



EU-RICHTLINIE NIS2

EU-Richtlinie NIS2: Open Source ist der Schlüssel zum Erfolg

Die EU macht Druck: Mit der NIS2-Richtlinie fallen deutlich mehr Unternehmen in den Bereich der kritischen Dienste, gleichzeitig steigen die Anforderungen an die Cybersicherheit. Unternehmen sollten sich jetzt auf die Umsetzung vorbereiten. Open Source Technologie kann dabei helfen, die Ziele in Sachen Cybersicherheit zu erreichen.

Cyberattacken und Betriebsunterbrechungen gehören zu den größten Geschäftsrisiken weltweit. Angesichts der steigenden Zahl an Angriffen hat die Europäische Union die gesetzlichen Anforderungen an die Cybersicherheit verschärft und im Dezember 2022 die NIS2-Richtlinie verabschiedet.

Dieses Regelwerk gilt für Unternehmen besonders kritischer Branchen und schreibt ihnen eine stringente Verteidigung gegen Cyberattacken vor. Das Management wird dabei explizit miteinbezogen.

Bis Oktober 2024 müssen die Mitgliedstaaten die Richtlinie in nationales Recht überführt haben. Auch wenn den Unternehmen dann noch etwas Zeit bleibt, sollten sie sich schon jetzt auf die Umsetzung vorbereiten, denn die Vorschriften sind umfangreich.

Ganzheitliche Sicherheit gefordert

Die erste Fassung der NIS-Richtlinie wurde 2016 auf den Weg gebracht. Damals war der Fokus stark auf die IT-Sicherheit gerichtet. Doch zwischenzeitlich haben sich die Rahmenbedingungen für die Cybersicherheit deutlich verändert. Mit der Digitalisierung wurden viele industrielle Systeme vernetzt, die bislang keine Verbindung zum Internet hatten und dafür auch gar nicht vorgesehen waren.

Durch die Vernetzung öffneten sich diese OT-Systeme und jetzt kommunizieren sie untereinander oder mit der Cloud. Jede Schnittstelle oder jede internetfähige Komponente wird damit zum potentiellen Einfallstor für Angreifer aus dem Netz.

Die EU hat in der NIS2 dieser Entwicklung Rechnung getragen und Vorschriften geschaffen, die das gesamte Unternehmen miteinbeziehen.

Cybersicherheit wird Chefsache

Mit einer Reihe von technischen Maßnahmen soll die Grundlage für mehr Cybersicherheit hergestellt werden. So fordert die NIS2 mindestens die Verschlüsselung von Daten und Informationen, ein Schwachstellenmanagement und eine konsequente Zugriffskontrolle.

Allerdings genügen diese Tools nicht aus, um ein angemessenes Sicherheitsniveau zu erreichen, denn auch die Angriffsmethoden werden zusehends raffinierter. Über den Chatbot ChatGPT beispielsweise lassen sich Texte verfassen, die sich kaum noch von denen unterscheiden, die ein Mensch geschrieben hat. Das macht es noch schwerer, Phishing-Mails zu erkennen, die ihre Leser zum Öffnen eines mit Schadsoftware infizierten Anhangs verleiten wollen.

Deshalb ist es wichtig, den Datenverkehr permanent zu überwachen, um den Normalzustand zu bestimmen. Sollte ein Angreifer die Firewall überwunden haben, so kann ein Intrusion Detection System (IDS) mögliche Unregelmäßigkeiten erkennen, beispielsweise einen höheren Datentransfer. Ein Intrusion Prevention System (IPS) kann dann den Angriff stoppen. Auch Deep Packet Inspection (DPI) gewinnt an Bedeutung. Dieses Tool analysiert Datenpakete, die über ein Netzwerk verschickt werden, und zwar bis in die Anwenderebene hinein, um Protokolle und Anwendungen zu erkennen und zu kategorisieren.

Neben den technischen Abwehrmechanismen werden eine ganze Reihe von organisatorischen Maßnahmen verpflichtend. Unternehmen sind aufgefordert, ein Risikomanagement zu etablieren, Notfallpläne aufzusetzen und ihre Mitarbeiter regelmäßig in Sachen IT-Sicherheit zu schulen. Damit kann das Management die Verantwortung für Cybersicherheit nicht mehr ausschließlich der IT-Abteilung zuweisen, sondern wird selbst in die Pflicht genommen.

Wichtig wird auch die Einbeziehung der Lieferketten, nachdem folgenschwere Angriffe über Zulieferer oder die Systeme anderer Unternehmen möglich sind. In diesem Zusammenhang werden Zertifizierungen für die Zuverlässigkeit von Systemen und Komponenten eine zentrale Rolle spielen, und die EU hat die Mitgliedsstaaten aufgefordert, passende Branchenstandards für die Zertifizierung festzulegen.

Welche Standards genau in Frage kommen, steht also noch nicht fest. In der Automation nutzen Entwickler von Komponenten sowie Integratoren bereits erfolgreich die IEC 62443. Diese Normenreihe für die Sicherheit industrieller Kommunikationsnetze hat demnach gute Chancen, sich in dem Bereich durchzusetzen und kann schon jetzt als Orientierung dienen.

Open Source Technologie klar im Vorteil

Nachdem deutlich mehr Unternehmen von der NIS2-Richtlinie betroffen sind, müssen sich viele zum ersten Mal mit den umfangreichen Vorschriften befassen und bestehende industrielle Anlagen nachrüsten. Da der Lebenszyklus bei OT-Systemen deutlich länger ist als in der IT, verfügen viele Betriebe über eine sehr heterogene Infrastruktur, die es zu vernetzen und jetzt auch abzusichern gilt.

IT-Sicherheitstools, die auf Open Source Technologie basieren, sind in dieser Situation klar im Vorteil. Wörtlich heißt es in der NIS2 Richtlinie: „Open-Source-Cybersicherheitswerkzeuge und -Anwendungen können zu einem höheren Maß an Offenheit beitragen und sich positiv auf die Effizienz industrieller Innovationen auswirken. Offene Standards erleichtern die Interoperabilität zwischen Sicherheitstools, was der Sicherheit der Interessenträger aus der Industrie zugute kommt.“

Open Source Technologie ermöglicht es, offene Kommunikationsstandards zu verwenden und bietet damit eine gute Lösung für die Vernetzung und Absicherung heterogener Infrastrukturen. Somit erhalten Unternehmen die notwendige Flexibilität und bleiben offen für zukünftige Innovationen, ohne sich von einzelnen Herstellern abhängig zu machen.

Weiter heißt es in der NIS2: „Maßnahmen zur Förderung der Einführung und nachhaltigen Nutzung von Open-Source-Cybersicherheitswerkzeugen sind besonders für kleine und mittlere Unternehmen wichtig, bei denen erhebliche Implementierungskosten anfallen, die durch die Reduzierung des Bedarfs an spezifischen Anwendungen oder Werkzeugen minimiert werden könnten.“

Viele Unternehmen haben im Rahmen der Digitalisierung bereits neue Hardware für die Vernetzung angeschafft. Diese jetzt aufgrund der NIS2 Sicherheitsvorschriften wieder komplett auszutauschen wäre eine große finanzielle Belastung. Auch hier kann Open Source Technologie helfen: Endian bietet beispielsweise ein IoT-Security-Gateway als Software-Version an. Mit diesem Endian 4i Software lässt sich jeder Industrie PC und jedes IoT-Gateway (x86) in eine komplette Sicherheitslösung verwandeln. Damit lässt sich vorhandene Hardware einfach weiternutzen.

Auch über die Cybersicherheit hinaus bietet Open Source Vorteile: Über Container-Technologie Docker lassen sich individuelle Unternehmensanwendungen nutzen oder die Anwendung von Drittanbietern integrieren. Damit können Geräte und Maschinen überwacht und deren Daten für die Optimierung der Prozesse analysiert werden.

Deutlich mehr betroffene Unternehmen

Nicht nur die Vorschriften werden mehr. Gegenüber der ursprünglichen Richtlinie erweitert sich auch die Zahl der Unternehmen, die in den Bereich kritischer Dienste fallen. Insgesamt umfasst die NIS2 Richtlinie 18 Sektoren und unterscheidet zwischen „Essential Entities“ und „Important Entities“. Eine komplette Liste findet sich hier.

Zu den grundlegenden Wirtschaftssektoren („Essential Entities“), gehören große Betreiber in den Bereichen Energie, Transport, Bankwesen, Finanzwesen, Gesundheit, Trinkwasser, Abwasser, Digitale Infrastruktur, ICT Service Management im B2B-Bereich, Raumfahrt sowie die öffentliche Verwaltung.

Die wichtigen Wirtschaftssektoren („Important Entities“) setzen sich aus sieben Bereichen zusammen, nämlich Post und Kurier, Abfall, Chemikalien, Lebensmittel, produzierende Industrie, digitale Dienste und Forschungsinstitute.

Neu ist auch die Größenregelung: So sind mittlere und große Unternehmen ab 50 Mitarbeitern oder 10 Millionen Euro Umsatz betroffen und zwar unabhängig von Leistung oder Schwellenwerten ihrer Anlagen. Bei manchen Betreibern spielt selbst die Unternehmensgröße keine Rolle mehr, wie bei Teilen der digitalen Infrastruktur oder der öffentlichen Verwaltung.

Fakt ist, dass die NIS2 deutlich mehr Unternehmen einschließt, als die derzeitigen NIS-Regeln. Schätzungen gehen von bis zu 40.000 zusätzlichen Unternehmen allein in Deutschland aus.

Strenge Sanktionen

Bei Verstößen gegen die Richtlinien sowie gegen die Meldevorschriften sind empfindliche Strafen vorgesehen. Bis zu 10 Millionen Euro oder 2 Prozent des weltweiten Umsatzes können fällig werden, wenn eine Organisation ihren Pflichten nicht nachkommt. Darin zeigt sich, dass die EU der Cybersicherheit zukünftig die gleiche Bedeutung beimisst wie dem Datenschutz.

Trotz der harten Strafen und der umfangreichen Pflichten stellt die NIS2 insgesamt einen Fortschritt dar. Denn nur, wenn alle Unternehmen Cybersicherheit ernst nehmen, lässt sich die Bedrohung zukünftig eindämmen. Und davon profitieren die Unternehmen letztlich selbst.