IT-Sicherheit

Widerstandskraft stärken

[10.04.2024] Die EU-Richtlinie NIS2 soll die Cyber-Sicherheit in Europa erhöhen. Von den Vorgaben sind deutlich mehr KRITIS-Unternehmen betroffen als bislang. Kommune21 sprach mit Dirk Arendt von Trend Micro darüber, wie ein Cyber-Risiko-Management aussehen muss.

Herr Arendt, Deutschland arbeitet derzeit am Umsetzungsgesetz für die NIS2-Richtlinie. Können Sie den aktuellen Stand und die Herausforderungen bei der Umsetzung beschreiben?

Wir stehen derzeit vor der Herausforderung, dass das Umsetzungsgesetz möglicherweise nicht wie geplant noch dieses Jahr verkündet wird – hoffentlich aber noch in dieser Legislaturperiode. Dies bringt natürlich auch viele Unsicherheiten für Unternehmen mit sich, die sich auf die Umsetzung des Gesetzes vorbereiten wollen.

Was sind die Hauptziele der Richtlinie?

Sie soll die Widerstandsfähigkeit Kritischer Infrastrukturen stärken und das allgemeine Niveau der Cyber-Sicherheit in der EU erhöhen. Stellen Sie sich vor, Kritische Infrastrukturen – von Stromnetzen bis hin zu Krankenhäusern – würden durch Cyber-Angriffe lahmgelegt. Das hätte verheerende Folgen für unsere Gesellschaft und unsere Wirtschaft.

Wie unterscheidet sich die NIS2-Richtlinie von ihrem Vorgänger?

Zum einen sind nun deutlich mehr Unternehmen betroffen. Die Zahl der Sektoren steigt auf insgesamt 18. Sieben neue „Important Entities“ kommen hinzu und die Schwellenwerte werden gesenkt. Zum anderen führt NIS2 zusätzliche Maßnahmen und Anforderungen im Bereich der Cyber-Sicherheit ein. Ein zentraler Fokus liegt dabei auf der Sicherheit der Lieferkette, sodass Unternehmen nun auch für die Sicherheit ihrer Zulieferer verantwortlich sind. Zudem wird ein verpflichtendes Cyber-Risiko-Management eingeführt. Unternehmen müssen in der Lage sein, potenzielle Risiken zu identifizieren, zu bewerten und entsprechende Maßnahmen zur Risikominimierung zu ergreifen. Ein oft übersehener Aspekt und erster Schritt für Unternehmen ist die Selbstregistrierung. Während Unternehmen unter der vorherigen NIS-Richtlinie von den Behörden darüber informiert wurden, dass sie die entsprechenden regulatorischen Anforderungen erfüllen müssen, besteht unter NIS2 eine neue Verpflichtung zur Selbstregistrierung.

Wie bereiten sich Unternehmen, insbesondere in den neu hinzugekommenen Sektoren auf die Umsetzung der NIS2-Richtlinie vor?

Obwohl diese Sektoren als Kritische Infrastrukturen gelten, sind viele von ihnen von den neuen Anforderungen, insbesondere in den Landesgesetzen, ausgenommen. Die Länder haben noch nicht viel vorbereitet und warten teilweise auf den Bund. Hochschulen, Polizei und Landesbehörden stehen besonders im Fokus, da sie vermehrt erfolgreichen Angriffen ausgesetzt sind. In den Kommunen fehlen einheitliche Cyber-Sicherheitsstandards, viele wichtige Einrichtungen wie Feuerwehren und Schulen sind noch nicht eingebunden. In den Kommunen selbst ist wenig geregelt, obwohl hier der größte Teil der Verwaltung agiert. Geregelt sind kommunale Eigenbetriebe, die unter die KRITIS-Merkmale fallen. Einrichtungen als GmbH oder AöR wie Stadtwerke, Krankenhäuser, Entsorgungsunternehmen und

Wasserwerke fallen per Gesetz darunter. Aber: Feuerwehren, die Kommunalverwaltung als solche oder Ämter, Schulen und Betreuungseinrichtungen fallen derzeit nicht darunter.

„Die Richtlinie gibt einen klaren Fahrplan für Sicherheitsvorfälle und aktives Risiko-Management vor.“ Können Sie die Kernelemente der Richtlinie näher erläutern?

Die NIS2-Richtlinie gibt einen klaren Fahrplan für Sicherheitsvorfälle und aktives Risiko-Management vor. Sie fordert die Implementierung von Systemen zur Angriffserkennung und einen umfassenden Notfallplan. Da sich die Angriffsfläche und das Bedrohungsumfeld ständig verändern, ist ein kontinuierliches Cyber-Risiko-Management unerlässlich. Stellen Sie sich vor, zehn Landkreise in Deutschland würden gleichzeitig gehackt. Solche Angriffe legen Städte und Gemeinden, Universitäten, Krankenhäuser komplett lahm.

Wie unterstützt Trend Micro Unternehmen und Behörden bei der Vorbereitung auf die neuen Regelungen?

Um NIS2-konform zu werden, sind zwei Faktoren wichtig: ein detailliertes Cyber-Risiko-Management und die Reduzierung des Schadensausmaßes. Beides kann mit modernen Sicherheitstechnologien wie Angriffsflächen-Risiko-Management (ASRM) und Extended Detection and Response (XDR) erreicht werden. Die Integration von ASRM und XDR in eine einzige Cyber-Sicherheitsplattform wie Trend Vision One ermöglicht ein nahtloses Zusammenspiel der beiden Technologien. Innerhalb dieser Plattform werden sie zentral überwacht und gesteuert.

Macht die Richtlinie das Thema Cyber-Sicherheit zur Chefsache?

Die NIS-Richtlinie betont die persönliche Haftung von Führungskräften für Schäden, die aus der Vernachlässigung ihrer Pflichten beim Cyber-Risiko-Management entstehen. Das bedeutet, dass Führungskräfte nicht nur über Risiken sprechen dürfen – sie müssen auch handeln. Sie sind dafür verantwortlich, Risiken zu identifizieren, ihre Auswirkungen zu verstehen und geeignete Maßnahmen zur Risikominderung zu ergreifen. Darüber hinaus müssen wir die Bedeutung der Cyber-Sicherheit für Kritische Infrastrukturen, insbesondere auf kommunaler Ebene, stärker ins Bewusstsein rücken. Wenn beispielsweise das Finanzsystem einer Stadt ausfällt und Grundsteuern nicht eingezogen werden können, kann dies zu einem ernsthaften Problem führen, das sogar die Dienstleistungen von Unternehmen bedroht.

Wie können Unternehmen den neuen Anforderungen gerecht werden?

Artikel 21 der Richtlinie definiert die Mindestanforderungen an die Cyber-Sicherheit, die neben dem Cyber-Risiko-Management auch das Back-up Management, das Incident-Management, kryptografische Konzepte sowie Zugangskontrollen und Identitätsmanagement umfassen. Unternehmen, die bereits bewährte IT-Sicherheitspraktiken implementiert haben, dürften viele dieser Anforderungen bereits erfüllen.

()

Dieses Interview ist in der Ausgabe April 2024 von Kommune21 erschienen. Hier können Sie ein Exemplar bestellen oder die Zeitschrift abonnieren.

Stichwörter: IT-Sicherheit, NIS2, Trend Micro