



Global Leader in  
Cybersecurity

# NIS2-Pflicht zum Cyber-Risikomanagement erfüllen

Attack Surface Risk Management (ASRM)



# BETREIBEN SIE SCHON CYBER-RISIKOMANAGEMENT?

Risikomanagement – das ist doch ein alter Hut. Oder etwa nicht? Natürlich haben Sie die Risiken für einen Stromausfall, einen Brand oder Hochwasser bewertet und entsprechende Vorkehrungen getroffen. Einmal aufgesetzt, dokumentiert, abgehakt. Cyber-Risikomanagement ist dagegen nie abgeschlossen, sondern muss kontinuierlich erfolgen. Denn eine IT-Umgebung, die heute sicher war, kann morgen schon hochgefährdet sein.

Vielleicht sind neue Assets hinzugekommen, Konfigurationsfehler passiert oder neue Schwachstellen und Angriffsszenarien bekannt geworden. Die Lage ist ernst: Gerade Behörden stehen derzeit im Fokus von Cyberkriminellen, weil es dort lukrative Daten zu erbeuten gibt. Dass Sie mit Ihrem knapp besetzten IT-Team kaum hinterherkommen, Schwachstellen zu schließen, spielt den Hackern in die Hände. Umso wichtiger ist es, die größten Risiken zuerst zu mindern. Nicht umsonst wird Cyber-Risikomanagement mit der NIS2-Richtlinie zur Pflicht.

## WAS BEDEUTET CYBER-RISIKOMANAGEMENT?

Sie müssen in der Lage sein, Cyberrisiken zu erkennen, zu bewerten und angemessene Gegenmaßnahmen zu ergreifen. Welche Risiken können Sie in Kauf nehmen? Welche müssen Sie unbedingt mindern? Was heißt angemessen? Ihr Chef erwartet von Ihnen eine Entscheidungsgrundlage. Wenn das nur so einfach wäre..



Sie haben keine Security-Kennzahlen zum Risikostatus und zu wenig Visibilität.



Ihr Schwachstellenscanner spuckt zwar jede Menge Warnmeldungen aus. Wie gefährlich diese tatsächlich sind, geht aus dem CVSS-Wert alleine aber nicht hervor. Sie brauchen den individuellen Kontext: Wie exponiert ist die Schwachstelle? Wird sie gerade häufig von Cyber-Gangs ausgenutzt? Wie hoch wäre das Schadensausmaß?



Um Cyberrisiken zu bewerten müssen Sie Ihre IT-Umgebung aus der Angreifer-Perspektive betrachten. Dafür müssen Sie unzählige interne und externe Security-Informationen sammeln und korrelieren. Nur wie?



Der aktuelle BSI-Lagebericht spricht von durchschnittlich knapp 70 neu entdeckten Schwachstellen in Softwareprodukten pro Tag. Sie wissen aber oft gar nicht, welche Komponenten in Ihren Fachanwendungen verbaut sind. Außerdem haben Sie keine Zeit, sich mit allen Schwachstellen zu befassen.

Cyber-Risikomanagement ist eine Mammut-Aufgabe, die Sie trotz Fachkräftemangel und angespannter Haushaltslage jetzt auch noch nebenbei erledigen müssen. Ohne Automatisierung ist das nicht machbar.

## SO SCHAFFEN SIE DAS AM BESTEN

Sie brauchen eine Lösung, die kontinuierlich den aktuellen Risikostatus Ihrer IT-Umgebung ermittelt und Ihnen hilft, richtig zu priorisieren sowie schnell zu reagieren. Genau das macht Attack Surface Risk Management (ASRM): Die Technologie sammelt Information aller angeschlossenen Sensoren aus der IT-Umgebung und korreliert sie KI-gestützt mit Security-Informationen aus unzähligen externen Quellen, darunter Veröffentlichungen von Analysten, Security-Unternehmen, Polizeiorganisationen und Regierungsbehörden.

Intelligente Algorithmen berechnen, ob und wie stark die IT-Umgebung von aktuellen Schwachstellen und Angriffsmustern betroffen ist. Sobald ein von Ihnen gesetzter Schwellenwert überschritten wird, schlägt das System Alarm. Eine Ampeldarstellung zeigt an, wie gefährlich die ermittelten Risiken sind. Außerdem sehen Sie, welche IT-Assets involviert sind, und erhalten Handlungsempfehlungen zu Gegenmaßnahmen. Das ASRM-System kann viele Risiken sogar automatisiert mindern und zum Beispiel Schwachstellen mit Virtual Patching auf Netzwerkebene, sodass Sie mehr Zeit gewinnen, um Hersteller-Patches einzuspielen.



## WÄHLEN SIE EINEN PLATTFORM-ANSATZ!

Cyber-Risikomanagement muss ganzheitlich auf einer übergeordneten Ebene erfolgen. Nur so können Sie Zusammenhänge herstellen und auch Risiken in den Security-Systemen selbst erkennen. Denn sogar Firewalls & Co. könnten einmal kompromittiert werden. Ideal ist eine Cyber-Defense-Plattform, die ASRM und XDR (Extended Detection & Response) vereint. Beide Technologien nutzen dieselben Sensoren und spielen perfekt zusammen. Während ASRM dazu dient, die Eintrittswahrscheinlichkeit eines Cyberangriffs zu reduzieren, hilft XDR, einen Vorfall schnell zu entdecken und das Schadensausmaß zu mindern.

## DARUM LOHNT SICH ASRM



- Sie gewinnen umfassende Visibilität und haben Ihren aktuellen Risikostatus immer im Blick.
- Ihrem Chef können Sie jederzeit fundierte Security-Kennzahlen liefern
- Risiken können Sie besser bewerten und richtig priorisieren
- Sie können schneller Gegenmaßnahmen ergreifen – sogar automatisiert
- Wenn eine neue Schwachstelle veröffentlicht wird, sehen Sie sofort, ob Ihre Systeme betroffen sind.
- Sie erfüllen Ihre NIS2-Dokumentationspflicht. Per Knopfdruck können Sie detaillierte Berichte aus dem System exportieren.

## DER PARTNER AN IHRER SEITE



Trend Micro Vision One integriert modernste XDR-Funktionen mit leistungsstarkem Angriffsflächen-Risikomanagement und dynamischen Zero-Trust-Tools. Laut MITRE ATT&CK Evaluations sind wir führend bei der Ersterkennung.

Trend Micro (börsennotiert in Tokyo) hat über 30 Jahre Erfahrung als Spezialist für Sicherheitslösungen. Das Unternehmen wird seit 15 Jahren erfolgreich von seiner Mitgründerin Eva Chen geleitet, die als Leading Woman in IT international anerkannt ist. Seit der Gründung im Jahr 1988 achtet sie mit ihrem Managementteam darauf, dass das Unternehmen gesund wächst und reinvestiert auch in Krisenzeiten umfangreich in Forschung und Entwicklung.

Ihr Credo: „Unsere einzige Konkurrenz sind Cyberkriminelle, denen man Einhalt gebieten muss.“



Copyright © 2023 Trend Micro Incorporated. Alle Rechte vorbehalten. Trend Micro, das Trend Micro Logo und das T-Ball-Logo sind Marken oder eingetragene Marken von Trend Micro Incorporated. Alle anderen Firmen- bzw. Produktnamen sind Unternehmenskennzeichen oder eingetragene Marken ihrer jeweiligen Eigentümer. Die in diesem Dokument enthaltenen Informationen können sich ohne vorherige Ankündigung ändern. Trend Micro, das Trend Micro Logo und das T-Ball-Logo tragen das Registered-Trade-Mark-Symbol der USA. Einzelheiten darüber, welche personenbezogenen Daten wir erfassen und warum, finden Sie in unserer Datenschutzerklärung auf unserer Website unter: [https://www.trendmicro.com/de\\_de/about/legal/privacy.html](https://www.trendmicro.com/de_de/about/legal/privacy.html).