Acronis

Microsoft 365 im Visier von Cyberkriminellen: Bedrohungen für die Identitäts- und Kontrollebene

Erfahren Sie, wie Acronis Security Posture Management sie aufdeckt und behebt

Einleitung

Microsoft 365 hat sich zur zentralen Steuerungsinstanz moderner Geschäftsabläufe entwickelt. Die Plattform verwaltet unternehmensübergreifend Identitäten, Zugriffsrechte, Kommunikation und Daten. Je wichtiger Microsoft 365 für Unternehmen wird, desto attraktiver wird es allerdings auch als primäre Angriffsfläche.

Die Art der Angriffe hat sich jedoch grundlegend verändert.

Die Bedrohungen von heute setzen nicht mehr auf Malware oder die Kompromittierung von Endpunkten. Stattdessen nutzen Cyberkriminelle Identitäten, Berechtigungen und Fehlkonfigurationen aus und agieren dabei vollständig innerhalb der legitimen Microsoft 365-Services. Ein einziges kompromittiertes Administratorkonto, eine übersehene Berechtigung oder eine unzureichende Richtlinie für den bedingten Zugriff reicht aus, um Cyberkriminellen dauerhaften Zugriff mit weitreichenden Folgen zu verschaffen – ohne dass herkömmliche Sicherheitssoftware Alarm schlägt.

Dieser Wandel stellt Managed Service Provider (MSPs) vor enorme Herausforderungen. Herkömmliche Sicherheitssoftware erkennt diese Angriffe oft nur begrenzt, während Fehlkonfigurationen und uneinheitliche Richtlinien zwischen den Mandanten anhaltende Sicherheitsrisiken verursachen.

Die Folge: Die Sicherheitsrisiken wachsen für alle Mandanten unbemerkt.

Dieser Leitfaden bietet eine praktische, an konkreten Fallbeispielen orientierte Schritt-für-Schritt-Anleitung, die zeigt, wie moderne Microsoft 365-Angriffe ablaufen und wie Acronis Security Posture Management (SPM) MSPs dabei unterstützt, diese Angriffe zu erkennen, zu verhindern und zu beheben.

Die neue Realität: Der Angriff hat bereits begonnen

Sie loggen sich in einen Kundenmandanten ein. Es sind weder Alarme noch Malware noch offensichtliche Anzeichen einer Kompromittierung vorhanden. Auf den ersten Blick scheint alles normal, doch das bedeutet nicht, dass die Umgebung sicher ist.

Cyberkriminelle könnten bereits Zugriff erlangt haben. Möglicherweise nutzen sie gültige Anmeldedaten oder dauerhafte Token, die sie durch Phishing oder den Missbrauch von Zustimmungen erlangt haben. Noch besorgniserregender ist die Möglichkeit, dass sie bereits vollständig innerhalb von Microsoft 365 agieren, ihre Aktivitäten in legitime Vorgänge einbetten und herkömmliche Erkennungsmechanismen umgehen.

Moderne Angriffe zielen nicht mehr auf das Eindringen in ein System ab, sondern finden direkt auf der Kontrollebene statt.

MSPs sehen sich einer grundlegend neuen Problematik gegenüber. Es geht nicht mehr nur darum, aktive Bedrohungen zu erkennen. Vielmehr müssen Sicherheitslücken identifiziert werden, bevor sie ausgenutzt werden können. Diese müssen dann konsistent über alle Mandanten hinweg behoben werden. Zudem muss sichergestellt werden, dass die Schutzmaßnahmen auch langfristig durchgesetzt werden können, während sich die Umgebungen weiterentwickeln.

Diese Schritt-für-Schritt-Anleitung zeigt, wie Acronis SPM diese Herausforderungen in der Praxis bewältigt.

Szenario 1

Password Spraying

„Es sieht alles okay aus, aber ein Konto wurde gerade kompromittiert.“

Cyberkriminelle müssen sich nicht mehr ins System hacken, sondern können sich ganz einfach anmelden. Indem sie gängige Passwörter für eine Vielzahl von Konten ausprobieren, umgehen sie eine Sperrung. Es ist nur eine Frage der Zeit, bis sie Zugang zu einem Konto erhalten. Mit den gültigen Anmeldedaten können sie auf Postfächer und Dateien zugreifen und sich wie legitime Benutzer:innen verhalten.

In der Regel gibt es keine Alarme, keine Malware-Erkennungen und keine eindeutigen Hinweise – alles sieht ganz normal aus.

Acronis SPM verlagert den Schwerpunkt deshalb von der Erkennung von Bedrohungen auf die Offenlegung von Risiken. Die Lösung zeigt Risiken wie fehlende Mehrfaktor-Authentifizierung (MFA), aktivierte veraltete Authentifizierungsmethoden und von den Best Practices abweichende Identitätskonfigurationen auf.

Auf dieser Grundlage wird die Sicherheit der Mandanten bewertet, die MFA wird durchgesetzt und veraltete Authentifizierungsmethoden werden deaktiviert. Mithilfe von Baseline-Templates können diese Sicherheitsmaßnahmen anschließend auf alle Mandanten angewendet werden. Eine kontinuierliche Überwachung stellt sicher, dass jede Abweichung von den Vorgaben erkannt und korrigiert wird.

So beseitigen Sie von vornherein die Voraussetzungen für solche Angriffe, anstatt einem kompromittierten Konto hinterherzujagen.

Vorgehensweise (in der Plattform)

1 **Audit on demand ausführen**
- Sofortige Bewertung des Mandanten anhand der Sicherheits-Baselines
- Identifizierung von Authentifizierungsschwachstellen

2 **Baseline-Behebung anwenden**
- Durchsetzung von MFA für alle Benutzenden
- Deaktivierung veralteter Authentifizierungsmethoden

3 **Mandantenübergreifende Automatisierung**
- Verwendung von Baseline-Templates
- Anwendung der optimierten Richtlinien auf alle Kundenunternehmen

4 **Kontinuierliche Überwachung aktivieren**
- Kontinuierliche Überwachung auf Baseline-Abweichungen durch Acronis SPM
- Benachrichtigung bei Erstellung neuer ungeschützter Benutzerkonten

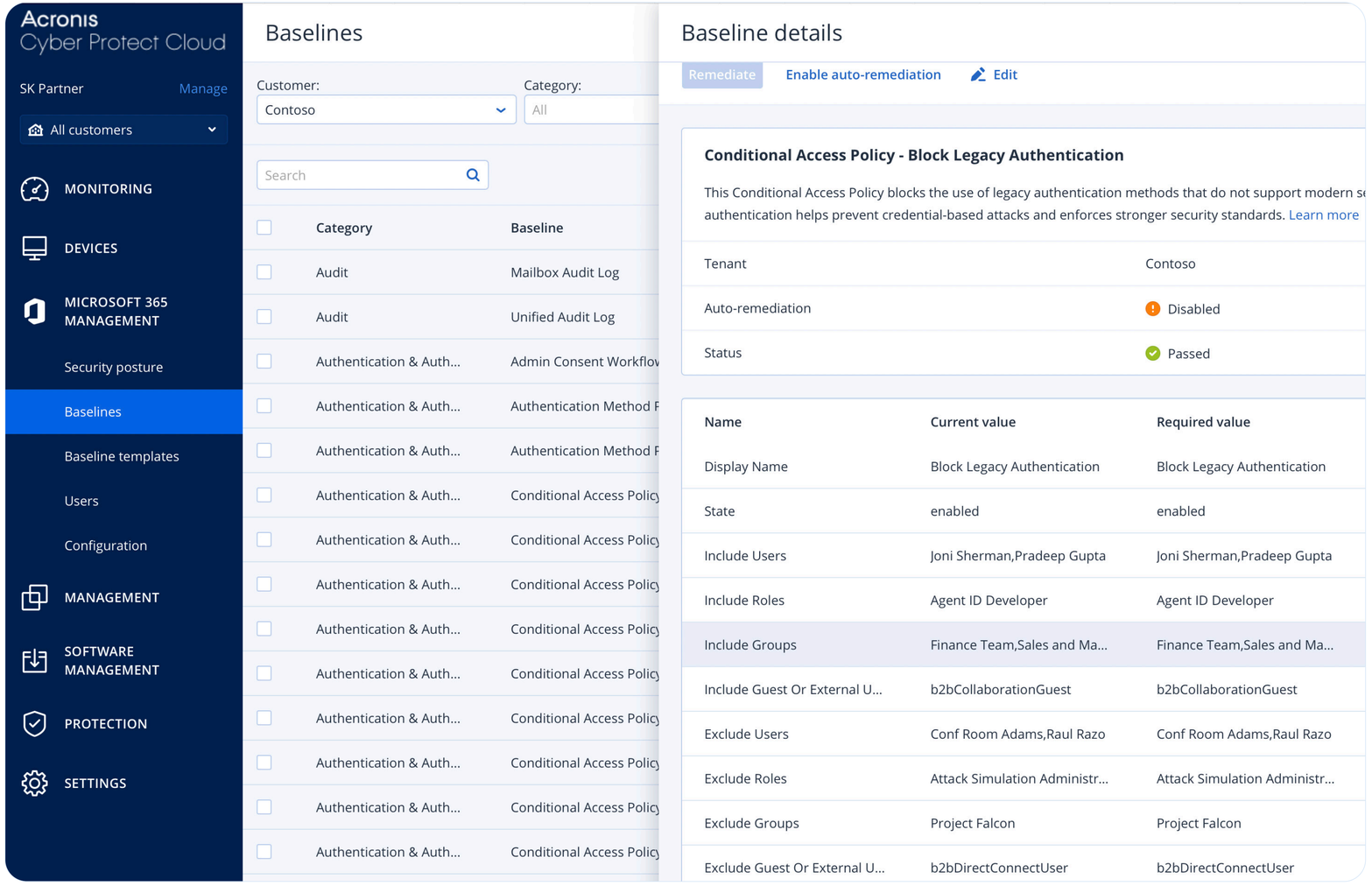
Was ist passiert?

Sie haben den Anmeldeversuch nicht nachverfolgt.

Was haben Sie gemacht:

- Sie haben systemische Identitätslücken identifiziert.
- Sie haben sie behoben.
- Sie haben sie für alle Mandanten konsistent durchgesetzt.
- Sie haben dafür gesorgt, dass sie nicht erneut auftreten.

Acronis SPM beseitigt die Voraussetzungen für erfolgreiche Password Spraying-Angriffe auf alle Ihre Mandanten.



Szenario 2

Missbrauch von OAuth-Zustimmungen

„Cyberkriminelle brauchen keine Anmeldedaten mehr.“

Ohne es zu wissen, genehmigen Benutzer:innen eine manipulierte OAuth-App. In diesem Fall benötigen Cyberkriminelle in Zukunft keine Anmeldedaten mehr. Über Microsoft Graph erhalten sie auf API-Ebene permanenten Zugriff auf E-Mails und Dateien, ohne dass dabei in der Regel ein Alarm ausgelöst wird.

Dabei werden keine Anmeldedaten kompromittiert und es gibt keine verdächtigen Anmeldeaktivitäten – alles wirkt legitim.

Acronis SPM macht dieses verborgene Risiko sichtbar. Die Lösung bietet mandantenübergreifende Transparenz für alle OAuth-Apps sowie für die gewährten Berechtigungen, beispielsweise „Mail.Read“ oder „Files.Read.All“. Sie warnt auch vor riskanten oder unbekannten Apps.

So können Sie Apps mit weitreichenden Berechtigungen oder neu hinzugefügte Apps schnell identifizieren und deren Berechtigungen widerrufen, um den unbefugten Zugriff zu unterbinden. Anschließend können Sie Richtlinien standardisieren, wodurch die Benutzerzustimmung eingeschränkt wird und eine Administratorfreigabe erforderlich ist. Die Automatisierung stellt sicher, dass diese Kontrollen in allen Mandanten durchgesetzt werden.

Anstatt identitätsbasierten Bedrohungen hinterherzujagen, können Sie dauerhafte Zugriffe auf App-Ebene aufdecken, beseitigen und ein erneutes Auftreten verhindern.

Vorgehensweise (in der Plattform)

1 **Riskante Apps identifizieren**
- Herausfiltern von Apps mit weitreichenden Berechtigungen
- Erkennung neu hinzugefügter oder unbekannter Apps

2 **Sofortige Behebung**
- Entzug der App-Berechtigungen
- Entfernung nicht autorisierter Integrationen

3 **Richtlinie standardisieren**
- Einschränkung der Benutzerzustimmung
- Administratorfreigabe erforderlich machen

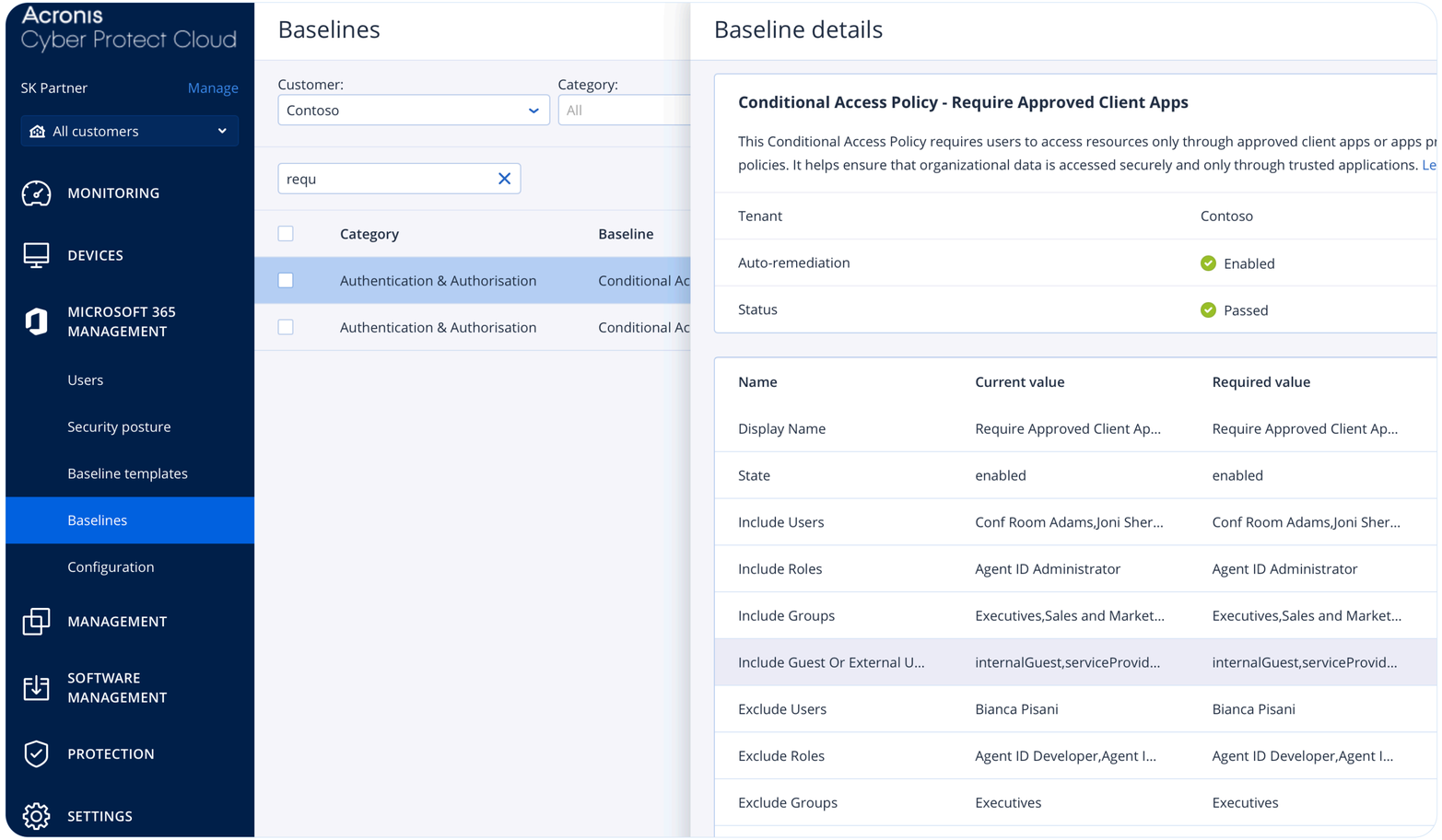
4 **Durchsetzung automatisieren**
- Anwendung von Governance-Richtlinien für Apps in allen Mandanten
- Automatische Erkennung neuer riskanter Apps

Was ist passiert?

Was haben Sie gemacht:

- Sie haben einen dauerhaften Zugriff gefunden, der die Identitätsprüfung umgeht.
- Sie haben ihn sofort entfernt.
- Sie haben dafür gesorgt, dass dieser nicht erneut auftritt.

Acronis SPM schafft Transparenz und Kontrolle über die App-Ebene, die Cyberkriminelle nutzen, um sich langfristigen Zugriff zu verschaffen.



Szenario 3

Device-Code-Phishing

„Die MFA hat funktioniert, aber die Cyberkriminellen sind trotzdem reingekommen.“

Ein:e Benutzer:in meldet sich ordnungsgemäß bei Microsoft an und durchläuft die MFA. Cyberkriminelle fangen jedoch das Authentifizierungstoken ab. Damit erhalten sie dauerhaften Zugriff auf das Postfach. Sie können E-Mails lesen und Postfachregeln erstellen, ohne dabei einen Alarm auszulösen.

Da es keine fehlgeschlagenen Anmeldeversuche gibt, scheint die MFA ordnungsgemäß zu funktionieren.

Acronis SPM macht die eigentliche Problematik jedoch sichtbar: Lücken in den Sicherheitsrichtlinien. Die Lösung deckt unzureichende oder fehlende Richtlinien für den bedingten Zugriff, fehlende Sitzungskontrollen sowie Identitätskonfigurationen, die von den Best Practices abweichen, auf.

Auf dieser Grundlage können Sie strengere Richtlinien für den bedingten Zugriff durchsetzen, Sitzungsbeschränkungen anwenden und diese Kontrollen einheitlich auf alle Mandanten anwenden. Eine kontinuierliche Überwachung stellt sicher, dass jede Abweichung von den Vorgaben erkannt und korrigiert wird.

Sie decken also nicht nur Token-Missbrauch auf, sondern beseitigen auch die Voraussetzungen dafür.

Vorgehensweise (in der Plattform)

1 **Baseline-Compliance-Check ausführen**
- Vergleich von Mandantenrichtlinien mit den Best Practices

2 **Identitätskontrollen durchsetzen**
- Stärkung des bedingten Zugangs
- Anwendung von Sitzungsbeschränkungen

3 **Behebung automatisieren**
- Anwendung von Richtlinien auf alle Mandanten
- Automatische Korrektur von Abweichungen

4 **Kontinuierliche Durchsetzung sichern**
- Überwachung auf Richtlinienabweichungen durch Acronis SPM
- Meldung jeder Schwächung der Kontrollen

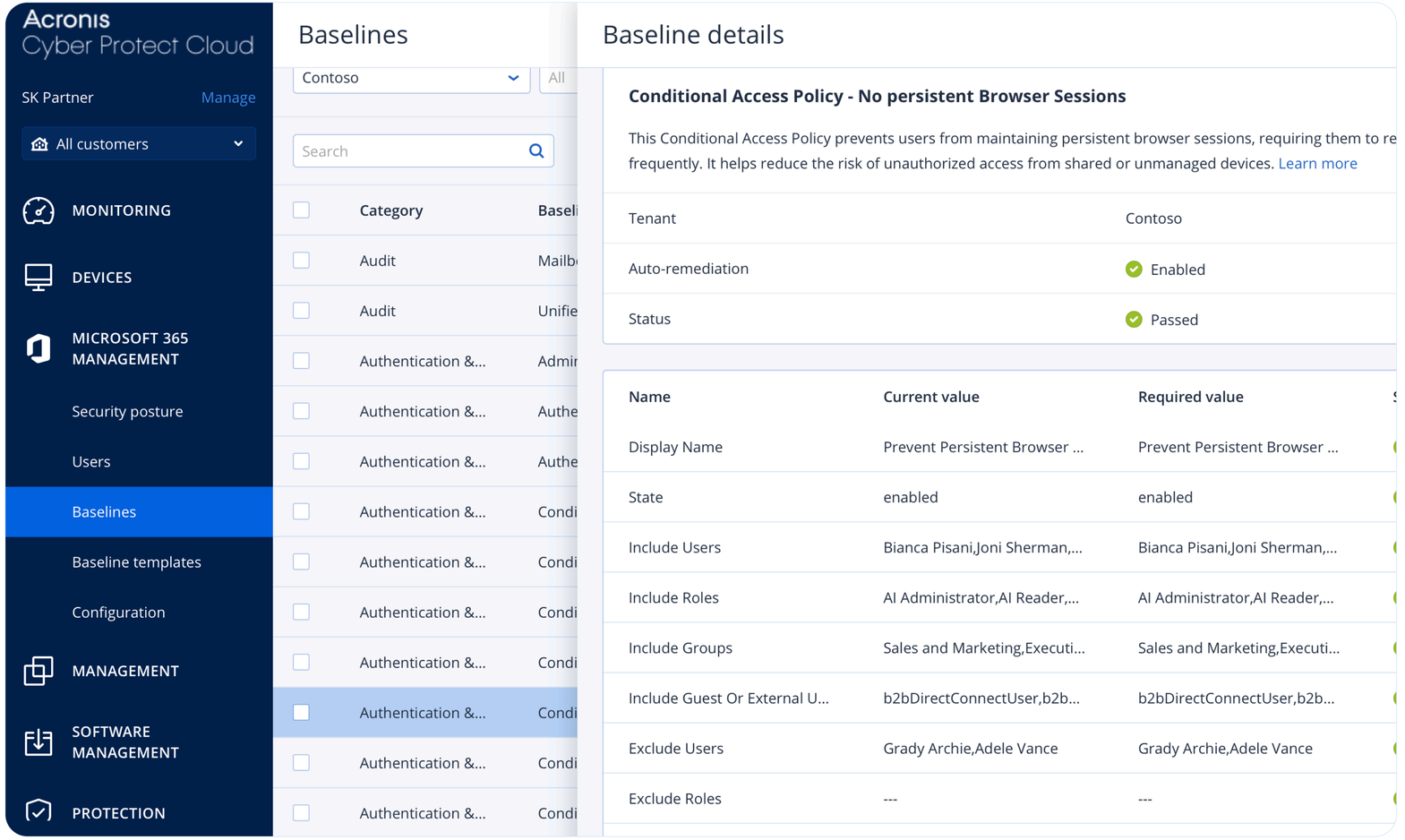
Was ist passiert?

Sie haben den Token-Diebstahl nicht erkannt.

Was haben Sie gemacht:

- Sie haben die Richtlinienlücken geschlossen, die dies ermöglicht haben.
- Sie haben die Kontrollen mandantenübergreifend standardisiert.
- Sie haben dafür gesorgt, dass die Kontrollen dauerhaft durchgesetzt werden.

Acronis SPM schützt sowohl Identitäten als auch Authentifizierungsabläufe.



Szenario 4

Rechteausweitung

„Ein Benutzerkonto wird zum gesamten Mandanten.“

Cyberkriminellen ist es gelungen, ein einziges Benutzerkonto zu kompromittieren und mit der Erkundung zu beginnen. Dabei entdecken sie übermäßige Rechte, mehrere globale Administratoren sowie eine schwache Rollentrennung. Das Ergebnis: Sie konnten ohne großen Aufwand die vollständige Kontrolle über den Mandanten übernehmen.

In der Regel verursacht dieses Szenario keine Warnmeldungen. Die Rechteausweitung geschieht schrittweise und bleibt ohne zentrale Transparenz unbemerkt.

Acronis SPM macht dieses Risiko jedoch deutlich sichtbar, indem es Administratorrollen mandantenübergreifend aufzeigt, Konten mit übermäßigen Berechtigungen identifiziert und das Risiko entsprechend einstuft.

Vorgehensweise (in der Plattform)

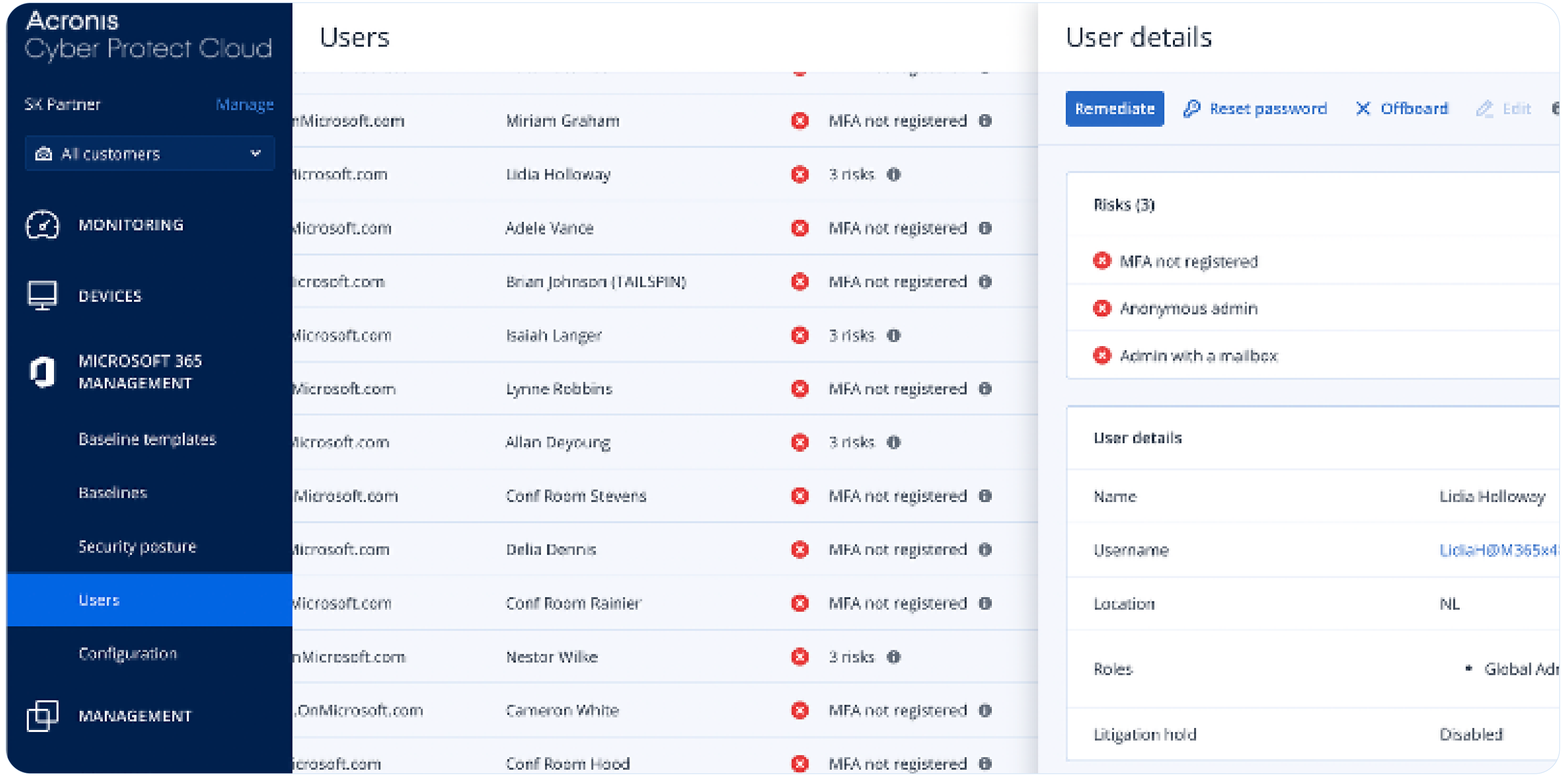
1. **Privilegierte Rollen überprüfen**
   - Identifizierung von übermäßigen Administratorkonten und -rechten
2. **Least-Privilege-Prinzip anwenden**
   - Reduzierung der Anzahl globaler Administratorkonten
   - Standardisierung der Rollenzuweisungen
3. **Mandantenübergreifende Automatisierung**
   - Baseline-Templates zur Durchsetzung rollenbasierter Richtlinien
4. **Lebenszykluskontrolle sichern**
   - Richtige Rollenzuweisung beim Onboarding
   - Aufhebung von Zugriffsrechten, Beenden von Sitzungen und Deaktivieren von Lizenzen beim Offboarding

Was ist passiert?

Was haben Sie gemacht:

- Sie haben eine weitreichende Kompromittierung verhindert.
- Sie haben die Rechte über alle Umgebungen hinweg standardisiert.
- Sie haben dafür gesorgt, dass der Identitäts-Lebenszyklus dauerhaft sicher ist.

Acronis SPM verhindert unkontrollierte Rechteausweitungen durch eine kontrollierte und durchsetzbare Richtlinie.



Im nächsten Schritt können Sie die privilegierten Rollen überprüfen, die Anzahl der globalen Administratorkonten reduzieren und mithilfe von Baseline-Templates Least-Privilege-Richtlinien für alle Mandanten durchsetzen. Das kontinuierliche Lebenszyklusmanagement gewährleistet die Zuweisung der korrekten Zugriffsrechte während des Onboardings und deren vollständigen Entzug beim Offboarding.

Verhindern Sie eskalierende Kontoübernahmen, indem Sie eine Ausbreitung von vornherein unterbinden.

Was haben all diese Angriffe gemeinsam?

In jedem Szenario:

Angriffstyp	Ursache
Password Spraying	Unsichere Identitätskontrollen
OAuth-Missbrauch	Fehlkonfiguration von App-Berechtigungen
Device-Code-Phishing	Sicherheitslücken in Richtlinien
Rechteausweitung	Übermäßige Berechtigungen

Das Muster

Der Zugriff erfolgt über die Identität.

Persistenz wird über die Konfiguration erreicht.

Die Auswirkungen sind mandantenweit.

Vorteile von Acronis SPM

Acronis SPM deckt nicht nur Risiken auf.

Es ermöglicht MSPs, skalierbare Sicherheitspraktiken umzusetzen.

Kontinuierliche Überwachung

- Rund-um-die-Uhr-Überwachung auf Abweichungen von den Sicherheitsstandards
- Identifizierung neuer Risiken in Echtzeit

Baseline-gesteuerte Sicherheit

- Vordefinierte Best Practice-Baselines
- Benutzerdefinierte Baseline-Templates
- Standardisierte Sicherheit für alle Mandanten

Automatische und manuelle Behebung

- Behebung von Problemen direkt in der Konsole
- Automatische Behebung wiederkehrender Risiken
- Verringerung wiederkehrender manueller Arbeiten

Mandantenfähiges Management

- Zentrale Kontrolle aller Kundenumgebungen
- Skalierbare Richtliniendurchsetzung

Vollständige Kontrolle über den Identitäts-Lebenszyklus

- Sicheres Onboarding mit den richtigen Rollen und Richtlinien
- Sicheres Offboarding mit Sitzungswiderruf und Bereinigung

Operative Einbindung

- Integration mit PSA-Tools
- Optimierte Workflows für MSP-Teams

Schlussgedanken

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

- Die Risiken sind unsichtbar.
- Es gibt keine konsistente Behebung.
- Es erfolgt keine kontinuierliche Durchsetzung.

Acronis SPM ändert das.

Acronis SPM bietet MSPs folgende Vorteile:

- Die Risiken werden für jeden Mandanten sichtbar.
- Sie können sofort behoben werden.
- Die Durchsetzung erfolgt automatisch.
- Eine dauerhafte Durchsetzung wird sichergestellt.

Security Posture Management ist ein zentraler Bestandteil von Protected 365

Acronis SPM ist keine optionale Zusatzfunktion, sondern eine grundlegende Komponente von Acronis Protected 365: Nur mit SPM kann die Plattform ihr Versprechen einhalten und Microsoft 365 mit einem umfassenden, KI-gestützten 7-in-1-Schutz sichern. SPM arbeitet dabei eng mit anderen Funktionen – Backup, Email Security, Collaboration Security, XDR, E-Mail-Archivierung und Security Awareness Training – zusammen, um die durch das Modell der geteilten Verantwortung von Microsoft bei Exchange, Teams, SharePoint und OneDrive entstehenden Sicherheitslücken zu schließen.

SPM spielt eine entscheidende Rolle in der Phase „Lücken mit Standard Protection schließen" des Protected 365-Reifegradmodells und unterstützt Unternehmen dabei, sich vom Basis-Schutz hin zu proaktiver Resilienz zu entwickeln. Während Backup und Email Security einen Basis-Schutz bieten, ermöglicht SPM eine kontinuierliche Risikobewertung, die Durchsetzung von Richtlinien und eine automatische Behebung. Somit wird sichergestellt, dass die Umgebungen stets den Best Practices entsprechen und die sich weiterentwickelnden Vorschriften erfüllen.

Durch die kontinuierliche Überwachung von Konfigurationen, die Erkennung von Abweichungen und eine schnelle Behebung geht SPM direkt auf eines der häufigsten und am häufigsten übersehenen Risiken in Microsoft 365 ein: benutzerseitige Fehlkonfigurationen und unbemerkte Abweichungen von den Sicherheitsstandards. Dadurch wird aus einem reaktiven Sicherheitsansatz eine proaktive, richtliniengesteuerte Praxis, die Risiken mindert, die Einhaltung von Vorschriften verbessert und die Cyber-Resilienz insgesamt stärkt.

Von entscheidender Bedeutung ist, dass SPM auf derselben zentralen, mandantenfähigen Acronis Plattform bereitgestellt wird. Dies unterstreicht das zentrale Wertversprechen von Protected 365: ein Anbieter, ein Vertrag, eine integrierte Lösung. Dadurch werden unzählige Einzellösungen überflüssig, der Betriebsaufwand wird reduziert und MSPs sowie IT-Teams können effizient skalieren und gleichzeitig die Servicequalität und Rentabilität verbessern.

Acronis

Weitere Informationen erhalten Sie unter **acronis.com**