Apps	Deviated
☐	Authentication & Authorisation	Conditional Access Policy - Require Compliant Or Hybrid Azure AD joined Device...	Deviated
☐	Authentication & Authorisation	Conditional Access Policy - Restrict Access To Azure Portal	Deviated
☐	Authentication & Authorisation	Conditional Access Policy - Restrict Access To Microsoft Admin Portal	Deviated
☐	Authentication & Authorisation	Conditional Access Policy - Securing Security Info Registration	Deviated
☐	Authentication & Authorisation	Conditional Access Policy - Sign-In Risk-Based Multifactor Authentication...	Deviated
☐	Authentication & Authorisation	Customer Lockbox	Deviated
☐	Authentication & Authorisation	Password Policy	Deviated
☐	Authentication & Authorisation	SharePoint Modern Auth Enforced	Deviated
☐	Authentication & Authorisation	User Consent Settings	Deviated
☐	Email Security	Automatic Forwarding - Block	Deviated
☐	Email Security	Default Hosted Outbound Spam Filter Policy	Passed

Baseline details

Remediate

Enable auto-remediation

Edit

Conditional Access Policy - Block Unknown Or Unsupported Device Access

Users will be blocked from accessing company resources when the device type is unknown or unsupported. [Learn more](#)

Tenant	Contoso
Auto-remediation	Disabled
Status	Deviated

Name	Current value	Required value	Status
Display Name	---	CA004 - Enforce Block Unk...	Deviated
State	---	enabled	Deviated
Include Users	---	All	Deviated
Include Roles	---	---	Deviated
Include Groups	---	---	Deviated
Include Guest Or External U...	---	---	Deviated
Exclude Users	---	---	Deviated
Exclude Roles	---	---	Deviated
Exclude Groups	---	---	Deviated
Exclude Guest Or External U...	---	---	Deviated
Include Platforms	---	All,all	Deviated
Exclude Platforms	---	android,iOS,macOS,windows	Deviated
Grant Controls	---	block	Deviated

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

The screenshot displays the Acronis Cyber Protect Cloud interface. The left sidebar contains navigation options: SK Partner, Manage, All customers, MONITORING, DEVICES, MICROSOFT 365 MANAGEMENT, Configuration, Security posture (selected), Baseline templates, Baselines, Users, MANAGEMENT, SOFTWARE MANAGEMENT, PROTECTION, and SETTINGS.

The main content area is divided into two panels:

- Security posture:** Shows 1 tenant and 35 tenant baseline deviations. A table lists tenants with columns for Name, Tenant baselines, and Users. The tenant 'Contoso' is highlighted, showing 35 deviations and 34 users.
- Risk dashboard:** Provides a summary of baseline and user account risks.

Baselines		
Tenant baselines	8 passed	35 deviated

Baseline categories		
Audit	1 passed	0 deviated
Authentication & Authorisation	0 passed	18 deviated
Email Security	3 passed	6 deviated
General	1 passed	0 deviated
Intune	0 passed	6 deviated
Mobile Access	0 passed	1 deviated
Remote Access	2 passed	0 deviated
Sharing	1 passed	4 deviated

User account risks	
MFA	29 affected user accounts
Admin mailboxes	6 affected user accounts
Anonymous admins	6 affected user accounts
Shared mailboxes	1 affected user account
Dormant accounts	No affected user accounts
Dormant admins	No affected user accounts
Guests	No affected user accounts

7. Rechteauserweiterung und Missbrauch von Rollen mit übermäßigen Berechtigungen



Realer Vorfall

Mehrere Vorfälle von Entra ID-Rechteauserweiterungen (Midnight Blizzard)



Sicherheitsmaßnahmen zur Risikominimierung

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



Angriffstechnik

Es wurden übermäßige Administratorrechte ausgenutzt, um die Rechte auszuweiten.



Acronis SPM bietet MSPs folgende Vorteile

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



Ausgenutzte Schwachstellen

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

Compliance Posture Summary

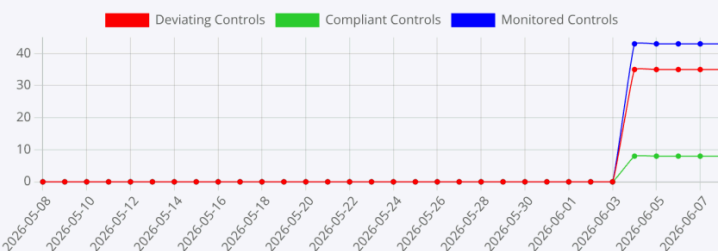
Baselines

Current Posture Summary (All time)

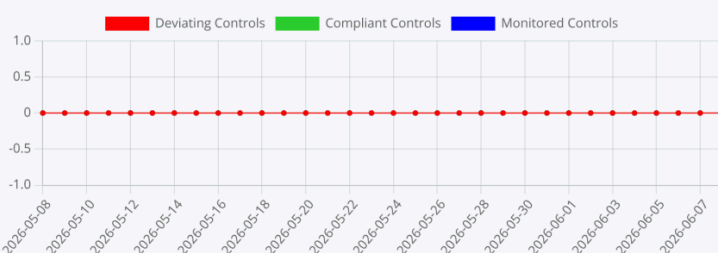
Tenant		Group	
Passing:	8	Passing:	-
Deviating:	35	Deviating:	-

Posture Summary (In this period) *

Tenant Baselines Posture Summary Chart



Group Baselines Posture Summary Chart



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

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

Acronis Cyber Protect Cloud

SK Partner Manage

All customers

MONITORING

DEVICES

MICROSOFT 365 MANAGEMENT

Baselines

Users

Baseline templates

Security posture

Configuration

MANAGEMENT

SOFTWARE MANAGEMENT

PROTECTION

SETTINGS

Baselines

☐	Authentication & Authorisation	SharePoint Modern Auth Enforced	Deviated
☐	Authentication & Authorisation	User Consent Settings	Deviated
☐	Email Security	Automatic Forwarding - Block	Deviated
☐	Email Security	Default Hosted Outbound Spam Filter Policy	Passed
☐	Email Security	DKIM Signing For Default Domain	Deviated
☐	Email Security	Mail Auto Forwarding	Deviated
☐	Email Security	Malicious Attachment Types Filter Policy - DEPRECATED	Passed
☐	Email Security	Malware Internal Sender Filter Notification Policy - DEPRECATED	Passed
☐	Email Security	Preset EOP Policy (Standard)	Deviated
☐	Email Security	Preset EOP Policy (Strict)	Deviated
☐	Email Security	Standard Default Anti Phishing Policy	Deviated
☐	General	Security Defaults Policy	Passed
☐	Intune	Android Enterprise - Compliance Policy	Deviated
☐	Intune	iOS/iPadOS - Compliance Policy	Deviated
☐	Intune	MAC OS - Compliance Policy	Deviated
☐	Intune	Windows 10 Or Later - Compliance Policy	Deviated
☐	Intune	Windows 10 or later Configuration Policy - Block Password Saving in Google Chr...	Deviated
☐	Intune	Windows 10 or later Configuration Policy - Block Password Saving in Microsoft E...	Deviated
☐	Mobile Access	Default Mobile Device Mailbox Policy	Deviated
☐	Remote Access	Modern Authentication	Passed
☐	Remote Access	SMTP Access	Passed
☐	Sharing	Anonymous Links Expiry	Deviated
☐	Sharing	External (Guest) Users Resharing	Deviated
☒	Sharing	Global Default Sharing Policy	Deviated
☐	Sharing	SharePoint Block Infected Files Download	Deviated
☐	Sharing	SharePoint Storage Warning	Passed

Baseline details

Remediate Enable auto-remediation Edit

Global Default Sharing Policy

Controls the organisation-wide sharing level for SharePoint and OneDrive. This setting defines the maximum external sharing allowed across the tenant and governs how users can share files, folders, and sites. [Learn more](#)

Tenant	Contoso
Auto-remediation	Disabled
Status	Deviated

Name	Current value	Required value	Status
Content can be optionally s...	Anyone	Existing guests	Deviated
Content can be optionally s...	Anyone	Existing guests	Deviated
Default File and Folder Shar...	Anyone with the link	Specific people (only the pe...	Deviated
Default Sharing Link Permis...	Anyone with the link has NO...	View	Deviated
Viewer Activity in OneDrive	Enabled	Enabled	Passed
Viewer Activity in SharePoint	Enabled	Enabled	Passed

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

Acronis Cyber Protect Cloud

SK Partner

Manage

All customers

MONITORING

DEVICES

MICROSOFT 365 MANAGEMENT

Baselines

Users

Baseline templates

Security posture

Configuration

MANAGEMENT

SOFTWARE MANAGEMENT

PROTECTION

SETTINGS

Baselines

☐	Authentication & Authorisation	SharePoint Modern Auth Enforced	Deviated
☐	Authentication & Authorisation	User Consent Settings	Deviated
☐	Email Security	Automatic Forwarding - Block	Deviated
☐	Email Security	Default Hosted Outbound Spam Filter Policy	Passed
☐	Email Security	DKIM Signing For Default Domain	Deviated
☐	Email Security	Mail Auto Forwarding	Deviated
☐	Email Security	Malicious Attachment Types Filter Policy - DEPRECATED	Passed
☐	Email Security	Malware Internal Sender Filter Notification Policy - DEPRECATED	Passed
☐	Email Security	Preset EOP Policy (Standard)	Deviated
☐	Email Security	Preset EOP Policy (Strict)	Deviated
☐	Email Security	Standard Default Anti Phishing Policy	Deviated
☐	General	Security Defaults Policy	Passed
☐	Intune	Android Enterprise - Compliance Policy	Deviated
☐	Intune	iOS/iPadOS - Compliance Policy	Deviated
☒	Intune	MAC OS - Compliance Policy	Deviated
☐	Intune	Windows 10 Or Later - Compliance Policy	Deviated
☐	Intune	Windows 10 or later Configuration Policy - Block Password Saving in Google Chr...	Deviated
☐	Intune	Windows 10 or later Configuration Policy - Block Password Saving in Microsoft E...	Deviated
☐	Mobile Access	Default Mobile Device Mailbox Policy	Deviated
☐	Remote Access	Modern Authentication	Passed
☐	Remote Access	SMTP Access	Passed
☐	Sharing	Anonymous Links Expiry	Deviated
☐	Sharing	External (Guest) Users Resharing	Deviated
☐	Sharing	Global Default Sharing Policy	Deviated

Baseline details

Remediate

Enable auto-remediation

Edit

MAC OS - Compliance Policy

Compliance policy for MAC OS devices [Learn more](#)

Tenant

Contoso

Auto-remediation

Disabled

Status

Deviated

Name	Current value	Required value	Status
Display name	—	MAC OS - Compliance Policy	Deviated
Description	—	Compliance policy for Mac ...	Deviated
Require system integrity pr...	—	Required	Deviated
Minimum OS version	—	12	Deviated
Maximum OS version	—	—	Deviated
Minimum OS build version	—	21A559	Deviated
Maximum OS build version	—	—	Deviated
Require a password to unlo...	—	Required	Deviated
Simple passwords	Allowed	Block	Deviated
Minimum password length	—	8	Deviated
Password type	—	alphanumeric	Deviated
Number of non-alphanume...	—	1	Deviated
Maximum minutes of inacti...	Not configured	15 minutes	Deviated
Password expiration (days)	—	365	Deviated
Number of previous passwo...	—	5	Deviated

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

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

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!

