axians Microsoft

Modern SecOps
im Microsoft-Ökosystem

Wie Schweizer Unternehmen aus vorhandenen Sicherheits-Funktionen langfristige Cyber Resilience schaffen

2026





01

Von Security-Funktionen zu **operativer Resilienz**

Schweizer Unternehmen, die bereits auf die Security-Lösungen von Microsoft setzen, erleben ein Dilemma: Zwischen der Vielzahl an vorhandenen Funktionen und wirklich wirksamer Cyber Resilience klafft eine Lücke.

Diese Lücke entsteht, da die Security-Funktionen einzeln laufen, Signale nicht zusammenkommen, IT-Teams Alerts manuell bewerten und Daten nicht klar klassifiziert sind. Das erhöht die Komplexität für IT- und Security-Verantwortliche. Gleichzeitig steigen regulatorische Anforderungen, Cyberrisiken und die Erwartungen der Geschäftsleitung, umfassende Sicherheit auf allen Ebenen zu gewährleisten.

Modern SecOps schliesst diese Lücke. Der Ansatz verbindet Schutz, Erkennung, Reaktion, Datenkontrolle und laufende Verbesserung zu einem klaren Betriebsmodell. Microsoft liefert dafür die integrierte Plattform. Axians Somnitec macht sie im Schweizer Unternehmensalltag wirksam: mit Architektur, Governance, Umsetzung, Betrieb und kontinuierlicher Optimierung.

So wird aus den Security-Lösungen von Microsoft mehr als ein Set von Tools. Unternehmen schaffen Transparenz über ihre Risiken, priorisieren Massnahmen nach Wirkung, nutzen vorhandene Lizenzen besser und entlasten ihre internen Teams. Sie reagieren schneller auf Bedrohungen, steuern ihre Security Posture messbar und stärken ihre Resilienz Schritt für Schritt.

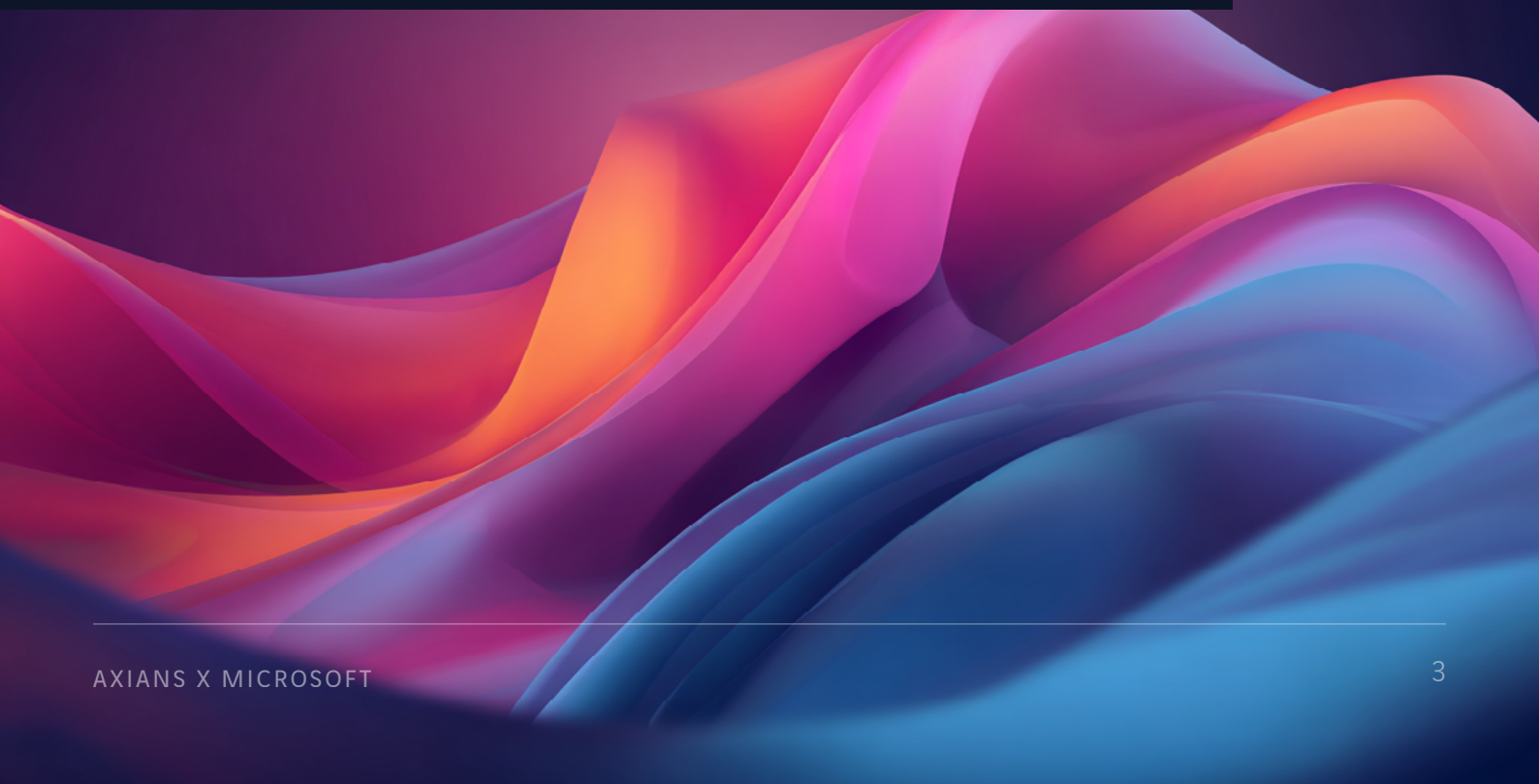
Dieser Guide zeigt, wie Sie als Sicherheitsverantwortlicher Ihres Unternehmens Ihre Microsoft-Security-Umgebung zum operativen Sicherheitsmodell weiterentwickeln. Damit Sie Ihre Systeme nicht nur technisch absichern, sondern Cybersecurity als steuerbaren Beitrag zu Stabilität, Compliance und Vertrauen weiterentwickeln.

02

Security-Komplexität trotz Microsoft-Investment

In der Praxis von Schweizer Unternehmen bleibt das Sicherheitsniveau oft hinter den Möglichkeiten zurück, welche die eingekauften Microsoft-Lösungen auf dem Papier bieten.

Es fehlt das verbindende Betriebsmodell. Security-Funktionen laufen neben-, statt miteinander. Obwohl Unternehmen auf einen bewährten Anbieter mit umfangreichen Funktionalitäten setzen, entsteht Komplexität und am Ende weniger Sicherheit.



Die häufigsten Ursachen

01

Lizenzen sind vorhanden, aber nicht ausgeschöpft.

Oft bezahlen Unternehmen für Funktionen, die sie nur teilweise nutzen. Das betrifft besonders Microsoft 365 E5, Defender, Entra, Purview oder Sentinel. Ohne klare Roadmap bleibt unklar, welche Fähigkeiten bereits verfügbar sind und welche Wirkung sie entfalten könnten.

02

Security-Tools arbeiten nicht als Einheit.

Auch im Microsoft-Ökosystem entsteht kein automatischer Sicherheitsbetrieb. Erst wenn Signale, Richtlinien, Rollen und Prozesse zusammenspielen, entsteht ein klares Lagebild.

03

Alerts erzeugen Aufwand statt Orientierung.

Security-Teams erhalten viele Hinweise, aber nicht immer klare Prioritäten. Ohne Korrelation und definierte Reaktionswege wird jeder Alert zur Einzelfallprüfung.

04

Daten bleiben schwer steuerbar.

Unternehmen wissen nicht genau, wo sensible Informationen liegen, wer Zugriff hat und wie Daten geschützt werden. Mit wachsender Nutzung von KI, Copilot und Cloud-Services wird diese Frage geschäftskritisch.

05

Assessments bleiben punktuell.

Ein Secure Score oder ein Audit zeigt einen Zustand. Doch Cyber Resilience entsteht erst, wenn Unternehmen Risiken laufend messen, priorisieren und reduzieren.

Was das für Schweizer Unternehmen bedeutet

In der Schweiz treffen diese Herausforderungen auf ein besonders anspruchsvolles Umfeld. Unternehmen müssen Verfügbarkeit, Datenschutz, Compliance und Vertrauen sicherstellen, oft über mehrere Standorte, Sprachregionen und regulatorische Kontexte hinweg. Gleichzeitig erwarten Geschäftsleitung, Kunden und Partner belastbare Antworten auf Cyberrisiken.



03

Modern SecOps: Sicherheit als operativer Zustand



Unternehmen reagieren auf diese Entwicklung oft mit zusätzlichen Tools, neuen Richtlinien oder punktuellen Projekten. Doch mehr Technologie allein reduziert die Komplexität nicht. Im Gegenteil: Ohne klare Integration wächst der operative Aufwand weiter.

Modern SecOps verfolgt deshalb einen anderen Ansatz.

Der Fokus liegt nicht auf einzelnen Security-Produkten, sondern auf einem durchgängigen Sicherheitsbetrieb. Ziel ist es, Risiken früh sichtbar zu machen, Bedrohungen schneller einzuordnen und Sicherheitsmassnahmen kontinuierlich weiterzuentwickeln – über Identitäten, Endpunkte, Cloud-Umgebungen, Anwendungen und Daten hinweg. Security wird damit nicht mehr als Sammlung einzelner Massnahmen verstanden, sondern als laufender, zentral orchestrierter Prozess.

Was Modern SecOps verändert

Modern SecOps verbindet dafür Prävention, Erkennung, Reaktion und Governance in einem integrierten Modell. Sicherheitsrelevante Signale laufen zentral zusammen. Risiken lassen sich priorisieren. Teams erhalten mehr Kontext und weniger operative Reibung.

Dadurch verschiebt sich der Fokus:

» weg von isolierten Tools

» weg von manueller Korrelation

» weg von reaktiver Incident-Bearbeitung

Hin zu:

» kontinuierlicher Transparenz

» automatisierter Priorisierung

» schnellerer Reaktion

» messbarer Verbesserung der Security Posture

Für Unternehmen bedeutet das vor allem eines: **mehr Steuerbarkeit.**

Security-Verantwortliche erhalten ein klareres Bild über Risiken, Angriffspfade und Schwachstellen. Gleichzeitig sinkt der operative Druck auf interne Teams, weil sich Prozesse standardisieren, Signale zusammenführen und wiederkehrende Aufgaben automatisieren lassen.

Die **vier Kernbereiche** von Modern SecOps

Ein modernes Sicherheitsmodell verbindet dafür vier zentrale Fähigkeiten:

SOC kontinuierlich optimieren

Security Operations entwickeln sich laufend weiter. Unternehmen verbessern ihre Detection-Regeln, Reaktionsprozesse und Sicherheitsrichtlinien kontinuierlich statt nur punktuell nach Audits oder Incidents.

Angriffspfade sichtbar machen

Moderne Sicherheitsplattformen analysieren Zusammenhänge zwischen Identitäten, Geräten, Cloud-Ressourcen und Berechtigungen. Risiken lassen sich dadurch früher erkennen und gezielter priorisieren.

Bedrohungen ganzheitlich erkennen

Angriffe entstehen selten nur an einem Punkt. Modern SecOps führt Signale aus verschiedenen Bereichen zusammen und schafft ein gemeinsames Lagebild über die gesamte Umgebung hinweg.

Schneller und intelligenter reagieren

Automatisierung und KI unterstützen Security-Teams bei der Einordnung von Vorfällen, der Priorisierung von Massnahmen und der Beschleunigung von Reaktionsprozessen.

Der entscheidende Unterschied

Modern SecOps ersetzt dabei keine bestehende Sicherheitsstrategie. Der Ansatz verbindet vorhandene Fähigkeiten zu einem operativen Gesamtmodell. Genau darin liegt für viele Schweizer Unternehmen der nächste Entwicklungsschritt: vorhandene Microsoft-Security-Funktionen nicht nur technisch zu nutzen, sondern daraus einen belastbaren, kontinuierlich gesteuerten Sicherheitsbetrieb zu machen.



Die **Microsoft Unified Security** Plattform

04

Dafür braucht es eine Sicherheitsarchitektur, die Informationen zusammenführt statt voneinander trennt. Genau dafür hat Microsoft seine Security-Lösungen als integrierte Plattform aufgebaut.

Identitäten, Endpunkte, E-Mails, Cloud-Services, Anwendungen und Daten erzeugen laufend sicherheitsrelevante Signale. Die Microsoft Unified Security Plattform verbindet genau diese Ebenen zu einem gemeinsamen Sicherheitsmodell.

Sicherheit über alle Ebenen hinweg verbinden

Microsoft Defender XDR bildet dabei die operative Grundlage für Erkennung und Reaktion. Die Plattform führt Signale aus unterschiedlichen Bereichen zusammen und schafft daraus einen gemeinsamen Sicherheitskontext.

Microsoft Sentinel erweitert dieses Modell um zentrale Analyse- und Automatisierungsfunktionen.

Mit **Microsoft Entra** rückt die Identität in den Mittelpunkt der Sicherheitsstrategie. Zugriffe, Berechtigungen und Benutzerkontexte werden kontinuierlich bewertet, um Risiken frühzeitig zu erkennen und Zero-Trust-Prinzipien umzusetzen.

Microsoft Purview ergänzt die Plattform um die Datenperspektive. Unternehmen erhalten mehr Transparenz darüber, wo sensible Informationen liegen, wie sie genutzt werden und wie sich Daten besser schützen lassen.

Security Copilot schliesslich unterstützt Security-Teams KI-basiert dabei, Informationen schneller einzuordnen, Zusammenhänge besser zu verstehen und Reaktionsprozesse effizienter zu gestalten.

Von einzelnen Signalen zu operativer Steuerbarkeit

Die Stärke dieser Plattform liegt in der Orchestrierung. Ein verdächtiger Login etwa bleibt nicht isoliert sichtbar. Er lässt sich mit Geräteinformationen, Datenzugriffen, Benutzerverhalten oder Cloud-Aktivitäten verbinden. Genau dieser Kontext entscheidet heute über die Wirksamkeit von Security Operations.

Unternehmen gewinnen damit:

- mehr Transparenz über Risiken
- weniger operative Reibung
- schnellere Priorisierung
- konsistentere Sicherheitsprozesse
- eine bessere Grundlage für Governance und Compliance

05

Data Security als Grundlage für den sicheren Einsatz von KI

Mit der zunehmenden Nutzung von KI verändert sich auch die Rolle von Cybersecurity. Unternehmen schützen heute nicht mehr nur Geräte, Benutzerkonten oder Anwendungen. Im Mittelpunkt stehen zunehmend die Daten selbst. Denn KI-Systeme arbeiten genau mit den Informationen, die Unternehmen täglich erzeugen, speichern und teilen. Je stärker KI in Arbeitsprozesse integriert wird, desto wichtiger wird die Frage:

Welche Daten darf ein System überhaupt sehen, verarbeiten oder weitergeben?

Damit rückt Data Security ins Zentrum moderner Security-Strategien.



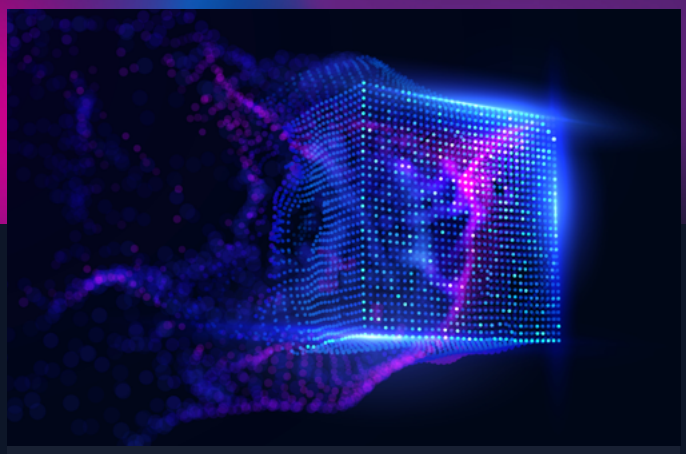


KI erhöht den Druck auf Governance und Transparenz

Das schafft neue Herausforderungen:

- sensible Daten werden zu breit zugänglich
- Berechtigungen wachsen historisch und unkontrolliert
- Informationen werden falsch klassifiziert oder gar nicht geschützt
- Daten verlassen definierte Sicherheitskontexte
- Compliance- und Datenschutzanforderungen werden schwerer steuerbar

Die Einführung von KI macht bestehende Schwachstellen damit sichtbarer – und in vielen Fällen auch kritischer.



Data Security braucht Kontext

Genau deshalb reicht klassische Perimeter-Security heute nicht mehr aus. Unternehmen müssen verstehen:

- wo sensible Daten liegen
- wer darauf zugreifen kann
- wie Informationen genutzt werden
- welche Risiken durch Freigaben, Cloud-Dienste oder KI-Nutzung entstehen

Microsoft Purview erweitert die Sicherheitsarchitektur genau um diese Perspektive. Daten lassen sich klassifizieren, Schutzrichtlinien definieren und Zugriffe besser kontrollieren.

Microsoft Purview erweitert die Sicherheitsarchitektur genau um diese Perspektive. Daten lassen sich klassifizieren, Schutzrichtlinien definieren und Zugriffe besser kontrollieren.

Besonders im Schweizer Umfeld gewinnt dieser Ansatz an Bedeutung. Datenschutz, regulatorische Anforderungen und der vertrauensvolle Umgang mit Informationen spielen für Unternehmen, Kunden und Partner hier eine zentrale Rolle.

06

Von punktueller Security zu kontinuierlicher Resilienz

Datenschutz, Governance und Data Security lassen sich damit nicht mehr isoliert betrachten. Sie stehen in direktem Zusammenhang mit der Frage, wie widerstandsfähig ein Unternehmen gegenüber Cyberrisiken tatsächlich ist.

Genau deshalb reicht es nicht aus, Security nur punktuell zu bewerten. Sie entsteht im laufenden Betrieb. Ein modernes Sicherheitsmodell entwickelt sich ständig weiter. Risiken verändern sich, Angriffsmuster passen sich an und digitale Umgebungen wachsen kontinuierlich. Unternehmen benötigen deshalb einen Ansatz, der Security laufend verbessert.

Genau hier setzen moderne Plattformfunktionen wie Secure Score, Exposure Management oder Attack Path Analysis an. Sie helfen dabei:

01 Sicherheitslücken frühzeitig sichtbar zu machen

02 Risiken nach tatsächlicher Relevanz zu priorisieren

03 kritische Angriffspfade zu erkennen

04 Fortschritte messbar nachzuverfolgen

05 Sicherheitsmassnahmen gezielt weiterzuentwickeln

Statt isolierter Einzelmassnahmen entsteht ein kontinuierlicher Zyklus aus Bewertung, Priorisierung, Umsetzung und Optimierung.

Von punktueller Security zu kontinuierlicher Resilienz

Besonders wichtig ist dabei der Blick auf Zusammenhänge. Ein einzelnes Risiko wirkt oft harmlos, bis es mit anderen Schwachstellen kombiniert wird.

Ein übersehener Gerätezugang, zu weit gefasste Berechtigungen oder ungeschützte sensible Daten können gemeinsam kritische Angriffspfade erzeugen. Moderne Security-Plattformen helfen dabei, genau diese Verbindungen sichtbar zu machen.

Das verändert auch die Priorisierung im Security-Alltag. Teams konzentrieren sich nicht mehr nur auf die Anzahl von Alerts oder Schwachstellen, sondern auf deren tatsächlichen Einfluss auf das Risiko des Unternehmens.



07

Von der Plattform zum sicheren Betrieb mit Axians Somnitec

Doch selbst leistungsfähige Plattformen entfalten ihren Wert erst dann vollständig, wenn Unternehmen Risiken in ihren Kontexte nicht nur erkennen, sondern daraus klare Prozesse, Verantwortlichkeiten und Massnahmen ableiten.

Entscheidend ist daher, wie konsequent Security in den laufenden Betrieb integriert wird. Erst durch die operative Einbindung in Prozesse, Rollen und Sicherheitsabläufe entsteht echte Cyber Resilience. Genau hier setzt Axians Somnitec an. Axians Somnitec unterstützt Unternehmen dabei, aus vorhandenen Microsoft-Sicherheitsfunktionen ein integriertes Sicherheitsmodell zu entwickeln, abgestimmt auf Organisation, Risikolage und bestehende IT-Strukturen.

Der Fokus liegt dabei auf einem kontinuierlich steuerbaren Sicherheitsbetrieb. Dazu gehören:

01 die Definition einer belastbaren Security Baseline

02 die Integration zentraler Microsoft-Security-Komponenten

03 die Entwicklung klarer Betriebs- und Reaktionsprozesse

04 die laufende Optimierung der Security Posture

05 die Entlastung interner Teams durch standardisierte Security Operations

Axians verbindet damit technologische Umsetzung mit Governance, Betrieb und kontinuierlicher strategischer Weiterentwicklung.

Ein Modell, das zur Schweizer Realität passt

Für Schweizer Unternehmen spielen neben Technologie vor allem Verlässlichkeit, Transparenz und Governance eine zentrale Rolle. Security muss nicht nur wirksam sein, sondern auch nachvollziehbar steuerbar bleiben – gegenüber Geschäftsleitung, Kunden, Partnern und regulatorischen Anforderungen.

Axians Somnitec verbindet dafür Microsoft Security mit lokalem Betriebsverständnis, klaren Verantwortlichkeiten und einem strukturierten Modern-SecOps-Ansatz.

So entsteht aus einzelnen Security-Funktionen ein Sicherheitsbetrieb, der Risiken reduziert, interne Teams entlastet und Cyber Resilience langfristig stärkt.



08

Wo stehen Sie? Der Weg zu **Modern SecOps**

Dabei geht es nicht darum, das eigene Sicherheitssystem auf einen Schlag umzugestalten. Unternehmen entwickeln ihre Sicherheitsorganisation schrittweise weiter, abhängig von Risikolage, Ressourcen, regulatorischen Anforderungen und bestehender IT-Landschaft. Das folgende Reifegrad-modell zeigt, wie sich Unternehmen typischerweise in Richtung Modern SecOps entwickeln.

01

REIFEGRAD 1

Tool-basierte Security

Microsoft-Sicherheitsfunktionen sind vorhanden, arbeiten jedoch weitgehend isoliert.

Typische Merkmale:
- viele manuelle Prozesse
- hohe Alert-Belastung
- begrenzte Transparenz
- Security wird vor allem technisch betrieben

02

REIFEGRAD 2

Integrierte Sicherheitsplattform

Security-Signale aus Identitäten, Geräten, Cloud und Daten werden stärker zusammengeführt.

Typische Merkmale:
- bessere Transparenz über Risiken
- erste Automatisierungen
- Security Baselines und Richtlinien
- messbarere Security Posture

03

REIFEGRAD 3

Operativer Modern-SecOps-Betrieb

Security wird organisatorisch verankert und kontinuierlich gesteuert.

Typische Merkmale:
- definierte Betriebs- und Reaktionsprozesse
- laufendes Monitoring und Reporting
- klarere Priorisierung
- Entlastung interner Teams

04

REIFEGRAD 4

Resiliente Security Organisation

Security entwickelt sich zu einem kontinuierlich optimierten Betriebsmodell.

Typische Merkmale:
- proaktive Risikoanalyse
- integrierte Data Security und Governance
- KI-unterstützte Abläufe
- hohe Transparenz und Steuerbarkeit



Jetzt Kontakt **aufnehmen**

Wollen auch Sie wissen, wo Sie heute stehen? Ein Modern SecOps Readiness Assessment mit Axians Somnitec zeigt Ihnen, welche Potenziale in Ihren Microsoft-Security-Lösungen bereits vorhanden sind.

Gemeinsam identifizieren wir dann die Massnahmen, welche den grössten Sicherheits- und Business Impact schaffen, abgestimmt auf Ihre Anforderungen und Ressourcen. Kontaktieren Sie uns!