Die Vorstellung einer Studie zum Thema **Cybersicherheit für IT-Netzwerke unter NIS-2**

Prof. Dr. Dennis-Kenji Kipker

Neue rechtliche Anforderungen an das unternehmerische Cybersecurity Management und ihre konkrete Ausgestaltung mit dem Schwerpunkt Risikomanagement

CYBER|INTELLIGENCE .Institute

Unterstützt durch

LANCOM SYSTEMS

01

Inhaltsverzeichnis

Summary | Einleitung

Die europäische NIS-2-Richtlinie, deren nationale Umsetzung in Deutschland voraussichtlich ab Oktober 2024 in Kraft tritt, bringt neue Anforderungen an das Cybersecurity-Management vieler Unternehmen mit sich. Die Richtlinie betrifft nicht nur neue Unternehmen, sondern enthält auch neue Vorgaben für das Management der Cybersicherheit. Die Erweiterung des Anwendungsbereichs von NIS-2 zielt darauf ab, Regelungslücken im Cyberschutz zu schließen und das europäische Cybersicherheitsniveau allgemein zu erhöhen.

Die NIS-2-Richtlinie ist ein technologieoffener Ansatz für effektive und nachhaltige Cybersicherheit. Es geht nicht nur darum, bestimmte Produkte oder Hersteller zu verwenden, sondern individuelle Maßnahmen auszuwählen, zu implementieren und aufeinander abzustimmen. Ein prozessbezogener Ansatz steht im Vordergrund, da Cybersicherheit als fortlaufender Prozess betrachtet wird.

Besonders wichtig ist der Schutz von IT-Netzwerken durch Technische und Organisatorische Maßnahmen (TOMs), da sie das Rückgrat jedes Unternehmens darstellen. Das Papier stellt drei wesentliche TOMs des Risikomanagements in den Vordergrund: Ausfallsicherheit, Zugriffskontrolle und Nachvollziehbarkeit.

Die gute Nachricht: Viele der umrissenen TOMs sind bereits heute mit moderner IT-Netzwerktechnik realisierbar. Moderne IT-Netzwerk-Komponenten sind dabei ein wichtiger Baustein, benötigen aber auch immer eine fundierte IT-Netzwerkplanung inklusive Rollen- und Rechtekonzepte, zuverlässiger Betriebskonzepte sowie definierter Prozesse im Angriffsfall mit eindeutigen Verantwortlichkeiten. NIS-2 fördert einen ganzheitlichen Ansatz der Cybersicherheit, so dass langjährig erfahrene Systemhaus-Partner eine optimale individuelle Lösung für Unternehmen und Institutionen entwickeln können.

NIS-2 bietet den Impuls, sich mehr um IT-Sicherheit zu kümmern und die sicherlich schon bestehenden organisatorischen und technischen Maßnahmen weiter zu entwickeln. Das Ziel von mehr Cybersicherheit ist alternativlos und ein Aufschub einer fundierten Überprüfung sowie Modernisierung ist in jedem Fall fahrlässig. Wer dabei auf europäische Player setzt, fördert direkt die digitale Souveränität und inkludiert bereits Vorteile einer DSGVO-Konformität und Backdoor-Sicherheit.

03 Überblick

Mit der nationalen Umsetzung in Deutschland voraussichtlich im Oktober 2024 bringt die europäische NIS-2-Richtlinie (Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148) neue Anforderungen an das Cybersecurity Management einer Vielzahl von Unternehmen mit sich. Der EU-Rechtsakt, welcher die Vorgängerregelung aus dem Jahr 2016 ablöst, wird in Deutschland durch das „Gesetz zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung“ (NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz – NIS2UmsuG) umgesetzt und betrifft nicht nur zahlreiche neue Unternehmen, sondern enthält auch neue und zusätzliche Vorgaben an das Management von Cybersicherheit.

Die Studie soll einerseits einen Überblick über die neuen regulatorischen Vorgaben geben und andererseits Informationen im Hinblick auf ihre Umsetzung unter besonderer Berücksichtigung des Produktportfolios des Herstellers LANCOM bereitstellen.

NIS-2 betrifft nicht nur KRITIS, sondern auch KMU

Mit der Ausdehnung des Anwendungsbereichs von NIS-2 gegenüber der Vorgängerregelung NIS-1 will der europäische Gesetzgeber zum einen Regelungslücken im Cyberschutz schließen, zum anderen das europäische Cybersicherheitsniveau deutlich stärker als bislang vereinheitlichen. Deshalb wird der Anwendungsbereich von NIS-2 nicht nur qualitativ im Sinne zusätzlicher betroffener Sektoren und Branchen ausgedehnt, sondern auch quantitativ, indem der Schwellenwert für betroffene Unternehmen abgesenkt wird. Hierbei wird Bezug genommen auf die Empfehlung 2003/361/EG. Betroffen sind zahlenmäßig demgemäß grundsätzlich Unternehmen, die gemäß dieser Empfehlung als mittlere Unternehmen gelten oder die Schwellenwerte für mittlere Unternehmen überschreiten. Betroffen von NIS-2 können darüber hinaus auch Unternehmen unabhängig von ihrer Größe sein, soweit sie durch den Rechtsakt vorgegebene qualifizierende Anforderungen erfüllen. Dazu gehören kann beispielsweise eine besondere Kritikalität der erbrachten Leistung dergestalt, dass sie für die Aufrechterhaltung kritischer gesellschaftlicher oder wirtschaftlicher Tätigkeiten unerlässlich ist. Ebenfalls genannt werden wesentliche Systemrisiken infolge der Störung eines erbrachten Dienstes.

NIS-2 erweitert und ergänzt die bestehenden Vorgaben zum Cybersecurity Risikomanagement

Die unternehmerische Governance von Cybersicherheit nimmt in NIS-2 eine deutlich stärkere Rolle als in NIS-1 ein. Dabei gilt jedoch nach wie vor: Cybersecurity Prävention sollte im Mittelpunkt aller unternehmerischen Bemühungen für mehr digitale Resilienz stehen. Deshalb verpflichtet NIS-2 die betroffenen Unternehmen, geeignete und verhältnismäßige technische, operative und organisatorische Maßnahmen zu ergreifen, um die Cybersicherheitsrisiken zu minimieren.

Wenn Sie das ganze Dokument lesen möchten, dann können Sie das komplette techconsult PDF kostenlos über unser Kontaktformular erhalten.

LANCOM SYSTEMS