NIS2-Richtlinie

Schutz vor Cyber-Kriminellen

[12.02.2024] Um den Gefahren aus dem Cyber-Raum zu begegnen hat die EU die Richtlinie NIS2 erlassen. Die Vorgaben müssen bis Mitte Oktober 2024 umgesetzt werden. Der IT-Dienstleister Axians gibt Tipps, wie Kommunen und kommunale Unternehmen jetzt vorgehen sollten.

Eine Viertelmillion neu entdeckte Schadprogrammvarianten, 2.000 identifizierte Schwachstellen in Software-Produkten pro Monat, 21.000 neu infizierte Systeme pro Tag, 68 erfolgreiche Ransomware-Angriffe und zwei Angriffe pro Monat allein auf kommunale Einrichtungen oder kommunale Unternehmen. Der aktuelle Lagebericht Cyber-Sicherheit des Bundesamts für Sicherheit in der Informationstechnik (BSI) nennt alarmierende Zahlen: Das Amt warnt, dass die Kriminellen auf dem Vormarsch sind. Professionelle Cyber-Kriminelle sind heute stark vernetzt und gehen arbeitsteilig vor. Sie nutzen Künstliche Intelligenz (KI) und andere moderne Technologien für ihre Angriffe.

Vorgaben der NIS2-Richtlinie

Aufgrund dieser Bedingungen in der Cyber-Sicherheitslandschaft hat die EU die Richtlinie NIS2 erlassen. Die Anforderungen der Richtlinie werden derzeit in nationales Recht überführt und müssen bis zum 17. Oktober 2024 umgesetzt werden. Alle betroffenen Institutionen sind dann verpflichtet, eine Reihe von Cyber-Sicherheitsmaßnahmen zu ergreifen.
Die Unternehmen müssen unter anderem ein Risiko-Management-Konzept vorweisen, Notfallpläne erstellen und Sicherheitsvorfälle an das BSI melden. Vorgeschrieben sind technische Schutzmaßnahmen wie systematische Datensicherung, Zugriffskontrollkonzepte, Verschlüsselung und Schwachstellen-Management. Analog zum IT-Sicherheitsgesetz 2.0 schreibt NIS2 auch vor, dass Unternehmen die Schwachstellen ihrer Lieferkette in ihr Sicherheitskonzept einbeziehen müssen, damit Kriminelle nicht über Zulieferer in Systeme eindringen können. Es ist wichtig, den Stand der Technik umzusetzen, indem Sicherheitsstandards und Prozesse berücksichtigt werden, die bereits vor NIS2 als Best Practices empfohlen wurden.
Wer in den vergangenen Jahren darauf geachtet hat, seinen Betrieb nach den geltenden Standards gegen Kriminelle abzusichern, wird nur wenige Anpassungen vornehmen müssen, um den Anforderungen gerecht zu werden. Unternehmen und Institutionen, die neu in den NIS2-Bereich fallen und das Thema Cyber Security bisher stiefmütterlich behandelt haben, stehen nun aber vor großen Herausforderungen.

Fünf Schritte zu mehr Sicherheit

Um sich auf die Anforderungen vorzubereiten, sollten Unternehmen frühzeitig Schutzmaßnahmen ergreifen. Der Weg dorthin führt über fünf Schritte.
Zunächst sollten Unternehmen klären, ob sie zum erweiterten Kreis der NIS2-Regelung gehören. Es gibt zwei Hauptgruppen: Betreiber kritischer Anlagen und „besonders wichtige“ oder „bedeutende“ Anlagen. Entscheidend ist, ob diese Unternehmen in Wirtschaftsbereichen tätig sind, die der Regulierung unterliegen. Gerade hier herrscht noch viel Unsicherheit. Um Klarheit zu schaffen, sollten sich Unternehmen folgende Fragen stellen: Bin ich in einem der regulierten Sektoren tätig? Erreicht mein Geschäft die offiziellen Schwellenwerte? Ist der Umsatz hoch genug und stimmt die Anzahl der Mitarbeitenden? Können diese Fragen mit Ja beantwortet werden, gelten die Schutzbestimmungen der

NIS2. Es empfiehlt sich aber für alle Unternehmen – unabhängig davon, ob sie unter NIS2 fallen oder nicht – die eigenen Sicherheitskonzepte auf den Prüfstand zu stellen und zu klären, ob sie dem Stand der Technik entsprechen. Die IT-Verantwortlichen sollten auch nicht vergessen, die zu schützenden Unternehmensbereiche zu definieren.
Im nächsten Schritt gilt es herauszufinden, wo die größten Schwachstellen liegen. Wie ist die Cyber Security im Unternehmen aufgestellt? Wie hoch ist das aktuelle Schutzniveau? Eine Risikobewertung zeigt, wo die Sicherheitsstrategie am besten ansetzen sollte – nämlich dort, wo Unternehmen am schnellsten Verbesserungen erzielen können. Danach sollte der Prozess in regelmäßigen Abständen wiederholt werden. Eine kontinuierliche Bewertung kann dazu beitragen, die Resilienz der IT schrittweise zu erhöhen.

Schwachstellen in der Lieferkette

Bei der verpflichtenden Risikobewertung sollten nicht nur die eigenen Unternehmensrisiken eine Rolle spielen, sondern auch die spezifischen Schwachstellen in der Lieferkette berücksichtigt werden. Werden Schwachstellen identifiziert, müssen Gegenmaßnahmen ergriffen werden, um die regulatorischen Anforderungen zu erfüllen und die Schnittstellen zu schützen. Hierbei helfen beispielsweise External Attack Surface (EAS) Scans. Es empfiehlt sich, proaktiv zu handeln und eine Risikoanalyse durchzuführen, um mögliche Schwachstellen in der Lieferkette zu identifizieren. Anschließend können betroffene Einrichtungen mit ihren Zulieferern ein gemeinsames Sicherheitskonzept erarbeiten.
Um die geforderte Sicherheit der Informationssysteme zu gewährleisten, werden auch Angriffserkennungssysteme empfohlen. Für viele Unternehmen ist die Implementierung einer Security Information and Event Management (SIEM)-Lösung ratsam, da sie als Basis für die meisten Angriffserkennungssysteme gilt. Das SIEM sammelt Daten, die auch in einem Security Operations Center (SOC) ausgewertet werden können. Es liefert nützliche Informationen für den IT-Betrieb, zum Beispiel Hinweise auf Fehlkonfigurationen. Die Vielfalt der SIEM-Optionen bietet zahlreiche Möglichkeiten, um den unternehmensspezifischen Anforderungen gerecht zu werden. So können Unternehmen beispielsweise wählen, ob sie ein selbstverwaltetes SIEM-System oder die Dienste eines professionellen SOC in Anspruch nehmen möchten. Die Bandbreite der angebotenen Services reicht von einem Inhousebetrieb oder einem Co-Managed SIEM bis hin zu vollständig gemanagten IT/OT SOC-Services von externen ICT-Dienstleistern wie Axians.

Regeln und Prozesse etablieren

Es ist wichtig, nicht nur IT-Sicherheitssysteme aus Hard- und Software zu beschaffen. Vielmehr müssen Regeln und Prozesse etabliert werden, welche die Informationssicherheit kontinuierlich definieren, steuern, kontrollieren, aufrechterhalten und verbessern. Unternehmen können dabei nach dem Baukastenprinzip vorgehen: Zunächst sollten Maßnahmen ergriffen werden, die das Sicherheitsniveau schnell erhöhen. Danach kann der Schutz Schritt für Schritt ausgebaut werden. Sicherheitsstandards wie BSI-Grundschutz oder ISO 2700x sowie eine Zero-Trust-Architektur können als Orientierung dienen. Insbesondere die Orientierung am Grundschutzkompendium bietet eine große Hilfestellung, da es einen Best-Practice-Katalog von Sicherheitsmaßnahmen enthält.

Professionelle Beratung

Der Gesetzgeber hat den Ernst der Lage erkannt und mit neuen Regelungen die Anforderungen verschärft. Die wachsende Bedrohungslage zeigt, dass Unternehmen die Umsetzung direkt angehen sollten. Um sich nicht in technischen Detailentscheidungen zu verlieren, können sie auf die Unterstützung

erfahrener IT-Dienstleister wie Axians zurückgreifen. Diese implementieren bei ihren Kunden täglich Systeme, wie sie die NIS2-Verordnung vorschreibt. Professionelle Assessments, Beratung im Vorfeld und kontinuierliche Begleitung helfen, schnell eine geeignete Strategie zu entwickeln und entlasten die IT-Abteilungen der Kommunen und kommunalen Unternehmen.

()

BSI-Bericht: Die Lage der IT-Sicherheit in Deutschland 2023 (PDF; 2,5 MB)

Stichwörter: Informationstechnik, Cybersicherheit, IT-Sicherheit, NIS2-Richtlinie