Executive Insights

NIS2-konformes Risikomanagement:
Cyberrisiken als Geschäftsführungsverantwortung

Die EU-Richtlinie zur Netzwerk- und Informationssicherheit (NIS2) verankert das Management von Cyberrisiken als Teil des unternehmerischen Risikomanagements. Die Verantwortung der Geschäftsführungsebene für die Abwehr von Cyberrisiken wird unterstrichen. Dabei reicht es nicht mehr wie bisher, nur das eigene Unternehmen zu betrachten. Bei der Bewertung der Verhältnismäßigkeit von Maßnahmen muss auch berücksichtigt werden, welche Folgen für die deutsche Gesellschaft und Wirtschaft durch einen erfolgreichen Angriff entstehen könnten.

Aber auch dem Gesetzgeber ist klar, dass niemals alle Risiken im Voraus eliminiert werden können. Das liegt nicht allein an technischen, sondern auch an wirtschaftlichen Faktoren: Bei manchen Risiken liegt der Aufwand für eine Behebung schlicht über einem möglichen Schaden. NIS2 beschränkt also nicht den unternehmerischen Ermessenspielraum, fordert aber von Geschäftsführungen eine bewusste Auseinandersetzung mit der Risikolage. Dazu gehört der Einsatz von Maßnahmen zur Risikoabwehr sowie fundierte und dokumentierte Entscheidungen zur individuellen Risikominimierung – und das nicht als Einmalmaßnahme, sondern fortwährend.

Zentrales Cyberrisikomanagement mit Trend Micro

Cyberrisikomanagement bringt spezielle Herausforderungen mit sich: Risikolagen können sich buchstäblich über Nacht ändern, die Effektivität von Maßnahmen lässt sich erst im Ernstfall bestimmen und auch die Verhältnismäßigkeit ist schwer zu bewerten, solange Eintrittswahrscheinlichkeit und Schadensausmaß unbekannt sind. Risikobetrachtungen müssen außerdem kontinuierlich erfolgen und lassen sich nicht auf gelegentliche Schnappschüsse reduzieren.

Diese Anforderungen sind für Unternehmen mit herkömmlichen technischen Methoden und vorhandenem Personal kaum umzusetzen. Trend Micro, einer der weltweit führenden IT-Sicherheitshersteller, hat deshalb eine Lösung entwickelt, die alle Sicherheits-, Compliance- und Risikomanagementaufgaben moderner Unternehmen auf einer einzigen Software-Plattform vereint.

Alle Informationen sowie proaktive und reaktive Maßnahmen stehen zentral bereit, ohne zwischen verschiedenen Programmen hin und her wechseln zu müssen. Das spart Kosten im laufenden Betrieb und Zeit im Ernstfall. Trend Micro deckt den gesamten Lebenszyklus von Bedrohungen ab:

Vor dem Angriff:

Risiken erkennen, priorisieren und beheben.

Während des Angriffs:

Bedrohungen schneller aufspüren, Risiken eindämmen und gezielte Reaktionen einleiten.

Nach dem Angriff:

Normalbetrieb wiederherstellen und Folgeangriffen vorbeugen.

Angriffsoberfläche überwachen & Risiken gezielt eliminieren

Die Angriffsoberfläche ist die Summe aller Schwachstellen, Fehlkonfigurationen und blinden Flecken, die von Angreifern ausgenutzt werden können. Um die Angriffsoberfläche überwachen zu können, muss sie erfasst werden: Trend Micro identifiziert bekannte, versteckte und vergessene Assets (z.B. Computer, Benutzer und zugehörige Daten) und sammelt alles in einer zentralen Übersicht.

Auf Basis von gewichteten Faktoren wird für einzelne Assets ein individueller Risk Score errechnet, um die Frage zu beantworten: Wie wahrscheinlich ist ein erfolgreicher Angriff auf dieses Asset und wie schwer wären die Schäden? Unternehmen wissen also sofort, wo die größten Risiken lauern und welche Schwachstellen etc. priorisiert werden sollten. Der Detailgrad wird auf die Bedürfnisse von technischen Mitarbeitern und Geschäftsführung abgestimmt, sodass alle Verantwortlichen über fundierte Informationen verfügen.

Der prägnante Risk Score ist auch für das Gesamtunternehmen verfügbar, was anonymisierte Vergleiche mit anderen Unternehmen aus derselben Region bzw. Branche ermöglicht. Umgekehrt lässt sich der Wert als Zielvorgabe nutzen: So kann Trend Micro einen detaillierten Maßnahmenkatalog empfehlen, um einen bestimmten Risk Score zu erreichen und das Sicherheitsprofil effektiv zu verbessern.

Angriffe schneller identifizieren durch verknüpfte Daten

Trend Micro sammelt und verknüpft sicherheitsrelevante Daten aus dem gesamten Unternehmen, also zum Beispiel von Computern, Servern, Email-Systemen usw. Das geht weit über die Möglichkeiten von Punktlösungen hinaus, die sich immer nur auf bestimmte Bereiche konzentrieren.

Die gesammelten Daten fließen zu einem Data Lake zusammen, der mit weiteren Bedrohungsinformationen aus den weltweiten Trend Micro Forschungszentren angereichert und mittels künstlicher Intelligenz analysiert wird. In diesem Zusammenhang ist zu beachten, dass Trend Vision One das vom Bundesamt für Sicherheit in der Informationstechnik (BSI) entwickelte C5-Testat für datenschutzkonforme Cloud-Lösungen erhalten hat. Die Datenverarbeitung in der Cloud führt zu klaren Sicherheits- und Effizienzvorteilen:

- **Präzisere Alarme** reduzieren den Aufwand und ermöglichen gezielte Priorisierung.
- **Identifikation neuer Bedrohungen**, die von Punktlösungen nicht erkannt werden.
- **Schnellere Reaktionen** durch Bereitstellung von Kontextinformationen.

Der Data Lake kann zudem effizient nach Anzeichen für einen Angriff durchsucht werden, falls das BSI eine entsprechende Warnung ausgibt. Die schnelle Verarbeitung dieser Warnungen ist eine weitere Vorgabe von NIS2, die so auf elegante Weise abgedeckt werden kann.

Normalbetrieb wiederherstellen & vorbeugen

Die Trend Micro Lösung ermöglicht die Integration von externen Services, mit denen Trend Micro selbst oder Trend Micro Partner internen IT-Abteilungen bei der Bewältigung von Angriffen zur Seite stehen. Ein Beispiel ist der Incident Response Service, bei dem Trend Micro Experten innerhalb kurzer Zeit und in enger Zusammenarbeit mit der internen IT-Abteilung angepasste Aktionspläne entwickeln, sobald sie im Ernstfall kontaktiert werden. Trend Micro stellt das Personal und Werkzeuge bereit, um die Aktivitäten im Unternehmensnetzwerk zu beobachten. Gleichzeitig starten im Hintergrund bereits die Identifikation und Absicherung nicht betroffener Assets. Die Unterstützung interner Teams durch externe Experten ermöglicht eine schnellere Rückkehr zum Normalbetrieb:

- Stop laufender Angriffe und Identifikation der Ursachen.
- Schneller Start des Wiederaufbaus der Produktionsumgebung.
- Schutz nicht betroffener Assets.
- Angriffsvorbeugung durch Anpassung der Sicherheitsmaßnahmen.

Erfahren Sie hier mehr über proaktives Risikomanagement gemäß NIS2 und die Vorteile von Trend Micro. Bei Fragen zu XDR und der Überwachung von Angriffsoberflächen sprechen Sie uns jederzeit gerne an: Kontakt

Copyright © 2024 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.