# Risk und Vulnerability Management

## Cybersecurity-Leitfaden für Attack Path Management

XM Cyber

GRAVITATE

# Executive Summary

In der Cybersicherheitsbranche lässt sich eine positive Entwicklung beobachten. IT-Teams werden immer erfahrener und sind sich der Bedrohungen, denen sie heute ausgesetzt sind, immer bewusster. Deshalb haben Unternehmen ein besseres Verständnis dafür entwickelt, dass der Schutz kritischer Unternehmensressourcen vor dem Hintergrund immer raffinierterer Angriffe eine ständige Identifizierung und Behebung der größten Cyberrisiken erfordert. Sie müssen verstehen, wie diese Risiken in verschiedenen Umgebungen zusammenwirken, um kritische Ressourcen zu gefährden.

Wenn Unternehmen **Attack Path Management** (APM oder Angriffspfad-Management) für ihre On-Premise-, SaaS- und Cloud-Umgebungen einsetzen, können sie ihr Risiko kontinuierlich reduzieren. Sie können verborgene Angriffspfade aufdecken, Lücken in den Sicherheitskontrollen identifizieren, Sicherheitsrisiken priorisieren und Abhilfemaßnahmen gezielt einsetzen.

Das Angriffspfad-Management geht dabei über die Identifizierung verschiedener technischer Schwachstellen wie Schwachstellen, Fehlkonfigurationen und Identitätsverletzungen hinaus. Es ermittelt auch, wie Angreifer verschiedene Angriffstechniken einsetzen können, um einen Weg zur Ausnutzung kritischer Unternehmensressourcen zu finden. Die Identifizierung von Angriffsvektoren und Angriffswegen mit hoher Priorität verringert das Risiko und hat den zusätzlichen Vorteil, dass der Gesamtaufwand für die Behebung von Schwachstellen reduziert wird, da Patches mit geringem Risiko nicht mehr vorrangig behandelt werden müssen.

Untersuchungen haben ergeben, dass mit einer geeigneten Lösung die Wahrscheinlichkeit einer schwerwiegenden Sicherheitsverletzung **um 90 % gesenkt** werden kann, da die Angriffspfadverwaltung vor Ort, in der Cloud und bei SaaS eine große Bandbreite abdeckt und einen ROI von bis zu 400 %[1] ermöglicht.


Dieser Leitfaden beschreibt, wie Sie Ihre Cyberrisiken reduzieren können und erläutert, warum viele Unternehmen sich für den Einsatz der neuen Technologie des Attack Path Managements entscheiden. Darüber hinaus bietet er Ratschläge zur Bewertung von APM-Lösungen und zur Evaluierung des Einsatzes einer solchen Lösung.

1 Forrester Total Economic Impact Study, 2022

# Wie können Unternehmen Angriffspfade verwalten und ihr Risiko verringern?

## Was ist ein Angriffsweg (Attack Path)

Der Attack Path ist der Weg, den ein Angreifer vom Einbruchspunkt bis zu Ihrem kritischen IT Dienst oder eine Anwendung nimmt. Dabei nutzt der Angreifer bei jedem Schritt auf dem Pfad eine Technik, um die Entität zu kompromittieren, und dringt dann zur nächsten Entität vor. Untersuchungen haben ergeben, dass 94% der kritischen Anlagen in weniger als vier Anläufen vom ersten Einbruchspunkt aus kompromittiert werden können.[2]

Um einen Angriffspfad klar zu verstehen, muss man wissen, was ein Angriffsvektor ist. Ein Angriffsvektor ist eine Methode, die Cyberangreifer verwenden, um in ein System einzudringen. Obwohl die Begriffe manchmal vermischt werden, sind **Angriffsvektoren nicht mit einer Angriffsfläche zu verwechseln**, die am besten als jeder mögliche Punkt definiert wird, an dem ein Angreifer versuchen kann, in Ihr Netzwerk oder System einzudringen.

Ein Angriffspfad ist also eine Visualisierung der Ereigniskette, die auftritt, wenn Angriffsvektoren ausgenutzt werden. In diesem Sinne stellt ein Angriffsvektor eine Tür dar, während ein Angriffspfad eine Karte ist, die zeigt, wie ein Angreifer durch die Tür gekommen ist und wohin er gegangen ist. **Malware, Ransomware oder Phishing** sind alles Beispiele für gängige Angriffsvektoren.

Während Cloud-Angriffsvektoren verwendet werden können, um eine Sicherheitslücke in Ihrem Netzwerk oder System auszunutzen, können Vektoren auch genutzt werden, um **menschliche Fehler** auszunutzen.

Angreifer nutzen oft mehrere Vektoren, um einen Angriff durchzuführen. Wenn Sie mehrere Angriffstechniken miteinander kombinieren, können Sie einen Angriffsvektor schaffen, und wenn Sie mehrere Angriffsvektoren miteinander kombinieren, können Sie einen Angriffspfad schaffen.
Es ist auch wichtig zu wissen, dass es Angriffsvektoren geben kann, auch wenn sie scheinbar entschärft sind. Ein sehr sicheres Passwort hilft beispielsweise nicht viel, wenn Sie nicht wissen, dass dieses Passwort im Dark Web verfügbar ist und nur darauf wartet, dass ein Angreifer es gegen Sie verwendet.

2 XM Cyber Attack Path Management Impact Report, 2022

# Warum ist das Angriffspfad-Management so wichtig?

Im Vergleich zu vor zwei Jahren nehmen die Cyberrisiken zu. Laut ESG-Forschungsergebnissen geben 82 %[3] der Unternehmen an, dass das Cyberrisiko in den letzten zwei Jahren gestiegen ist.

Dieser Anstieg ist auf Faktoren wie die Zunahme von Cyberbedrohungen, die größere Abhängigkeit von der IT bei der Erfüllung des Geschäftsauftrags und die Zunahme der Anzahl von Assets auf den Angriffsflächen zurückzuführen. Führungskräfte und Unternehmensvorstände haben diesen Trend erkannt und drängen die CISOs, den Schutz vor Cyberrisiken zu verbessern.

Vielen Unternehmen fehlt jedoch oft das richtige Maß an Risikobewusstsein. Mit anderen Worten: Sie wissen nicht, ob die zunehmende Gefährdung ihrer kritischen Vermögenswerte ein Risiko darstellt. Diese Situation stellt CISOs vor offene Fragen, da sie den Geschäftsmanagern keinen genauen Cyberrisikostatus vermitteln können und nicht sicher sind, wie sie Investitionen zur Risikominderung priorisieren sollen.

Während Unternehmen oft auch mehrere isolierte Tools und manuelle Prozesse für das Cyberrisikomanagement verwenden, nutzen Angreifer automatisierte Tools, um die Angriffsfläche kontinuierlich nach benutzer- und geschäftskritischen Schwachstellen zu durchsuchen.

Insgesamt zeigt sich ein Missverhältnis: **Zwei Drittel der Unternehmen haben bereits einen Cyberangriff** erfahren, der von einem unbekannten, schlecht verwalteten oder ungeschützten internetfähigen System ausging. Einmal kompromittiert, können sich Angreifer leicht seitlich durch Netzwerke bewegen. Hierunter fallen Ransomware-Angriffe, Datenschutzverletzungen und Verstöße gegen gesetzliche Vorschriften.

**Die wichtigsten Herausforderungen, denen sich Unternehmen heute stellen müssen:**

- Cyberkriminelle werden immer besser und agieren immer häufiger.
- Anders als bei Penetrationstests werden bei vielen Alternativlösungen nur einzelne Anlagen bewertet, ohne dass die Pfade und die Beziehung zu kritischen Anlagen effektiv bewertet werden.
- Penetrationstests werden aufgrund von Kosten, Geschäftsunterbrechungen und Arbeitsaufwand nur in regelmäßigen Abständen durchgeführt.
- Unternehmen haben eine ständige Liste mit Tausenden bis Hunderttausenden von Patches.
- Eine sich ständig verändernde IT-Infrastruktur schafft neue Wege und Möglichkeiten für cyberkriminelle Angriffe.

# Was ist Attack Path Management (APM)?

## Was sind die wichtigsten Aspekte einer APM-Lösung?

Jedes Unternehmen möchte sein Cyberrisiko verringern. Attack Path Management schafft einen fortlaufenden Prozess zur Identifizierung und Beseitigung von Angriffspfaden auf kritische Ressourcen. Es kann Unternehmen dabei helfen, ihre kritischsten Risiken wie Fehlkonfigurationen, riskante Benutzer und Software-Schwachstellen in der gesamten hybriden Umgebung zu identifizieren, kosteneffiziente Abhilfemaßnahmen zu ergreifen, indem Ressourcen auf die Behebung von Engpässen gerichtet werden, Knotenpunkte, durch die viele Angriffspfade verlaufen zu erfassen, Risikominderungsstrategien zu identifizieren und den Erfolg im Laufe der Zeit zu verfolgen.

**APM-Lösungen sollten:**

- Eine automatisierte Methodik zur häufigen Analyse der Sicherheitsrisiken in der gesamten Infrastruktur des Unternehmens bieten, ohne dass es zu Ausfällen, Unterbrechungen oder Leistungsproblemen kommt.
- Cyberangriffspfade verstehen und Sicherheitsprobleme identifizieren, die die kritische Infrastruktur am stärksten gefährden.
- Sofort einsatzbereite Szenario-Analyse sowie benutzerdefinierte Abläufe bereitzustellen, die auf einzigartigen Kundenerfahrungen oder spezifischen Bedrohungen wie Malware oder Zero-Day-Schwachstellen basieren.
- Den Bedarf an anderen Schwachstellenmanagement-Aktivitäten reduzieren, insbesondere an Pen-Tests.

# Der Verlauf von APM-Angriffsflächen

### Breach Points

APM identifiziert potenzielle Schwachstellen und Angriffspunkte in der IT-Infrastruktur des Unternehmens, die von Angreifern ausgenutzt werden könnten, um in das Netzwerk einzudringen.

### Kritische Assets

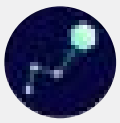
APM erkennt die kritischen Assets des Unternehmens, die bei einem erfolgreichen Angriff am meisten Schaden anrichten könnten. Dazu zählen etwa Datenbanken, Kundendaten oder geistiges Eigentum.

### Kampagnen

APM simuliert Angriffe, um zu testen, wie gut die IT-Sicherheitsmaßnahmen des Unternehmens funktionieren. Dabei können verschiedene Angriffsszenarien durchgespielt werden.

### Szenarien

APM erstellt maßgeschneiderte Angriffsszenarien, die auf die spezifischen Schwachstellen und kritischen Assets des Unternehmens abgestimmt sind. Dadurch können gezielte Angriffe simuliert werden, wie sie auch von echten Angreifern durchgeführt werden könnten.



### Choke Points

APM identifiziert die "Choke Points" im Netzwerk, also die Engpässe, die bei einem Angriff besonders kritisch werden könnten. Dazu zählen etwa Firewalls, Gateways oder VPNs. Durch gezielte Angriffe auf diese Choke Points kann getestet werden, ob die IT-Sicherheitsmaßnahmen des Unternehmens auch unter extremen Bedingungen funktionieren.

# Andere Bewertungsüberlegungen

## Simulation von Sicherheitsverletzungen und Angriffen - Breach and Attack Simulation (BAS)

Es handelt sich hier um Lösungen, welche die Bewertung der Sicherheitslage automatisieren, indem sie technische und prozessuale Sicherheitskontrollen zwischen verschiedenen Segmenten interner und externer Netze kontinuierlich überprüfen.

Welche Arten von Sicherheitskontrollen werden mit BAS-Lösungen getestet? Und was testen sie nicht? EPP (Endpoint Protection Platform), E-Mail-Gateways, IPS, IDS-Lösungen und Secure Web Gateways sind einige der Kontrollen, die getestet werden. Was jedoch nicht getestet wird, sind Risiken in PAM-Lösungen (Privileged Access Management), Fehlkonfigurationen in Active Directory und potenzielle Risiken von Identitäten und Schwachstellen. Durch nicht verwaltete Aktivitäten wie Fehlkonfigurationen, gemeinsam genutzte Anmeldeinformationen und unzureichende Benutzeraktivitäten können Angreifer diese Sicherheitslücken ausnutzen, um kritische Ressourcen zu kompromittieren.

## Vulnerability Scanner

Es handelt sich um einen regelmäßigen Prozess zur Identifizierung, Bewertung, Meldung, Verwaltung und Behebung von Sicherheitsschwachstellen und fehlenden Patches auf internen und externen Endgeräten und Systemen. Das Schwachstellenmanagement in seiner heutigen Form ist in erster Linie in Bezug auf den gesamten Prozess der Schwachstellenerkennung, -priorisierung und -behebung ineffektiv. Die Kombination aus unregelmäßigen Scans und nicht integrierten Pen-Tests hinterlässt Lücken und blinde Flecken, ist auf den Kontext der Umgebung beschränkt und viele kritische Schwachstellen fehlen noch immer in der Bewertung.

Traditionell suchen Lösungen nach ausnutzbaren Schwachstellen unter Verwendung von CVSS-Scoring, das sich allgemein auf das Risiko der kritischen Assets - und nicht auf die gezielte Herkunft und Stoßrichtung dieser konzentriert. Es ist nahezu unmöglich, die Risikoexposition zu priorisieren, wenn man die Vor- und Nachbedingungen sowie die Angriffspfade nicht kennt und keine Angriffspunkte sieht, um die Angriffspfade an wichtigen Punkten zu unterbrechen.

## Penetrationstests (Pen-Tests)

Sicherheitslücken entstehen oft durch fehlerhaften Softwarecode, Hintertüren in Betriebssystemen, unsachgemäße Konfigurationen und andere ähnliche Probleme. Bei einem Pen-Test wird versucht, solche Probleme aufzudecken, indem Server, drahtlose Netzwerke, mobile Geräte und andere mögliche Einstiegspunkte für Angreifer ins Visier genommen werden. Wie Sie sich vielleicht vorstellen können, sind manuelle Pen-Tests in der Regel ressourcenintensiv, es fehlt eine Priorisierung, und die Ergebnisse sind oft schon veraltet, sobald sie veröffentlicht werden. Die meisten Unternehmen müssen geschulte White Hat Pen Testing- oder Red Team Pen Testing-Experten von Dritten mit der Durchführung der Übung beauftragen.

Alternativ können sie auch ihre eigenen Red, Blue oder Purple Teams aus internen Mitarbeitern zusammenstellen, wenn sie über das entsprechende Fachwissen verfügen. Die Ergebnisse von Penetrationstests liefern für einen begrenzten Bereich sehr zuverlässige Ergebnisse, allerdings mit einem hohen manuellen Aufwand. Mit einer Attack Path Management-Lösung können Unternehmen ihre Kosten für Penetrationstests über einen Zeitraum von drei Jahren um bis zu 1,3 Millionen Euro senken[3].

3 Forrester Total Economic Impact Study, 2022

## Angriffsflächen-Management - Attack Surface Management (ASM)

Die Angriffsflächen haben sich in den letzten Jahren rapide vergrößert, was zum Teil auf die Cloud und die zunehmende Beliebtheit von Remote-Arbeiten zurückzuführen ist. Dies hat Angreifern eine reichhaltige Angriffsfläche für ihre Aktivitäten geboten. ASM-Lösungen werden von Unternehmen eingesetzt, um nach außen gerichteten Ressourcen zu erkennen, zu analysieren, zu kategorisieren und zu verwalten.

Die Klassifizierung und Überwachung einer ständig wachsenden Angriffsfläche ist nicht einfach - die meisten Unternehmen geben an, dass sie sich nicht darum bemühen. Einige überwachen nur einen kleinen Teil ihrer Angriffsfläche, und eine beunruhigend große Zahl von Unternehmen verfügt über mit dem Internet verbundene Geräte in ihren Netzwerken, von denen sie nicht einmal wissen. Eine der besten Möglichkeiten, um eine starke ASM-Cybersicherheit zu erreichen, ist die Einführung einiger grundlegender Sicherheits-Frameworks, die dazu beitragen, die Entstehung neuer Fehlkonfigurationen/Schwachstellen zu reduzieren, wie z. B. ein Zero-Trust-Framework im gesamten Unternehmen.

# Wichtige Merkmale und Funktionen, die bei APM-Lösungen zu bewerten sind

### Kontextualisierung
Kontextualisierung von Fehlkonfigurationen, Schwachstellen und risikobehafteten Benutzern und wie sie alle genutzt werden können, um kritische Ressourcen in On-Premise-, Cloud- und SaaS-Umgebungen zu gefährden.

### Prioritätensetzung
Betrachtet alle Risiken und priorisiert sie nach ihrer Auswirkung auf kritische Ressourcen, damit Sie wissen, welche Maßnahmen Sie ergreifen müssen, um die schädlichsten Angriffspfade zuerst zu unterbrechen.

### Kontinuierlich
Die moderne Angriffsfläche ist dynamisch und verändert sich ständig. Versteht ständig die Angriffswege und wie leicht sie mit den neuesten Schwachstellen und Angriffstechniken zu aktualisieren sind, sowie den operativen Aufwand, der für eine kontinuierliche Ausführung erforderlich ist.

### Betriebliche Sicherheit und Auswirkungen
Hier geht es um zwei Bereiche. Erstens, wie riskant es ist, die Tools in Produktionsumgebungen einzusetzen, z. B. durch den Einsatz von Live-Exploits! Zweitens, wie einfach die Tools im Betrieb zu handhaben sind und wie hoch der Planungs- und Ressourcenaufwand für den Betrieb des Tools ist.

### Umfassend
Die Lösung sollte alle Workstations, Entitäten, virtuellen Maschinen, Container, Benutzeraktivitäten und Konfigurationen usw. als Teil der Angriffspfadanalyse berücksichtigen, um sicherzustellen, dass Sie alle Möglichkeiten sehen, wie Ihr Unternehmen gefährdet ist, um priorisierte Abhilfemaßnahmen zu planen.

### Auflösung
Sparen Sie Zeit für Analysten, indem Sie die Angriffspfade an den wichtigsten Knotenpunkten, den sogenannten Choke Points, mit einem kostengünstigen Ansatz mit maximaler Wirkung unterbrechen.
Durch den Einsatz von Attack Path Management können Unternehmen Kosten für die Behebung von Mängeln, Bußgelder, Kundenkosten, Umsatzeinbußen und den Wiederaufbau der Marke in Höhe von bis zu 11,5 Millionen Euro über drei Jahre vermeiden[4]. Unternehmen reduzieren die Häufigkeit und Schwere von Cybersecurity-Angriffen, indem sie das Attack Path Management nutzen, um den Fokus auf Sicherheitsrisiken und Abhilfemaßnahmen auf Probleme im Zusammenhang mit kritischen Anlagen zu legen.

### Verbesserung
Mit der automatisierten Planung von Abhilfemaßnahmen, die in Ihren Betrieb eingebettet ist, können Sie Geschäftsentscheidungen vorantreiben und feststellen, dass sich Ihre Sicherheitsinvestitionen auszahlen.
Untersuchungen haben gezeigt, dass Unternehmen mit einem kostengünstigen Ansatz wie Attack Path Management 80 % weniger Probleme beheben müssen, wenn sie wissen, wo sie die Angriffspfade unterbrechen müssen[5].

### Berichterstattung auf Vorstandsebene
Ermöglicht eine genaue Risikobewertung und kann die Berichterstattung an die Geschäftsleitung und die operativen Prozesse unterstützen. Der Vorstand kann schnell nachvollziehen, wie sein Unternehmen angegriffen werden kann, wie sich die Situation im Laufe der Zeit aufgrund von Sicherheitsinvestitionen, Prozessänderungen oder der Implementierung von Umgebungshärtung verbessert hat und vor allem, wie hoch das Risiko für kritische Anlagen ist.

4 Forrester Total Economic Impact Study, 2022
5 XM Cyber Attack Path Management Impact Report, 2022

# Beispiele aus der realen Welt:

## Durch Attack Path Management entdeckte Risikopotenziale

1

*"Eine Schwachstelle in einem globalen Unternehmen ermöglichte es nicht privilegierten Benutzern, Administratorkonten zu kompromittieren. Mit der Zero-Logon-Schwachstelle konnte das Active Directory am asiatischen Standort des Unternehmens kompromittiert werden, das mit allen anderen ADs in der Organisation vertrauenswürdig war."*

Leiter der Abteilung Technical Enablement

2

*"Jeder Administrator hatte ein einziges Login für jede administrative Aufgabe. Benutzerverwaltung, Datenbank, usw. Dies ist eine schlechte Praxis, denn wenn das Konto kompromittiert wird, hat der Angreifer freie Hand. Lösungen für das Attack Path Management können zeigen, wie Anmeldedaten ausspioniert werden können, was zur Kompromittierung kritischer Ressourcen führt."*

Technischer Direktor

3

*"In einer Produktionsumgebung kann es nicht nur zu Sicherheitsproblemen kommen, sondern auch zu Gesundheits- und Sicherheitsproblemen. Mit den gefundenen Angriffspfaden könnte ein Angreifer einen Server kompromittieren, der für die Steuerung von unbemannten Fahrzeugen zuständig ist, die in der Fabrik für den Transport von Produktionsgütern von A nach B verantwortlich sind. Mit Zugang könnte ein Angreifer die Kontrolle über die Geräte erlangen und physischen Schaden anrichten. "*

Technischer Direktor

4

*"Das Securityteam entdeckte einen Angriffspfad, der einen Entwicklungsserver nutzte, der den größten Teil des Unternehmensnetzwerks kompromittieren konnte. Nachdem sie sich den Server angesehen hatten, erkannten sie, dass er keinen Zweck erfüllte und ein unnötiges Risiko im Netzwerk darstellte."*

Leiter des Serviceteams

5

*"Die interessantesten Angriffspfade kombinieren mehrere Kategorien von Telemetriedaten: Lokale Anmeldeinformationen wurden genutzt, um zu einem anderen Windows-Rechner überzuwechseln. Der Angreifer wurde dann strategisch im Netzwerk positioniert, wo er auf einen Proxy-Broadcast von der kritischen Anlage reagieren konnte. Die neue Netzwerkpositionierung ermöglichte es ihm, eine falsch konfigurierte Windows-Update-Anfrage abzufangen und eine Schwachstelle auf dem kritischen System auszunutzen, um den Computer zu kompromittieren."*

Direktor für Vertriebstechnik

# Zu beachtende Trends bei der Verringerung des Risikos mit APM-Lösungen

### ⇢ Hybride Cloud-Sicherheit

Unternehmen verlagern wichtige Ressourcen in die Cloud, können aber nicht erkennen, wie diese Ressourcen angegriffen werden können!

### ⇢ Cyberrisiko-Berichterstattung

Viele Unternehmen wissen nicht, wie sie die wichtigste Frage beantworten sollen: Sind unsere kritischen Anlagen geschützt?

### ⇢ Lieferkette und Drittparteirisiko

Sie wissen, dass Ihre Geschäftspartner gefährdet sein werden. Aber Sie können nicht erkennen, wie Ihr Unternehmen dadurch gefährdet wird!

### ⇢ Fusionen und Akquisitionen

Unternehmen müssen ihre Infrastruktur konsolidieren und integrieren, können aber nicht erkennen, wie all diese Veränderungen das Programm gefährden.

### ⇢ Schwachstellenbewertung und Schwachstellenmanagement

Unternehmen wissen nicht, welche Schwachstellen ausgenutzt werden können, um ihre wichtigen Anlagen zu gefährden.

### ⇢ Operationalisierung

Sehen Sie Ihre hybride Angriffsfläche, um Risiken zu verringern und die digitale Transformation zu beschleunigen.

### ⇢ Ransomware-Bereitschaft

Sie wissen, dass Angreifer den ersten Fuß in die Tür setzen werden, aber Sie wissen nicht, wie sich dies auf Ihre kritischen Anlagen auswirken wird.

### ⇢ OT-Sicherheit

Erkennen Sie Sicherheitslücken und Korrelationen zwischen Umgebungen, um gezielte Abhärtungsmaßnahmen zu ergreifen.

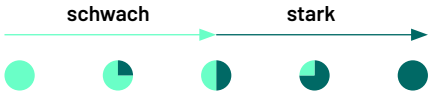
# Wie die Anbieter aufgestellt sind

| Anwendungsfälle | XM Cyber | Cloud Security | Breach and Attack Simulation | Vulnerability Prioritization |
|---|---|---|---|---|
| Vorbeugung von Cybersicherheitsrisiken auf der Grundlage der tatsächlichen Ausnutzbarkeit von Risiken und des Aufwands für deren Behebung in der Hybrid Cloud | ● | ◕ | ◑ | ◑ |
| Erkennung von anomalem Verhalten | ○ | ◑ | ◕ | ○ |
| Risikotransparenz und Prioritätensetzung für geschäftskritische Anlagen | ● | ◕ | ◕ | ◑ |
| Verknüpfung von Fehlkonfigurationen, Benutzerverhalten und Schwachstellen zur Identifizierung versteckter Angriffspfade | ● | ◕ | ◑ | ◔ |
| Verstehen des Risikos für kritische Anlagen durch unternehmensweite Risikobewertung | ● | ◕ | ◕ | ◔ |
| Unterstützung für große Infrastrukturen (nicht-intrusiv, kein bösartiger Code in der Produktion, keine Ermüdung durch Alarme) | ● | ● | ◔ | ◕ |
| Behebungsorientierter Ansatz zur Verbesserung der Sicherheitslage | ◕ | ◑ | ◑ | ◔ |
| Security Posture Scoring, das an das tatsächliche Risiko angepasst ist und Trends im Zeitverlauf aufzeigt | ● | ◑ | ◑ | ○ |

| Leistungen Cloud Security | XM Cyber | Wiz | Orca | PAN | Check Point |
|---|---|---|---|---|---|
| Einzelansicht aller Angriffspfade in On-Premise- und Cloud-Umgebungen | ● | ○ | ○ | ○ | ○ |
| Choke-Point-Analyse für kosteneffektive Abhilfemaßnahmen | ● | ○ | ○ | ○ | ○ |
| Verwaltung der Sicherheitslage in der Cloud (CSPM) | ● | ● | ● | ● | ● |
| Ganzheitliche Ansicht der Risikoexposition in der gesamten hybriden Umgebung mit Sicherheitsbewertung und Trends im Zeitverlauf | ● | ◕ | ◕ | ◕ | ◕ |
| Einfache Definition von Risikoszenarien mit Angriffspfaden, die sich auf kritische Ressourcen konzentrieren, um Sicherheitslücken zu erkennen und Risiken zu reduzieren | ● | ◑ | ◑ | ○ | ○ |

| Leistungen<br>Breach & Attack Simulation | XM Cyber | Cymulate | SafeBreach | Pentera | Picus Security |
|---|---|---|---|---|---|
| Abdeckung konstanter Szenario-Simulationen und die Pen-Test-Aktivitäten zu reduzieren | ● | ◕ | ◑ | ● | ◔ |
| Kontinuierliche und sichere Simulation | ● | ◕ | ◑ | ◔ | ◑ |
| Validierung von Sicherheitskontrollen und automatisierte Penetrationstests | ◐ | ● | ● | ● | ● |
| Angriffspfadanalyse für Active Directory in der Hybrid-Cloud-Umgebung | ● | ◔ | ○ | ◔ | ○ |
| Breites Spektrum an Anwendungsfällen, einschließlich Risikomanagement von Drittanbietern, Erstellung von Geschäftsrisikoprofilen und proaktiver Risikoverringerung | ● | ◕ | ◑ | ◔ | ◑ |

| Leistungen<br>Priorisierung von Schwachstellen | XM Cyber | Tenable.io | Microsoft Defender VM | Qualys VMDR | Rapid 7 Insight VM |
|---|---|---|---|---|---|
| Priorisierung von Schwachstellen auf der Grundlage der risikoreichsten Anlagen und der Ausnutzbarkeit von CVEs | ● | ● | ● | ● | ● |
| CVE-Priorisierung auf der Grundlage der Ausnutzbarkeit von Angriffspfaden | ● | ○ | ○ | ○ | ○ |
| Entdeckung von Anlagen im gesamten Netzwerk | ◐ | ● | ● | ● | ● |
| Kombinieren Sie mehrere Arten von Gefährdungen über CVEs hinaus, um zu wissen, was angreifbar ist | ● | ● | ● | ● | ● |
| Effiziente Abhilfemaßnahmen auf der Grundlage der Analyse von Engpässen | ◔ | ◔ | ● | ● | ◔ |




# Wichtige Fragen an die Anbieter

CISOs können ihre kritischen Risikopositionen mit Attack Path Management-Lösungen identifizieren, da sie viele Funktionen in einer einzigen Plattform vereinen.

**Attack Path Management nimmt die Perspektive des Angreifers ein, um Fragen zu beantworten wie:**

Wie kann ich angegriffen werden?
Welche meiner kritischen Anlagen sind gefährdet?
Wie kann ich diese Risiken mit minimalem Aufwand mindern?

Mit diesem Wissen können CISOs ihre kritischsten Risiken wie Fehlkonfigurationen, riskante Benutzer und Software-Schwachstellen in On-Premise-, Cloud- und SaaS-Systemen identifizieren. CISOs können auch kosteneffiziente Abhilfemaßnahmen ergreifen, indem sie Ressourcen zur Behebung von Engpässen einsetzen - jenen Knotenpunkten, durch die viele Angriffspfade verlaufen. Diese Maßnahmen können CISOs dabei helfen,

# Cybersecurity-Leitfaden für Attack Path Management

GRAVITATE

Gravitate GmbH
Fürther Straße 27
D-90429 Nürnberg

Tel. + 49 911 28 7070 78
info@gravitate.eu

**www.gravitate.eu**

XM Cyber