IT-Sicherheitsrecht in Kanzleien, Unternehmen und der öffentlichen Hand – was muss ich 2025 beachten?

Rechtsanwältin Dr. Judith Nink beschäftigt sich seit 20 Jahren mit Datenschutz-, Sicherheits- und IT-Themen. Sie leitet ab Juni 2025 den Fachbereich Cybersicherheit bei Unternehmen im Bundesamt für Sicherheit in der Informationstechnik (BSI).

IT- und Cybersicherheit sind zu einem Top-Management-Thema geworden. Sicherheitsrisiken bedrohen Unternehmen und öffentliche Institutionen. Neue rechtliche Verpflichtungen und technologische Fortschritte im Bereich der IT-Sicherheit stellen Kanzleien, Unternehmen und die öffentliche Hand vor Herausforderungen.

Cybersicherheitsstrategie der EU

Die EU-Cybersicherheitsstrategie von 2020 zielt darauf ab, die Resilienz gegen Cyberbedrohungen zu stärken. Die EU-Kommission hat Gesetzesinitiativen wie die NIS-2-Richtlinie ((EU) 2022/2555), die CER-Richtlinie ((EU) 2022/2557), DORA ((EU) 2022/2554), den Cyber Resilience Act ((EU) 2024/2847), den AI Act ((EU) 2024/1689), den Cyber Solidarity Act ((EU) 2025/38) sowie den Cybersecurity Act ((EU) 2019/881) auf den Weg gebracht.

Stand der Umsetzung der NIS-2- und der CER-Richtlinie

Die NIS-2- und CER-Richtlinien zielen darauf ab, wichtige und kritische Einrichtungen gegen Cyberangriffe reaktionsfähig zu machen. Die Umsetzungsfrist war der 17.10.2024. Deutschland hat die Richtlinien noch nicht umgesetzt, Vertragsverletzungsverfahren laufen (Pressemitteilungen vom 28.11. 2024 u. vom 7.5.2025). Betroffene Einrichtungen sollten sich vorbereiten.

Betroffenheitsprüfung

In einem ersten Schritt sollten Kanzleien, Unternehmen und die öffentliche Hand (nachfolgend »Einrichtungen«) prüfen, ob sie von dem Anwendungsbereich einer der Richtlinien und/oder Verordnungen betroffen sind. Entlang der Wertschöpfungskette bei Hochrisiko-KI-Systemen ist auch das »Anbieter-Upgrade« nach Art. 25 AI Act zu beachten.

> Im Fokus der Strategie steht der Aufbau und die Stärkung der Resilienz von Infrastruktur, Produkten, Dienstleistungen und Lieferketten.

CER-Richtlinie: Einrichtungen, die wesentliche Dienste erbringen, in Deutschland tätig sind und deren Ausfall erhebliche Störungen verursachen würde, fallen unter die Richtlinie. Wesentliche Dienste sind solche, die für die Aufrechterhaltung wichtiger gesellschaftlicher Funktionen wesentlich sind. Die Einstufung als Kritische Infrastruktur (KRITIS) ist maßgeblich für die Klassifizierung als Sicherheitsvorfall und hat langfristige Auswirkungen. Das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) bietet eine aktuelle Übersicht über die entsprechenden KRITIS Sektoren.

NIS-2-Richtlinie: Die Betroffenheit einer Einrichtung von der NIS-2-Richtlinie ist anhand der Art. 2 und 3 der NIS-2-Richtlinie zu prüfen. Die Richtlinie macht Vorgaben, die die Mitgliedstaaten bei der Umsetzung nicht unterschreiten dürfen (auch wenn der deutsche Gesetzgeber eine solche unzulässige Einschränkung des Anwendungsbereichs in § 28 Abs. 3 Nr. 1 BSIG-Entwurf, BT-Dr. 20/13184, für die Berechnung der Schwellenwerte vorgenommen hatte). Lediglich bei Einrichtungen der öffentlichen Verwaltung auf lokaler Ebene sowie bei Bildungseinrichtungen, insbesondere wenn sie kritische Forschungstätigkeiten durchführen, liegt es im Ermessen der Mitgliedstaaten, ob diese von der Regulierung erfasst werden sollen.

Die Bestimmung des Anwendungsbereichs ist jedoch deutlich komplexer als bei der CER-Richtlinie.
Es empfiehlt sich, für die initiale grobe Prüfung auf ein Tool zurückzugreifen. Das BSI bietet bspw. den Betroffenheitscheck, mit dem Einrichtungen einen Hinweis bekommen können, ob sie unter den Anwendungsbereich fallen.

Verantwortung und Schulung
Nach allen Gesetzen sind angemessene Schulungsmaßnahmen erforderlich, insbesondere zur Sensibilisierung für die IKT/IT-Sicherheit. Diese Schulungen richten sich an das Personal und, gemäß der NIS-2-Richtlinie und DORA, auch an Leitungsorgane. Letztere tragen die Verantwortung für die Implementierung von Risikomanagement-Maßnahmen.
Cybersicherheit wird somit zu einer Führungsaufgabe. Im Bereich des AI Acts ist es unerlässlich, dass Nutzer:innen KI-Kompetenz vermittelt wird.

Betroffene Einrichtungen sind daher angehalten, entsprechende Schulungspläne, -inhalte und -konzepte auszuarbeiten oder auf externe Angebote zurückzugreifen, diese zu implementieren und regelmäßig auf ihre Effizienz zu überprüfen. Ein besonderes Augenmerk ist auf die Schulung der Leitungsorgane zu legen, damit diese eine ausreichende Cybersicherheitskompetenz erlangen, um ihrer Verantwortlichkeit gerecht zu werden.

Meldepflichten bei Sicherheitsvorfällen / Schwachstellen
Die NIS-2-, CER-Richtlinie, DORA, der Cyber Resilience Act sowie der AI Act sehen Meldepflichten bei Sicherheitsvorfällen und Schwachstellen vor. Einrichtungen sollten Prozesse und Alarmierungssysteme einrichten und Personal schulen.

> „Betroffene Organisationen müssen für die sichere Entwicklung digitaler Inhalte sorgen.

Registrierungspflichten
Gemäß der NIS-2- und der CER-Richtlinie sowie DORA sind betroffene Einrichtungen dazu verpflichtet, sich bei der zuständigen Aufsichtsbehörde zu registrieren. Da die Registrierung die Einrichtung eines entsprechenden Systems voraussetzt, ist dies zunächst nur für unter den Anwendungsbereich von DORA fallende Einrichtungen relevant.

Risikomanagementmaßnahmen
Einrichtungen im Anwendungsbereich der NIS-2-Richtlinie müssen technische, operative und organisatorische Maßnahmen ergreifen, um Risiken zu beherrschen und Auswirkungen von Sicherheitsvorfällen zu minimieren (Art. 21 NIS-2-Richtlinie). Einrichtungen sollten ihre IT-Sicherheitsmaßnahmen überprüfen. Der CyberRisikoCheck des BSI und/oder externe Berater:innen können unterstützen.
DORA ergänzt Branchen-Pflichten im Finanz- und Versicherungssektor, insbesondere um Risikomanagementpflichten und Sicherungspflichten entlang der Lieferkette.

Cybersicherheit bei Produkten
Der Cyber Resilience Act gilt für Produkte mit digitalen Elementen. Herstellende Unternehmen müssen Cybersecurity-Anforderungen beachten, Nutzer:innen informieren, Konformitätserklärungen abgeben, Security Updates bereitstellen und Schwachstellenhandling betreiben. Die Pflichten des CRA greifen zeitlich gestuft: Ab dem 11.09.2026 greifen die Meldepflichten bei Schwachstellen und Sicherheitsvorfällen und ab dem 11.12.2027 alle Pflichten für neue Produkte mit digitalen Inhalten.

Der Fachbeitrag wurde redaktionell begleitet von Alexandra Nikolić.

Zu den Produkten
sack.de/kompass-nink-it

Zum Video
sack.de/kompass-video

Mit einem Klick zum vollständigen Beitrag
sack.de/kompass-nink-it-ext