

Cyberisiken besser managen

Attack Surface Risk Management (ASRM)



RISIKOMANAGEMENT WIRD PFLICHT

Als IT-Sicherheitsverantwortlicher in der Energiebranche stehen Sie vor einer wachsenden Bedrohungslage und zahlreichen Compliance-Vorgaben. Neben dem IT-Sicherheitsgesetz 2.0 müssen Sie auch die branchenspezifischen Sicherheitsstandards (B3S) beachten. Im Bereich Energie sind dies insbesondere der „Branchenspezifische Sicherheitsstandard für Anlagen oder Systeme zur Steuerung/Bündelung elektrischer Leistung (B3S Aggregatoren)“ und der „Branchenspezifische Sicherheitsstandard (B3S) für die Verteilung von Fernwärme (Fernwärmenetze)“.

Ihr Unternehmen zählt zu den kritischen Infrastrukturen, und die Einhaltung der neuen Vorschriften ist unabdingbar. Mit dem Ende der Umsetzungsfrist des IT-SIG 2.0 im Mai 2023 hatten Sie in der letzten Zeit alle Hände voll zu tun und Ihre Ressourcen sind zunehmend gebündelt. Verstöße können erhebliche Strafen nach sich ziehen, insbesondere für KRITIS-Organisationen. Mit einem Bußgeld von bis zu zwei Millionen Euro oder sogar 20 Millionen Euro für juristische Personen sind die finanziellen Konsequenzen erheblich. Die steigenden Energiepreise machen den Markt zudem noch härter, und ein Cybervorfall kann den Ruf und die Kundenbindung ernsthaft gefährden.

ALLES NICHT SO EINFACH

Wo würden die Hacker zuerst angreifen und welche Auswirkungen hätte das? Das sind zentrale Fragen, um Risiken zu bewerten. Dafür müssen Sie Ihre IT-Umgebung aus der Perspektive der Cyberkriminellen betrachten. Anschließend können Sie gezielt Maßnahmen ergreifen, um die größten Risiken zu mindern. In der Theorie klingt das einfach, aber Sie stehen vor vielfältigen Herausforderungen, darunter:



Die Anforderungen des IT-SIG 2.0 und die branchenspezifischen Sicherheitsstandards (B3S).



Verschärfte Meldepflichten bei Cybervorfällen nach IT-SIG 2.0.



Schnelles Einspielen von Patches bei einer Vielzahl von Servern mit begrenztem IT-Personal.



Sicherung von OT- und IoT-Systemen, bei denen oft keine herkömmliche Security-Software installiert werden kann.



Komplexität und besondere Sicherheitsherausforderungen durch den verstärkten Einsatz von Cloud Services.

Cyber-Risikomanagement ist eine Mammut-Aufgabe, die Sie trotz Fachkräftemangel stemmen müssen. Ohne Automatisierung ist das nicht machbar.

WIE BEWÄLTIGEN SIE DAS?

Um den aktuellen Risikostatus Ihrer IT-Umgebung zu ermitteln und angemessen zu reagieren, benötigen Sie eine Lösung, die kontinuierlich arbeitet. Attack Surface Risk Management (ASRM) bietet genau das: Es sammelt Informationen aller angeschlossenen Sensoren aus Ihrer IT-Umgebung und korreliert sie KI-gestützt mit externen Security-Informationen. Intelligente Algorithmen analysieren, wie stark Ihre IT-Umgebung von aktuellen Schwachstellen und Angriffsmustern betroffen ist. Bei Überschreitung eines vordefinierten Schwellenwerts erhalten Sie automatische Warnungen. Eine Ampeldarstellung zeigt Ihnen die gefährlichsten Risiken auf einen Blick. Zudem erhalten Sie Handlungsempfehlungen zu Gegenmaßnahmen, und viele Risiken können automatisiert gemindert werden, beispielsweise durch Virtual Patching auf Netzwerkebene.

PLATTFORM-ANSATZ FÜR EFFEKTIVES SECURITY-MANAGEMENT

Cyber-Risikomanagement sollte auf einer übergeordneten Ebene erfolgen. ASRM und XDR (Extended Detection & Response) spielen dabei perfekt zusammen und sollten idealerweise unter einer Plattform vereint sein. ASRM warnt Sie vor aktuellen Schwachstellen und Angriffsmustern, während XDR hilft, Vorfälle schnell zu entdecken und das Schadensausmaß zu mindern.



DIESE VORTEILE ERZIELEN SIE MIT ASRM



- Kontinuierliche Überwachung des Risikostatus Ihrer IT-Umgebung.
- Schnelle Erkennung und Reaktion auf gefährliche Risiken.
- Dokumentation fundierter Security-Kennzahlen für den Unternehmensvorstand.
- Automatisierte Minderung von Risiken, auch auf Netzwerkebene.
- Effektive Bewältigung von Compliance-Anforderungen des IT-SIG 2.0 und B3S.
- Transparenz und Kontrolle in der gesamten IT-Umgebung, einschließlich der Cloud.
- Nachvollziehbarkeit bei Cyberangriffen zur Erfüllung von Meldepflichten.

DER PARTNER AN IHRER SEITE



Trend Micro Vision One integriert modernste XDR-Funktionen mit leistungsstarkem Angriffsflächen-Risikomanagement und dynamischen Zero-Trust-Tools. Mit Security-Systemen wie TippingPoint Threat Protection, Deep Security oder Apex One XDR von Trend Micro erhalten Sie Best of Breed-Lösungen aus einer Hand von einem Marktführer. Diese können zu einem umfassenden Cybersecurity-Konzept zusammengesetzt werden. 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.