Whitepaper zur Umsetzung der NIS-2-Richtlinie

Ein Leitfaden für Unternehmen, Geschäftsleiter und Rechtsabteilungen

Connecting your world.

Einleitung

Die Zahl der Cyberangriffe auf Unternehmen in Deutschland steigt seit Jahren unaufhörlich an. Nach aktuellen Umfragen unter Unternehmensführern steht die Sorge davor, Opfer von Cyberattacken auf das eigene IT-System zu werden oder von Hacks auf die eingesetzten IT-Dienstleister betroffen zu sein, an oberster Stelle der befürchteten Risiken für den Bestand ihrer Unternehmen[1]. In den Fokus der Cyberkriminellen geraten dabei zunehmend auch weniger prominente und mittelständische Unternehmen. Den betroffenen Unternehmen können aus solchen Attacken empfindliche Umsatzverluste und Schäden im Umgang mit ihren Kunden entstehen. Neben dem individuellen Interesse der Unternehmer bedrohen die Cyberangriffe aber auch das öffentliche Interesse an einem funktionierenden Gemeinwesen, wenn wichtige Lieferketten oder die Produktion von Gütern gestört werden.

Der steigenden Gefahr tritt deshalb nun auch der Gesetzgeber entgegen. Im Januar 2023 ist eine neue Richtlinie der EU über Netz- und Informationssysteme in Kraft getreten, die NIS-2-Richtlinie. Die Vorgaben dieser europäischen Richtlinie müssen bis zum 17. Oktober 2024 in deutsches Recht umgesetzt werden. Hierzu liegen bereits ein umfassender Referentenentwurf für das „NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz“ (NIS-2-UmsuCG) und ein Diskussionspapier des Bundesinnenministeriums vor[2]. Ab dem 18. Oktober 2024 werden die neuen Compliance-Regelungen dann unmittelbare Anwendung finden – entweder in Form des Umsetzungsgesetzes oder, falls ein solches nicht vorliegt, in Form der unmittelbaren Anwendung der Richtlinie. Unternehmen und die Geschäftsleitung müssen dann vorbereitet sein.

Denn gegenüber der bisherigen Rechtslage werden sich die Pflichten und der Kreis der verpflichteten Unternehmen erheblich ausweiten und verschärfen. Im Falle eines Verstoßes gegen die neuen Compliance-Vorgaben drohen empfindliche Bußgelder in Millionenhöhe. Besonders wachsam müssen Geschäftsführer und Vorstände der betroffenen Unternehmen sein. Sie werden persönlich in die Pflicht und Haftung genommen. Auf der anderen Seite kann die Umsetzung der NIS-2 Vorgaben auch positive Effekte wie ein gesteigertes Kunden- oder Investorenvertrauen mit sich bringen. Insofern sollten Sie NIS-2 auch als Chance für Ihr Unternehmen ansehen.

In diesem Whitepaper erfahren Sie, ob Ihr Unternehmen nach dem aktuellen Stand der Gesetzesentwürfe von NIS-2 betroffen ist und was dies für Sie und Ihr Unternehmen bedeutet.

[1] Eine Umfrage aus dem Jahr 2023 ergab, dass rund 58 Prozent der befragten Unternehmen in Deutschland mindestens einmal Opfer einer Cyber-Attacke geworden waren.
https://de.statista.com/statistik/daten/studie/1230157/umfrage/unternehmen-die-in-den-letzten-12-monaten-eine-cyber-attacke-erlebt-haben/#statisticContainer.

[2] Ein formaler Gesetzesentwurf oder ein verabschiedetes Gesetz liegen zum Redaktionsschluss dieses Papiers nicht vor. Das Papier beruht daher auf den bis Februar 2024 öffentlich verfügbaren Gesetzentwürfen.

Ist mein Unternehmen betroffen?

In einem ersten Schritt sollten Sie sich einen Eindruck darüber verschaffen, ob Ihr Unternehmen möglicherweise von NIS-2 betroffen ist und wenn ja, in welcher Kategorie.

Der aktuelle Umsetzungsentwurf stellt – entsprechend den Vorgaben der Richtlinie – im Wesentlichen **zwei Kategorien** von Einrichtungen auf, für die jeweils eigene Cyberschutzpflichten gelten. Das sind zum einen die **besonders wichtigen Einrichtungen** und zum anderen die **wichtigen Einrichtungen**.

Spezielle zusätzliche Pflichten gelten für Betreiber von **kritischen Anlagen**, die eine Unterkategorie der *besonders wichtigen Einrichtungen* darstellen. *Kritische Anlagen* sind Anlagen, die von hoher Bedeutung für das Funktionieren des Gemeinwesens sind, weil im Falle ihrer Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit eintreten würden. Die *kritischen Anlagen* im Sinne der NIS-2-Regelung decken sich weitestgehend mit den bisherigen „kritischen Infrastrukturen“ nach den bereits seit langem geltenden KRITIS-Verordnungen[3].

Sonderregelungen gelten auch für TLD-Name-Registries und DNS-Diensteanbieter, für Betreiber öffentlicher Telekommunikationsnetzwerke und für Erbringer von öffentlichen Telekommunikationsdiensten, sowie für die Betreiber bestimmter Energieanlagen nach dem Energiewirtschaftsgesetz (EnWG).

Besonders wichtige Einrichtungen

Unterfällt Ihr Unternehmen einem der folgenden Sektoren, stellt es **per se** eine *besonders wichtige* Einrichtung dar, und zwar unabhängig davon, ob es seine Dienste entgeltlich oder unentgeltlich erbringt:

- Betreiber einer Anlage aus dem Sektor Öffentliche Verwaltung – Zentralregierung;
- Betreiber kritischer Anlagen;
- Qualifizierte Vertrauensdiensteanbieter[4];
- Top Level Domain Name Registries,
- DNS-Diensteanbieter.

Besonders geregelt sind auch **Anbieter von Telekommunikationsdiensten[5] und öffentlich zugänglichen Telekommunikationsnetzwerken**. Solche Anbieter unterfallen den *besonders wichtigen Einrichtungen*, wenn sie 50 oder mehr Mitarbeiter beschäftigen oder einen Jahresumsatz plus eine Jahresbilanzsumme von jeweils über EUR 10 Millionen aufweisen. Auf Entgeltlichkeit kommt es auch in diesem Bereich nicht an.

Für **alle bisher noch nicht genannten Unternehmen** kommt es für die Frage, ob sie der Kategorie der *besonders wichtigen Einrichtungen* unterliegen, einerseits auf die **Größe** des Unternehmens und z**usätzlich** auf die Zugehörigkeit zu einem bestimmten **Sektor** an. Nur wenn **beide Voraussetzungen zugleich** erfüllt sind, ist Ihr Unternehmen von NIS-2 als *besonders wichtige Einrichtung* erfasst. Im Gegensatz zu den oben genannten Sonderbereichen sind hier außerdem nur Unternehmen erfasst, die ihre Waren oder Dienstleistungen **gegen Entgelt** anbieten.

[3] Das betrifft vor allem die Sektoren Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung, Finanz- und Versicherungswesen sowie Siedlungsabfallentsorgung. Die KRITIS-Regelungen aus dem BSIG und der KRITIS-Rechtsverordnung gelten parallel weiter, werden aber im Zuge der Umsetzung einer anderen EU-Richtlinie (CER) ebenfalls überarbeitet. Der Begriff der kritischen Anlage wird dabei den der kritischen Infrastrukturen ersetzen, der sich in den neuen Gesetzesentwürfen nicht mehr wiederfindet.

[4] Zu den sog. Vertrauensdiensten zählen elektronische Dienste zur Erstellung, Überprüfung, Bewahrung und Validierung von elektronischen Signaturen oder ähnlichen Zertifizierungen. „Qualifiziert“ sind derartige Vertrauensdienste, wenn sie die speziellen Vorgaben der europäischen „eIDAS-Verordnung“ (electronic Identification, Authentication and Trust Service-Verordnung) erfüllen.

[5] Gemeint sind neben Diensten, die den Zugang zum Internet ermöglichen, v.a. Dienste, die eine Kommunikation im Verhältnis Mensch-Mensch oder Maschine-Maschine bezwecken (z.B.: Email- oder Chatprogramme). Nicht umfasst sind Dienste, bei denen die interpersonelle Kommunikation nur eine untergeordnete Nebenfunktion darstellt (nicht daher z.B. Onlineshops mit Chatfunktion).