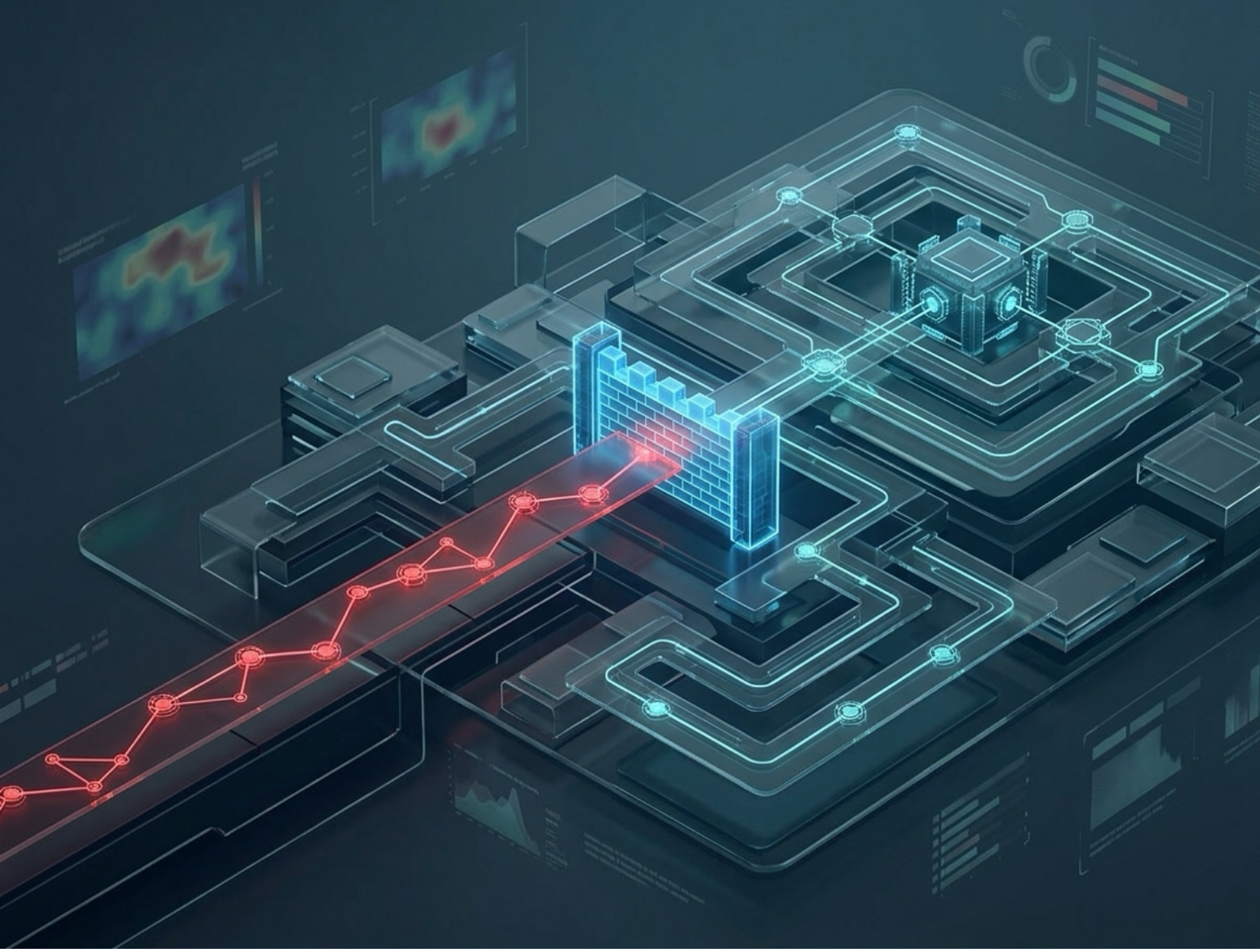


WHITE PAPER

Proaktive Verteidigung
Angriffspfade erkennen. Choke Points schliessen. Cyberrisiko senken.

Mit Continuous Threat Exposure Management (CTEM) und kontinuierlicher Angriffssimulation zu messbarer Sicherheit – für Verwaltungsräte, Geschäftsleitungen und IT-Entscheider.

SecureComply
Secure by Design. Compliant by Default.

SecureComply GmbH | April 2026

SecureComply

Secure by Design. Compliant by Default.

Attack Path Management

Angriffspfade verstehen, priorisieren und unterbrechen

Für Verwaltungsräte, Geschäftsleitungen und IT-Entscheider

94 % aller kritischen Unternehmens-Assets lassen sich in weniger als vier Schritten kompromittieren. Wissen Sie, welche Angriffspfade in Ihrer IT-Umgebung direkt zu Ihren sensibelsten Daten führen? Dieses White Paper zeigt, wie Attack Path Management und Continuous Threat Exposure Management (CTEM) die Cybersicherheit Ihres Unternehmens grundlegend verändern: weg von der reaktiven Behebung tausender Einzelschwachstellen, hin zur gezielten Unterbrechung der wenigen Angriffspfade, die wirklich zählen. Erfahren Sie, warum klassisches Schwachstellenmanagement und punktuelle Penetrationstests nicht mehr ausreichen – und wie Sie mit der Identifikation von Choke Points bis zu 80 % Aufwand einsparen, während Sie Ihr Cyberrisiko messbar senken.

Für Verwaltungsräte, Geschäftsleitungen und IT-Entscheider, die Transparenz über ihre tatsächliche Risikolage benötigen und ihre Sorgfaltspflicht gegenüber Regulatoren nachweisbar erfüllen wollen. Auf Basis des XM Cyber Impact Reports, mit Fokus auf Continuous Exposure Management, kontinuierliche Angriffssimulation und die Integration in bestehende Security-Tools.

Inhaltsverzeichnis

01 Executive Summary

Die Mehrheit der geschäftskritischen Assets in Unternehmen kann mit erschreckend wenig Aufwand kompromittiert werden. Ein Risiko, das weit über die IT-Abteilung hinausreicht und direkt die Verantwortung der Unternehmensführung betrifft. Gleichzeitig stehen Organisationen vor Tausenden von Schwachstellen, ohne zu wissen, welche davon tatsächlich einen Pfad zu kritischen Systemen eröffnen. Die finanziellen, regulatorischen und reputativen Folgen eines erfolgreichen Angriffs treffen letztlich die Organe, die für das Risikomanagement und die Sorgfaltspflicht verantwortlich sind.

Die Lösung von XM Cyber bietet messbare geschäftskritische Vorteile.

Risikotransparenz und Compliance:

- Vollständige Sichtbarkeit aller Angriffspfade zu geschäftskritischen Assets – on-premises, in der Cloud und hybrid
- Erfüllung regulatorischer Anforderungen (DSGVO, NIS2, ISO 27001) durch nachweisbare, kontinuierliche Risikoanalyse
- Dokumentierte Sorgfaltspflicht gemäss Art. 716a OR für Verwaltungsräte und Geschäftsleitungen

Operative Effizienz:

- 80 % weniger zu behebende Probleme durch gezielte Fokussierung auf Choke Points
- Priorisierung nach tatsächlichem Geschäftsrisiko statt nach CVSS-Score
- Kontinuierliche, automatisierte Analyse statt punktueller Penetrationstests

Strategischer Vorteil:

- Datenbasierte Entscheidungsgrundlage für die Priorisierung von Sicherheitsinvestitionen
- Messbare Risikoreduktion als Nachweis gegenüber Regulatoren und Stakeholdern
- Zukunftssichere Plattform für Continuous Threat Exposure Management (CTEM)

Dieses White Paper zeigt auf Basis des XM Cyber Impact Reports, wie Attack Path Management Angriffspfade sichtbar macht. Die Lösung identifiziert gezielt Choke Points und beseitigt das Unternehmensrisiko mit einem Bruchteil des Aufwands. Der Fokus liegt dabei nicht auf technischen Details, sondern auf der strategischen Frage:

Wie erhalten wir als Führungsgremium Transparenz über unsere tatsächliche Risikolage und wie weisen wir diese Sorgfalt gegenüber Regulatoren und Stakeholdern nach?

94 %	**73 %**	**80 %**	**2 Mio.**
der kritischen Assets in vier Schritten kompromittierbar	der Top-Angriffs-Techniken basieren auf Zugangsdaten-Problemen	weniger Aufwand durch gezielte Choke-Point-Behebung	Entitäten analysiert im XM Cyber Impact Report

02 Einleitung

Cyberangriffe werden immer raffinierter und betreffen Unternehmen jeder Grösse. Im Jahr 2024 verzeichnete das Bundesamt für Cybersicherheit (BACS) rund 63'000 Cybervorfälle (Quelle: BACS Halbjahresbericht 2024/II). Dies sind fast doppelt so viele wie im Vorjahr. Die Dunkelziffer liegt um ein Vielfaches höher. Gleichzeitig zeigt der XM Cyber „State of Exposure Management" Impact Report 2024, dass die Mehrheit der kritischen Unternehmens-Assets mit erschreckend wenig Aufwand kompromittiert werden kann.

Traditionelle Sicherheitsansätze konzentrieren sich auf die Erkennung und Behebung einzelner Schwachstellen. Doch isoliert betrachtet sagen Schwachstellen wenig über das tatsächliche Risiko für ein Unternehmen aus. Entscheidend ist nicht, ob eine Schwachstelle existiert, sondern ob sie Teil eines Angriffspfads ist, der zu geschäftskritischen Assets führt. Genau hier setzt Attack Path Management an.

XM Cyber analysiert kontinuierlich sämtliche Angriffspfade innerhalb der gesamten IT-Umgebung. Anstatt Sicherheitsteams mit Tausenden isolierter Schwachstellen zu konfrontieren, identifiziert die Plattform die wenigen entscheidenden Engstellen, sogenannte Choke Points, an denen sich mit minimalem Aufwand der maximale Schutz erzielen lässt.

Das Wichtigste in Kürze:
Die überwiegende Mehrheit der kritischen Assets ist über kurze Angriffspfade erreichbar. Der grösste Angriffsvektor: mangelhaft verwaltete Zugangsdaten. Die wirksamste Gegenmassnahme: gezielte Behebung weniger Choke Points, die den Remediations-Aufwand um bis zu 80 % reduziert und die Sicherheit gegen Angriffe massiv erhöht.

03 Warum klassische Sicherheitsansätze versagen

Die Angriffsfläche moderner Unternehmen hat sich grundlegend verändert. Hybride Cloud-Architekturen, Remote-Arbeit und eine wachsende Anzahl vernetzter Systeme schaffen eine Komplexität, die mit herkömmlichen Sicherheitstools kaum noch beherrschbar ist.

Die Grenzen traditioneller Ansätze

Vulnerability Management: Klassisches Schwachstellenmanagement bewertet Risiken anhand von CVSS-Scores. Doch ein hoher Score bedeutet nicht automatisch ein hohes Geschäftsrisiko. Eine kritische Schwachstelle auf einem isolierten System ohne Zugang zu sensiblen Daten ist weniger gefährlich als eine mittlere Schwachstelle, die direkt zu einem Domänencontroller führt.

Penetrationstests: Pentests liefern wertvolle Momentaufnahmen, bilden aber nur einen Bruchteil der möglichen Angriffspfade ab. Sie sind punktuell, teuer und veralten schnell, da sich die Umgebung kontinuierlich verändert.

Isolierte Sicherheitstools: SIEM, EDR, Firewalls und weitere Tools adressieren jeweils spezifische Aspekte der Sicherheit. Doch keines dieser Tools zeigt, wie ein Angreifer verschiedene Schwachstellen, Fehlkonfigurationen und Zugangsdaten-Probleme zu einem zusammenhängenden Angriffspfad kombinieren kann.

Die häufigsten Angriffsvektoren

73 %	der wichtigsten Angriffstechniken basieren auf mangelhaft verwalteten oder gestohlenen Zugangsdaten
27 %	der wichtigsten Techniken basieren auf Sicherheitslücken oder Fehlkonfigurationen

Was Unternehmen wirklich brauchen, ist ein Ansatz, der alle möglichen Angriffspfade kontinuierlich analysiert und die Frage beantwortet: Welche unserer Schwachstellen führen tatsächlich zu unseren geschäftskritischen Assets und wo können wir diese Pfade am effizientesten unterbrechen?

04 Methodik der Angriffspfade

Die graphenbasierte Simulationstechnologie von XM Cyber entdeckt kontinuierlich Angriffspfade, die zu kritischen Assets führen und ermöglicht so einen vollständigen Einblick in die Sicherheitslage des Unternehmens. Auf diese Weise können Nutzer nachvollziehen, wie Schwachstellen, Fehlkonfigurationen, Benutzerrechte und weitere Faktoren zu einem Cyberangriffspfad führen, der kritische Assets gefährdet.

Die Wahrscheinlichkeit der Gefährdung eines kritischen Assets wird anhand von zwei Hauptfaktoren bestimmt: der Komplexität des Angriffs und der Anzahl der Sprünge (Hops), die ein Angreifer benötigt, um zu den kritischen Assets zu gelangen.

Angriffspfad-Visualisierung – Vom Breach Point zum kritischen System (Quelle: XM Cyber)

Komplexität eines Angriffs

Die Komplexität eines Angriffspfads wird von vielen Faktoren bestimmt: Welche Voraussetzungen müssen erfüllt sein, wie lange dauert der Angriff, welcher Zugang ist erforderlich und wie viele Schritte legt der Angreifer vom Einbruchspunkt bis zu Ihren kritischen Assets zurück?

Anhand der Komplexität des Angriffspfads lässt sich bestimmen, wie viel Prozent der kritischen Assets in Unternehmen kompromittiert werden können:

55 % bei geringer Komplexität (Stufe 2) **75 %** bei beliebiger Komplexität

Das bedeutet:

Die Mehrheit der Assets kann kompromittiert werden. Ohne die Kenntnis, wo man suchen muss, ist man faktisch blind.

Wie viele Hops bis zur Kompromittierung?

Als Hops bezeichnet man die Anzahl der Schritte, die ein Angreifer vom Einbruchspunkt bis zur Kompromittierung kritischer Assets benötigt. Für jeden Schritt wird eine einzelne Angriffstechnik verwendet.

Die Daten im Detail: Nach einem Hop sind bereits 63 % erreichbar, nach zwei Hops 81 %, nach drei Hops 88 % und nach vier Hops 94 %. In vier Schritten oder weniger vom Einbruchspunkt aus können 94 % der kritischen Assets kompromittiert werden.

94 % der kritischen Assets können in vier Schritten oder weniger kompromittiert werden

05 Top-Angriffstechniken

Die analysierten zwölf Top-Angriffstechniken nutzten eine Kombination aus Schwachstellen, Fehlkonfigurationen und mangelhaft verwalteten oder gestohlenen Zugangsdaten, um kritische Assets zu kompromittieren.

Die zwölf häufigsten Techniken

1	**23,7 %**	Domain-Zugangsdaten (kompromittierte Zugangsdaten, Pass the Hash)
2	**14,2 %**	Manipulation gemeinsam genutzter Inhalte (Dateifreigabe, Berechtigungen)
3	**10,1 %**	Änderung von Gruppenrichtlinien (Domain Controller, Missbrauch von GPOs)
4	**9,5 %**	Lokale Zugangsdaten
5	**8,1 %**	PrintNightmare
6	**7,2 %**	Weitergabe von Zugangsdaten
7	**6,0 %**	Exe Share Hooking (Zugriffsrechte mit ausführbaren Dateien)
8	**5,6 %**	Microsoft-SQL-Zugangsdaten
9	**4,7 %**	WPAD Spoofing (Man-in-the-Middle-Technik)
10	**4,2 %**	Erreichbarkeit (Netzwerksegmentierungsprobleme)
11	**3,9 %**	Credential Dumping
12	**2,8 %**	Azure-Run-Befehl auf VM missbrauchen

Erkenntnis:
Solides Patch-Management reduziert die Angriffsvektoren. Doch wir sollten uns nicht nur auf Schwachstellen konzentrieren. Rund 27 % der Angriffstechniken nutzen Fehlkonfigurationen und Sicherheitslücken aus – zusätzlich zu den 73 %, die auf mangelhaft verwalteten Zugangsdaten basieren.

AWS-Angriffstechniken

Die sechs meistgenutzten AWS-Angriffstechniken zeigen ein klares Bild: 64 % basieren auf mangelhaft verwalteten oder gestohlenen Zugangsdaten (User Exploit, Update der Rollen-Zugriffsberechtigungen, Missbrauch aufgabenbezogener Zugangsberechtigungen und Credentials Stealer).

1	**24,5 %**	User Exploit
2	**19,5 %**	EC2 Exploit
3	**16 %**	Update der Rollen-Zugriffsberechtigungen
4	**16 %**	EC2-Modifizieren von Instance-Benutzerdaten
5	**12 %**	Missbrauch aufgabenbezogener Zugangsberechtigungen
6	**12 %**	Credentials Stealer

75 %	der Unternehmen haben einen nach aussen gerichteten EC2-Rechner, der ein Risiko für kritische Assets darstellt

Azure-Angriffstechniken

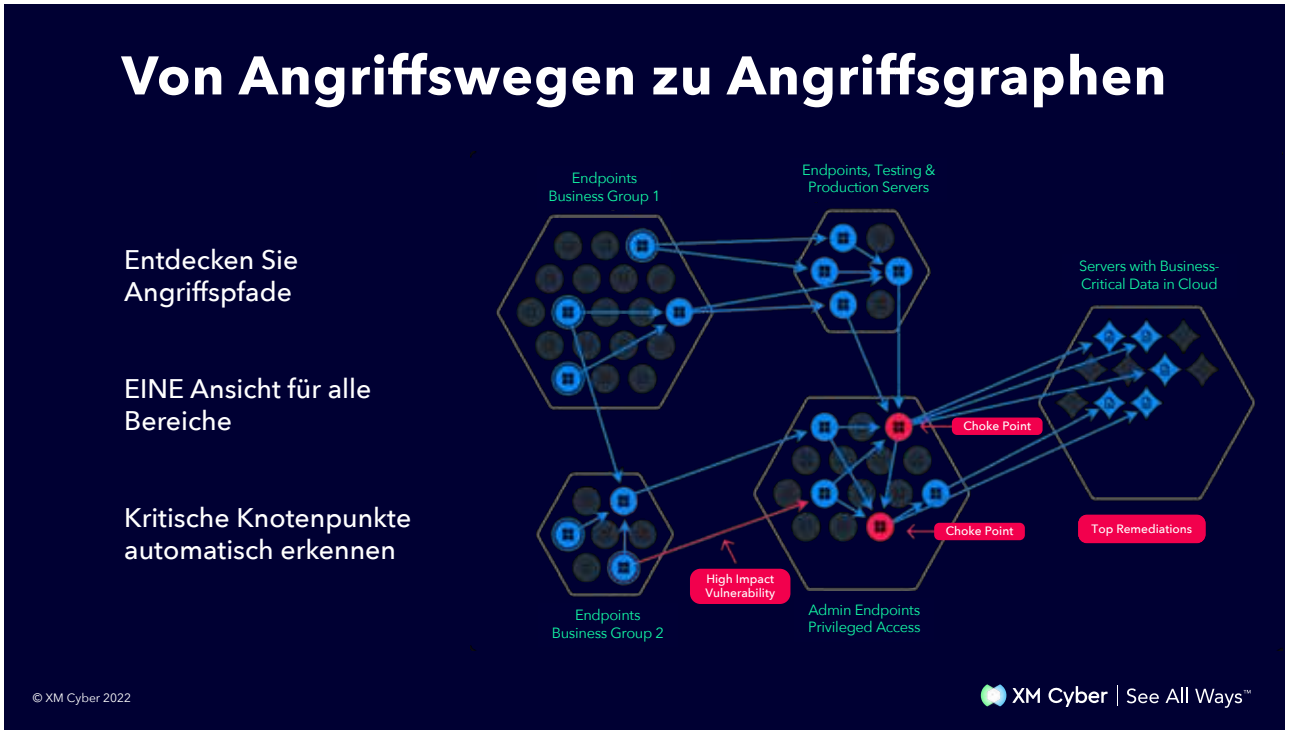
Bei Azure basieren 100 % der wichtigsten Techniken auf mangelhaft verwalteten oder gestohlenen Zugangsdaten:

1	**35 %**	Missbrauch Run-Befehl auf VM
2	**21 %**	Missbrauch Microsoft Intune Execute
3	**15,5 %**	Missbrauch Run-Befehl via VM Extensions
4	**12,5 %**	Application Owner kompromittiert Serviceprinzip
5	**8,5 %**	Blobs lesen
6	**7,5 %**	Blobs hochladen

Erkenntnis:
Die Hauptangriffsvektoren in der Cloud sind Fehlkonfigurationen und ein zu sorgloses Zugangsmanagement. Attack Path Management hilft, Schwachstellen zu identifizieren, die Angreifern in Kombination Zugang zur Cloud gewähren.

06 Choke Points: Risiken gezielt beseitigen

Eine Möglichkeit, die Aktivitäten des Sicherheitsteams zu priorisieren, besteht darin herauszufinden, wo die Angriffspfade zu kritischen Assets zusammenlaufen und dort gezielt zu korrigieren. Die XM-Cyber-Plattform identifiziert kontinuierlich verborgene Angriffspfade zu kritischen Assets in Cloud- und On-Premise-Umgebungen, sodass diese an wichtigen Knotenpunkten blockiert werden können.



Von Angriffswegen zu Angriffsgraphen – Choke Points automatisch erkennen (Quelle: XM Cyber)

Choke Points im Detail:
Von den fast zwei Millionen Entitäten in Unternehmen sind im Durchschnitt nur fünf für die Gefährdung von fast 58 % der kritischen Assets verantwortlich. Das heisst: Mehr als die Hälfte der Organisation könnte kompromittiert werden – und die Lösung liegt in der Behebung weniger, genau identifizierter Engstellen.

Bei 80 % der Unternehmen wurden zwar Sicherheitsprobleme entdeckt, aber kritische Assets wurden durch diese nicht gefährdet. Es handelte sich um Sackgassen im Angriffsgraphen. Diese Erkenntnis ist entscheidend. Nicht jede Schwachstelle erfordert sofortiges Handeln. Entscheidend ist der Kontext.

Wenn Unternehmen ihre Ressourcen darauf ausrichten, Probleme an einzelnen Schlüsselstellen zu beheben, lässt sich das Gesamtrisiko und die Anzahl der potenziellen Angriffspfade schnell reduzieren.

80 % weniger zu behebende Probleme, wenn man weiss, wo die Angriffspfade unterbrochen werden können

07 Cloud- und Hybrid-Erkenntnisse

Angriffspfade können in hybriden Netzwerkarchitekturen sehr komplex ausfallen. Die Untersuchung zeigt die Sicherheitslücken und Angriffstechniken, die typischerweise ausgenutzt werden und liefert damit die Grundlage für gezielte Gegenmassnahmen.

Plattformübergreifende Angriffe

Unternehmen folgen bei ihrer Migration in die hybride Cloud-Welt nicht immer einer klaren Strategie. Teams beschaffen Cloud-Dienste eigenständig, was zu einer fragmentierten Sicherheitslandschaft führt. Angreifer nutzen genau diese Brüche zwischen On-Premise und Cloud.

28 %	**23 %**
aller Unternehmen von plattformübergreifendem Angriff betroffen	kritischer Assets durch plattformübergreifende Technik gefährdet

Hybrid-Cloud

- 41 % der Hybrid-Cloud-Organisationen nutzten On-Prem-to-Cloud-Techniken
- 38 % der Azure-Organisationen nutzten Cloud-zu-On-Prem-Techniken
- 95 % der Benutzer besitzen langfristige Zugangsschlüssel, die offengelegt werden können

Obwohl Identitäten so konzipiert sein sollten, dass sie lateralen Traffic nicht zulassen, besteht eine hohe Wahrscheinlichkeit, dass sie kompromittiert werden können. Die Cloud ist keine isolierte Insel, sie ist direkt mit der On-Premise-Umgebung verbunden und muss als Teil der gesamten Angriffsfläche betrachtet werden.

08 Continuous Threat Exposure Management

Gartner hat 2022 mit Continuous Threat Exposure Management (CTEM) ein fünfstufiges Rahmenwerk definiert (Gartner, „Implement a Continuous Threat Exposure Management Program“, 2022), das Unternehmen hilft, ihre Sicherheitslage kontinuierlich zu verbessern. XM Cyber ist ein zentraler Baustein für die Umsetzung eines CTEM-Programms.

Continuous Security Posture Management – APM und CCM im Zusammenspiel (Quelle: XM Cyber)

Die fünf Phasen des CTEM

1. Scoping

Definition der geschäftskritischen Angriffsfläche:

Welche Assets sind für das Unternehmen essenziell? Dabei werden nicht nur technische, sondern auch geschäftliche Kriterien berücksichtigt.

2. Discovery

Identifikation aller Schwachstellen, Fehlkonfigurationen und Angriffspfade in der gesamten Umgebung – On-Premise, Cloud und hybrid.

3. Prioritization

Bewertung der Schwachstellen nach tatsächlichem Risiko:

Nicht der CVSS-Score allein zählt, sondern die Frage, ob ein Angriffspfad zu einem kritischen Asset führt.

4. Validation

Überprüfung durch kontinuierliche Angriffssimulation:

Ist der theoretische Angriffspfad auch praktisch ausnutzbar? XM Cyber simuliert dies rund um die Uhr, ohne den Betrieb zu beeinträchtigen.

5. Mobilization

Operationalisierung der Erkenntnisse:

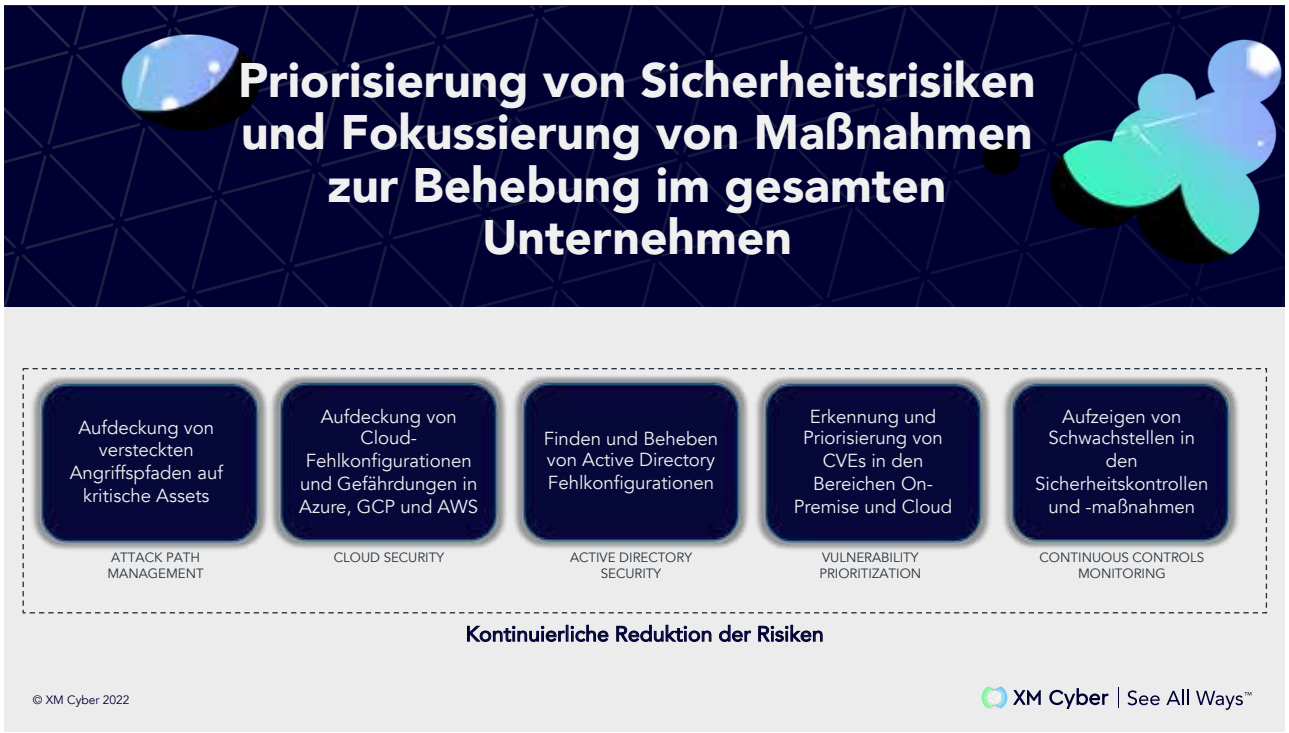
Klare, priorisierte Handlungsempfehlungen für Sicherheits- und IT-Teams, die sich auf die wirkungsvollsten Massnahmen konzentrieren.

Erkenntnis:
Durch die Kombination von CTEM mit Attack Path Management erreichen Unternehmen ein konsistentes Prognosemodell, das aufzeigt, was umgangen werden kann, wo die grössten Risiken liegen und welche Massnahmen die höchste Wirkung entfalten.

09 SecureComply GmbH als Partner

Unabhängig. Swiss-made. In Ihrer Sprache.

SecureComply GmbH ist ein Schweizer Cybersicherheitsunternehmen mit Fokus auf die Implementierung moderner Sicherheitsarchitekturen. Als Partner von XM Cyber unterstützt SecureComply Unternehmen bei der Einführung und dem Betrieb von Attack-Path-Management-Lösungen – von der initialen Risikoanalyse über das laufende Monitoring bis hin zu Board-Reporting und regulatorischer Compliance.



Priorisierung und Fokussierung von Sicherheitsmassnahmen im gesamten Unternehmen (Quelle: XM Cyber)

Unser Leistungsangebot

- **CTEM Assessment:** Initiale Analyse Ihrer Angriffsfläche mit XM Cyber, inklusive Priorisierung der kritischen Choke Points.
- **Managed Attack Path Management:** Kontinuierliche Überwachung, Analyse und Berichterstattung Ihrer Angriffspfade.
- **Board-Reporting:** Regelmässige, verständliche Berichte für Verwaltungsrat und Geschäftsleitung gemäss Art. 716a OR.
- **Integration:** Anbindung an bestehende SIEM- (z. B. Splunk, Microsoft Sentinel), SOAR- (z. B. Palo Alto XSOAR) und Ticketing-Systeme (z. B. ServiceNow, Jira). Die Plattform liefert priorisierte Findings direkt in bestehende Workflows, sodass Sicherheitsteams ohne Toolwechsel agieren können.
- **Schulung:** Workshops für Sicherheitsteams und Führungskräfte.

Gesetzliche Anforderungen

Gemäss Art. 716a OR trägt der Verwaltungsrat die Verantwortung für die Oberleitung und Überwachung des Risikomanagements. Cyberrisiken sind heute Geschäftsrisiken. Attack Path Management liefert dem Verwaltungsrat die notwendige Transparenz, um seiner Sorgfaltspflicht nachzukommen – mit quantifizierbaren Metriken und nachvollziehbarer Dokumentation.

Einordnung und Limitationen: Attack Path Management ist ein leistungsfähiger Baustein einer modernen Sicherheitsarchitektur, ersetzt jedoch nicht die Grundlagen wie Patch-Management, Netzwerksegmentierung und Security Awareness. Die in diesem Paper dargestellten Daten stammen aus dem XM Cyber Impact Report und spiegeln die Kundenbasis wider.

10 Mehrwert auf einen Blick

Dimension	Konkreter Nutzen
Risikotransparenz	Vollständige Sichtbarkeit aller Angriffspfade zu geschäftskritischen Assets – on-premises, Cloud und hybrid
Effizienz	80 % weniger zu behebende Probleme durch Fokussierung auf Choke Points statt auf Tausende isolierter Schwachstellen
Compliance	Nachweisbare Sorgfaltspflicht gemäss Art. 716a OR, DSGVO, NIS2 und ISO 27001 durch kontinuierliche, dokumentierte Risikoanalyse
Board-Reporting	Verständliche, datenbasierte Berichte für Verwaltungsrat und Geschäftsleitung – keine technischen Details, sondern Geschäftsrisiken
Cloud-Sicherheit	Erkennung plattformübergreifender Angriffspfade zwischen On-Premise, AWS und Azure
Kontinuität	24/7-Analyse statt punktueller Penetrationstests – kontinuierliche Verbesserung der Sicherheitslage
ROI	Gezielte Investitionen in die wirkungsvollsten Massnahmen statt Ressourcenverschwendung auf unkritische Schwachstellen
CTEM	Fundament für ein Continuous Threat Exposure Management nach Gartner-Framework

11 Fazit und Empfehlungen

Die Ergebnisse des XM Cyber Impact Reports sind eindeutig: Isolierte Sicherheitstools reichen nicht aus. Es ist die Kombination mehrerer Angriffstechniken, Schwachstellen, Fehlkonfigurationen und Zugangsdaten-Probleme, die Angreifern den Weg zu geschäftskritischen Assets ebnet. Attack Path Management macht diese Pfade sichtbar und ermöglicht eine gezielte, ressourcenschonende Risikoreduktion.

Empfehlungen

1. Konzentrieren Sie Ihre Sicherheitsmassnahmen auf verschiedene Umgebungen, um zu verstehen, wie Angreifer von On-Premise auf die Cloud wechseln können.
2. Betrachten Sie nicht nur Schwachstellen isoliert: 73 % der Top-Angriffstechniken basieren auf Zugangsdaten-Problemen.
3. Implementieren Sie Attack Path Management, um Choke Points zu identifizieren und mit minimalem Aufwand maximale Risikoreduktion zu erzielen.
4. Etablieren Sie ein CTEM-Programm für kontinuierliche Verbesserung Ihrer Sicherheitslage.
5. Stellen Sie sicher, dass Ihr Verwaltungsrat regelmässig über den Sicherheitsstatus informiert wird und dies mit verständlichen, risikobasierten Berichten.

Stellen Sie sich die wichtigsten Fragen

- Was könnte derzeit in meiner Umgebung kompromittiert werden?
- Wie viele verschiedene Wege führen zu meinen kritischen Assets?
- Welche Massnahmen hätten den grössten Einfluss auf meine Sicherheitslage?
- Sind meine Cloud- und On-Premise-Umgebungen wirklich voneinander getrennt?

Um zu verstehen, ob die kritischsten Assets Ihres Unternehmens sicher sind, müssen Sie wissen, wie sich die Dinge im Laufe der Zeit verändern und wie Angreifer verschiedene Schwachstellen kombinieren. Nur mit einem ganzheitlichen Ansatz wie Attack Path Management erhalten Sie die Transparenz, die Sie für fundierte Entscheidungen brauchen.

SecureComply
Secure by Design. Compliant by Default.

Jetzt Beratungsgespräch vereinbaren

Wir analysieren Ihre bestehende Infrastruktur und zeigen Ihnen, wie die Lösung von XM Cyber konkret bei Ihnen greift.

info@securecomply.ch | www.securecomply.ch

Antwort innerhalb von 24 Stunden