Muss IT-Sicherheit überhaupt reguliert werden?

Sven Hillebrecht vom IT-Unternehmen Adlon spricht über Hintergründe der NIS-Regulierung.

AdobeStock/butenkow

Das NIS-2-Umsetzungsgesetz wurde im Juli 2024 im Kabinett beschlossen, aber nicht verabschiedet. Grund dafür war die neue Bundestagswahl. Nun kann das Gesetz verabschiedet werden. Und das ist in Zeiten steigender Security-Vorfälle und hoher finanzieller Risiken im Sinne aller verantwortungsvollen Unternehmer. Oder?

Das europäische Parlament hat mit NIS-2 beschlossen, weitere Unternehmen in Sachen IT-Sicherheit in die Pflicht zu nehmen. Die Richtlinie enthält Vorgaben zu Sicherheitsmaßnahmen eingesetzter Informationstechnik. Sie zielt auf die Erhöhung unserer Cyber-Resilienz ab. Alle EU-Mitgliedsstaaten müssen die Richtlinie in nationales Recht umsetzen. Anschließend wird streng kontrolliert. Strafen folgen stante pede.

Hohe Abhängigkeiten und Intransparenz

ist Grund 1 für die Regulierung. Unternehmen, die zum KRITIS-Sektor zählen, haben oftmals eine Monopolstellung inne. Beispielsweise bei Grundversorgern wie Krankenhäusern oder Wasseranbietern. Deren Kunden haben keine Möglichkeit zu einem Anbieter mit höheren Sicherheitsstandards zum Beispiel für ihre Gesundheitsdaten zu wechseln.

Zudem existiert keinerlei Transparenz zu den IT-Sicherheitsmaßnahmen der Unternehmen. Wäre selbstredend ein zweischneidiges Schwert. Es ist für Kunden nicht nachvollziehbar, wie es um die Sicherheit der Daten bestellt ist. Der Gesetzgeber hat in beiden Fällen ein berechtigtes Interesse, IT-Sicherheitsstandards zum Schutz der Bevölkerung und Infrastruktur zu etablieren. Daher wurde in der ersten Phase der Standard beim KRITIS-Sektor erhöht. Mit NIS-2 werden weitere Unternehmen in die Pflicht genommen.

NIS-2 in Kürze

Die aktualisierte EU-Richtlinie fördert die Cybersicherheit in den Mitgliedsstaaten. Sie führt strengere Sicherheitsmaßnahmen ein und dehnt den Geltungsbereich auf weitere Sektoren aus.

Die Einhaltung der NIS-2 ist entscheidend für den Schutz vor Cyber-Bedrohungen, die Gewährleistung der Rechtskonformität und die Aufrechterhaltung der betrieblichen Widerstandsfähigkeit. NIS-2 fügt sich nahtlos in bestehende Sicherheits- und Compliance-Programme wie der DSGVO ein.

Fehlende Sicherheitsstandards trotz steigender Vorfälle und Angriffe

ist Grund 2 für die Regulierung. Obwohl man allerorts von Security-Vorfällen und Angriffen hört, zögern viele Unternehmen noch, ihre Cyber-Resilienz zu erhöhen. Umfragen wie der aktuelle BSI-Report 24 führen als Gründe mangelnde Ressourcen und fehlendes Knowhow der Unternehmen an. Unterschätzt bleibt wie so oft die strategische Ausrichtung des Outsourcings mittels Managed Security Services wie z. B. Managed XDR. Entgegen der Annahme, dass dies zur Abhängigkeit vom Dienstleister führt, schafft dieser Schachzug maximale Transparenz und klare Prozesse. Es entsteht mehr Freiraum für die eigene Wertschöpfung und gleichzeitig sinken Ressourcenmangel und Kostendruck.

Neue Sektoren der NIS-2 Umsetzung

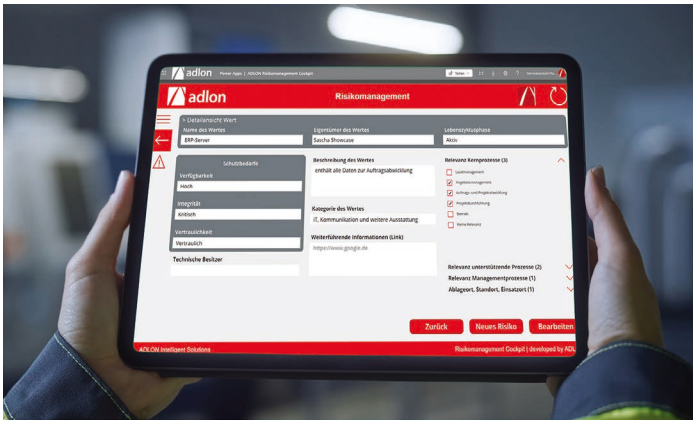
Für die Infrastruktur besonders relevante Sektoren, wie Energie, Bankwesen, Verkehr/Transport, Lebensmittel oder Gesundheitswesen (KRITIS) waren bereits in der vorherigen NIS-Direktive enthalten. Die NIS-2 fordert nun Unternehmen der folgenden Sektoren zur Umsetzung höhere Sicherheitsmaßnahmen auf:

- Trinkwasser und Abwasser
- Verwaltung von IKT-Diensten (B2B)
- Öffentliche Verwaltung
- Weltraum
- Post- und Kurierdienste
- Verarbeitendes Gewerbe / Herstellung von Waren
- Anbieter digitaler Dienste
- Forschung

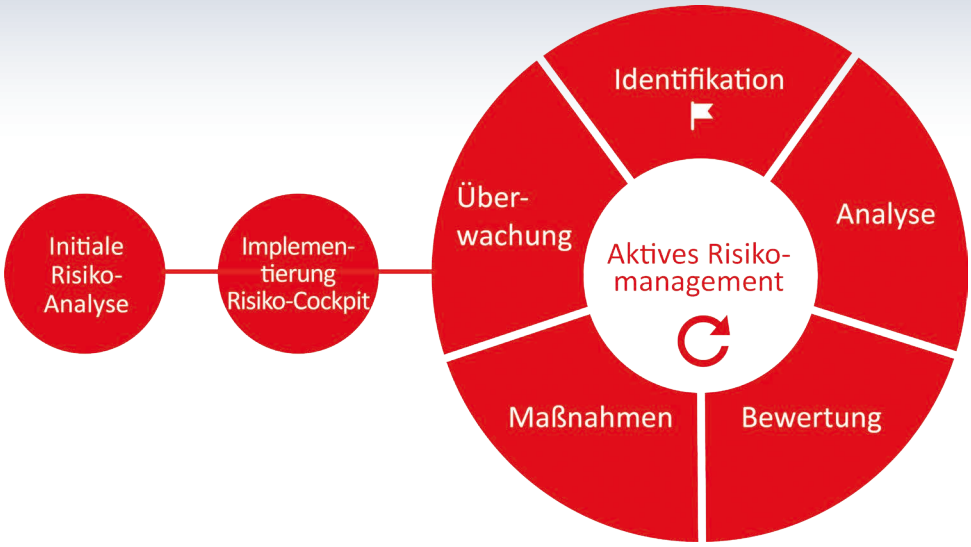
Als Schwellenwert in puncto Unternehmensgröße gilt eine Beschäftigtenzahl von mehr als 50 Mitarbeitern oder ein Jahresumsatz von mehr als 10 Millionen Euro. Insgesamt betrifft NIS-2 mehr als 50.000 Unternehmen in Deutschland.

Sven Hillebrecht lizenziert für Adlon, Quelle: Adlon

Autor:
Sven Hillebrecht
General Manager
Adlon Intelligent Solutions GmbH
www. adlon.de



Risikomanagement-App © AdobeStock/Gorodenkoff



Das Prinzip des aktiven Risikomanagement

Ein Termin schafft Tatsachen für zeitnahes Handeln

ist Grund 3 für die Regulierung. Mit dem Stichtag im Oktober 2024 hat das Bundesministerium einen Handlungszeitraum definiert, der bei den meisten Unternehmen eines ausgelöst hat: nichts. Von Aussitzen oder Verschiebung des Termins war die Rede. Alles Mutmaßungen hofften Sicherheitsbeauftragte, die den Mehrwert hinter dem Gesetz sahen. Und doch: eine bittere Wahrheit! Denn zum Stand der Veröffentlichung dieses Artikels ist das Gesetz in Deutschland noch nicht bestätigt worden. Wir wissen nicht, wann dies geschieht. Wir wissen nur: es kommt. Unternehmen können sich jetzt noch gezielt vorbereiten und Maßnahmen nachhaltig und ohne Zeitdruck etablieren.

Folgen bei Nichteinhaltung

Mögliche Vorfälle können zu technischen Ausfällen, finanziellen Verlusten und einem geschädigten Ruf führen. Und: die Verantwortlichen können auch persönlich haftbar gemacht werden.

- Geldbußen von bis zu 10 Millionen Euro oder 2 % des weltweiten Jahresumsatzes.
- Erzwungene zusätzliche Maßnahmen der Behörden
- Persönliche Haftung der Geschäftsführung

Regularien können kontrolliert werden

ist Grund 4 für die Regulierung. In der IT-Sicherheit gilt das Prinzip der Angemessenheit. Sicherheit soll nicht wegen eines Gesetzes erhöht werden, sondern im Verhältnis ihrer Auswirkungen bei einer Störung und deren Folgen. Die Risiko-Vermeidung soll aber auch nicht dem Zufall überlassen bleiben. Mit dem risikoorientierten Ansatz können KRITIS Unternehmen und mit NIS-2 auch weitere Sektoren auf die definierten Standards kontrolliert werden. Die Überprüfbarkeit scheint schwer realisierbar zu sein, da. Da die konkrete Ausgestaltung der Sicherheitsmaßnahmen stark individuell ist. Überprüft werden kann somit weniger der „Erfolg" der Maßnahme, sondern die Maßnahme selbst, die kontinuierliche Überwachung, Dokumentation und Prozessentwicklung.

Standards schaffen keine hundertprozentige Sicherheit, aber eine Grundlage

Mit NIS-2 sind Unternehmen aufgefordert, folgende Sicherheitsmaßnahmen einzuführen und nachzuweisen:

1. **Incident Management:** Monitoring, Bewertung, Reaktion & Behebung von Sicherheitsvorfällen
2. **Business Continuity Management (BCM):** Backup-Management, Wiederherstellung & Krisenmanagement
3. **Risikomanagement:** Insbesondere rund um Cybersicherheit, Sicherheit der Informationssysteme und Sicherheit in der Lieferkette
4. **Kryptografie und Verschlüsselung:** Verfahren für den Einsatz von Kryptografie und Verschlüsselung
5. **Authentifizierung:** Multi-Faktor-Authentifizierung oder kontinuierliche Authentifizierung
6. **„Cyberhygiene":** z. B. regelmäßige Updates, Mitarbeiter-Schulungen zur Cybersicherheit
7. **Meldesystem:** Bei erheblichen Sicherheitsvorfällen sind Unternehmen verpflichtet, innerhalb von 24 Stunden ab Kenntnis eine Frühwarnung an das BSI (Bundesamt für Sicherheit in der Informationstechnik) zu leisten. Innerhalb von 72 Stunden ist ein ausführlicher Bericht mit Bewertung einzureichen und nach einem Monat ein Abschlussbericht inklusive Maßnahmen.

Risikomanagement

Unter Risikomanagement versteht man allgemeinhin den Prozess der kontinuierlichen Identifikation, Analyse, Bewertung und Behandlung von Risiken. Kurzum: Die Augen und Ohren offen zu halten und möglichen Vorfällen vorzubeugen. Daher stellt Risikomanagement in NIS-2 eine wichtige Maßnahme dar.

Damit der Umgang mit Risiken nicht zufällig und planlos geschieht, unterstützt methodisch ein Risikomanagement-System, das die schutzbedürftigen Werte des Unternehmens benennt und dessen Risiken samt Eintrittswahrscheinlichkeit und Auswirkungsgrad transparent aufzeigt. So werden die Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit sichergestellt. Dazu reicht Excel und noch besser: ein smartes Tool.

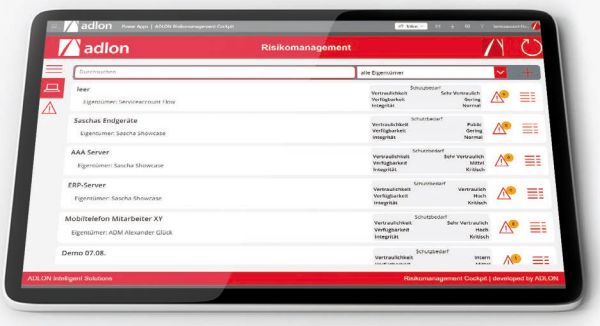
Aktives Risikomanagement stellt somit eine Entscheidungsgrundlage für ein effizientes Handeln dar. IT-Verantwortliche erhalten eine Priorisierung der potenziellen Gefahrenquellen für ihre Infrastruktur und somit proaktiven Handlungsspielraum.

Fazit

In einer perfekten Welt ginge es auch ohne Regularien, hier und jetzt hilft es aber! Uns allen ist an der Verbesserung der IT-Sicherheit gelegen, daher können grundlegende Sicherheitsmaßnahmen - wie in NIS-2 vorgegeben - auf lange Sicht nur förderlich sein. Ärgern sollte sich keiner, da ein Zögern und die Leichtsinnigkeit vieler Unternehmen größere Folgen hat. Ja, es scheint, wir brauchen Regularien, denn das Ziel ist klar. Die Methode bewährt. Ein allzu schneller Effekt darf durch regulatorische Maßnahmen jedoch nicht erwartet werden. Es obliegt noch immer verantwortungsvollem Unternehmertum, keine Türen im Unternehmen offen stehen zu lassen.

Wer schreibt:

Adlon Intelligent Solutions erhöht die Produktivität, Flexibilität und Innovationskraft seiner Kunden durch maßgeschneiderte IT-Lösungen. So entstehen Wettbewerbsvorteile, die Unternehmen brauchen, um in schnellen, datengetriebenen Märkten noch besser wirtschaften und nachhaltig wachsen zu können. ◄



Risikomanagement-App