

EU-Vorschriften zu mehr Cybersicherheit

Die Europäische Union bringt im Rahmen ihrer Digitalstrategie zwei wichtige Gesetze auf den Weg: den Cyber Resilience Act (CRA) sowie die sogenannte NIS2-Richtlinie. Da wir immer digitaler werden, muss auch immer mehr Wert auf Onlinesicherheit, oder wie es auf Neudeutsch heißt, Cybersecurity, gelegt werden.

Die EU-Kommission hat am 15. September 2022 einen Entwurf des CRA vorgeschlagen, der noch vom europäischen Parlament und vom Rat angenommen werden muss.

Recht auf Updates durch den CRA

Mit dem CRA werden erhöhte Sicherheitspflichten auf Hersteller, Vertreiber, Importeure und Händler von IT-Produkten zukommen. Dazu zählen insbesondere geplante Meldepflicht für aktiv ausgenutzte Schwachstellen und Sicherheitsvorfälle. Durch die Vorgaben des CRA sollen sicherere Hardware- und Softwareprodukte gewährleistet werden.

Zu den dabei erfassten Produkten zählt jedes Software- oder Hardwareprodukt sowie seine Datenfernverarbeitungslösungen, einschließlich Software- oder Hardwarekomponenten, die separat in Verkehr gebracht werden. Er ist anwendbar auf „Produkte mit digitalen Elementen“, also auf solche Produkte, die ohne ihre digitalen Elemente nicht sinnvoll genutzt werden können (z. B. Smartphones). Der CRA teilt die Produkte mit digitalen Elementen in drei Kategorien ein:

- Standardkategorie
- kritische Klasse I
- kritische Klasse II

In die Standardkategorie fallen voraussichtlich gut 90 Prozent aller Produkte, wie z. B. Textverarbeitung, Fotobearbeitung oder Festplatten. Zum CRA gehören verschiedene Anhänge. Darin, nämlich in Anhang III, werden die kritischen Produkte mit digitalen Elementen der Klassen I und II aufgeführt. Zur kritischen Klasse I zählen u. a. Software für Identitätsmanagementsysteme, Browser, Passwortmanager, Antivirensoftware, VPN-Lösungen, Netzwerkmanagementsysteme, Werkzeuge zur Verwaltung der Netzwerkkonfiguration, Systeme zur Überwachung des Netzwerkverkehrs, Verwaltung von Netzwerkressourcen, Systeme zur Verwaltung von Sicherheitsinformationen und -ereignissen (SIEM), Update-/Patch-Verwaltung (einschließlich Bootmanager), Systeme zur Verwaltung der Anwenderkonfiguration, Software zur Verwaltung mobiler Geräte, Firewalls, Router/Modems, Anwenderspezifische integrierte Schaltungen (ASIC) oder auch Industrielle Automatisierungs- und Steuerungssysteme (IACS). Zur kritischen Klasse II zählen hingegen insbesondere Betriebssysteme für Server, Desktops und mobile Geräte, Infrastrukturen für öffentliche Schlüssel und Aussteller digitaler Zertifikate, Hardwaresicherheitsmodule (HSM), sichere Kryptoprozessoren, Smartcards, Smartcard-Lesegeräte und Token oder auch Geräte des industriellen Internets der Dinge.

Folgende Pflichten sollen zukünftig auf die vom Anwendungsbereich des CRA erfassten Unternehmen zukommen:

- Berücksichtigung der Cybersicherheit schon in der Planungs-, Entwurfs- und Entwicklungsphase sowie auch in der Produktions-, Liefer- und Wartungsphase („Security by Design“)
- umfangreiche Dokumentationspflichten in Bezug auf Cybersicherheitsrisiken
- Meldepflicht für aktiv ausgenutzte Schwachstellen und Vorfälle
- Überwachungs- und Beseitigungspflichten von Schwachstellen während der erwarteten Produktlebensdauer

(max. fünf Jahre)

- Pflicht zur Lieferung von klaren und verständlichen Gebrauchsanweisungen
- Pflicht zur Bereitstellung von bestimmten Pflichtinformationen (u. a. Name, Anschrift und Kontaktdaten des Herstellers, Typen-, Chargen-, Versions- bzw. Seriennummer, Verwendungszweck, Art der technischen Sicherheitsunterstützung, die der Hersteller anbietet, sowie der Zeitpunkt, bis zu dem sie geleistet wird)
- Pflicht zur Bereitstellung von Sicherheitsupdates für jedenfalls fünf Jahre

Ganz konkret und unabhängig von der jeweiligen Kategorie müssen Produkte mit digitalen Elementen zudem immer einer Risikobewertung unterzogen werden.

Unter die Produkte mit digitalen Elementen im Sinne des CRA fallen jedoch weder „Produkte mit digitalen Inhalten“ noch „digitale Produkte“. Die Erstgenannten zeichnen sich dadurch aus, dass der digitale Teil des Produkts für dessen Funktionsfähigkeit nicht von zentraler Bedeutung ist (z. B. Kühlschrank mit Bestellfunktion via App). Bei den „digitalen Produkten“ handelt es sich um rein digitale Produkte (z. B. Apps oder Musikdateien). Der CRA hat folglich einen sehr weit gefassten Anwendungsbereich, von dem nur ein paar spezifische Produktkategorien ausgenommen werden, wie beispielsweise Medizinprodukte. Software, die als Dienstleistung angeboten wird, also Software-as-a-Service-bzw. Cloudleistungen, wird ebenfalls gesondert geregelt.

Sichere Infrastrukturen durch NIS2

Speziell auf den Bereich der sogenannten kritischen Infrastruktur (KRITIS) zielt die NIS2-Richtlinie ab. Es geht also um den besseren Schutz von Stromversorgung, Wasserwerken oder Telekommunikationsleitungen. Es soll ein Höchstmaß an

Ausfallsicherheit gewährleistet werden, um beispielweise Strom-Blackouts oder Störungen der Trinkwasserversorgung für die Bevölkerung möglichst zu vermeiden oder jedenfalls so schnell und gut wie möglich auf derartige Störungen reagieren zu können.

In Deutschland ist mit Blick auf den KRITIS-Sektor bereits 2015 das IT-Sicherheitsgesetz (IT-SiG) in Kraft getreten. Darin war auch eine Änderung des damaligen § 13 Telemediengesetz (TMG) enthalten, der in einem Absatz 7 die Pflicht für alle Websitebetreiber zur Absicherung ihrer Websites mit sich brachte (z. B. durch Verschlüsselung nach dem Stand der Technik per SSL-/TLS-Zertifikat). Diese Norm findet sich nach der letzten Änderung des TMG nun in § 19 Abs. 4 des Telekommunikations-Telemedien-Datenschutz-Gesetzes (TTDSG). Seit Mai 2021 ist nunmehr das zweite IT-Sicherheitsgesetz (IT-SiG2) in Kraft, welches sowohl den Adressatenkreis als auch den Pflichtenkatalog der KRITIS-Betreiber merklich erweitert hat.

Aber auch auf EU-Ebene tut sich einiges. 2016 ist die Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union (kurz: NIS-Richtlinie) in Kraft getreten. Sie ist der europäische Rahmen für Cybersecurity im KRITIS-Bereich und soll ein hohes Sicherheitsniveau für Netzwerke und Informationssysteme sicherstellen.

Seit dem Jahr 2021 wird die NIS-Richtlinie überarbeitet. Ihr Nachfolger, die sogenannte NIS2-Richtlinie, soll den bestehenden Rechtsrahmen modernisieren, um die Herausforderungen des zunehmenden Grades an Digitalisierung und der stetig wachsenden Bedrohungen für die Cybersicherheit meistern zu können. Nach Inkrafttreten der NIS2-Richtlinie muss diese noch in das jeweilige nationale Recht der EU-Mitgliedsstaaten umgesetzt werden. In NIS2 wird zwischen

kritischen und wichtigen Einrichtungen unterschieden:

- *Kritische Einrichtungen:* Energie (Strom, Fernwärme und Fernkälte, Erdöl, Erdgas und Wasserstoff); Verkehr (Luft, Schiene, Wasser und Straße); Bankenwesen; Finanzmarktinfrastrukturen; Gesundheitswesen; Herstellung pharmazeutischer Erzeugnisse (einschließlich Impfstoffe und kritischer Medizinprodukte); Trinkwasserversorgung; Abwasserwirtschaft; digitale Infrastrukturen (Internetknoten, DNS-Anbieter, Anbieter von Clouddienstleistungen, Anbieter von Rechenzentrumsdiensten, Netze zur Bereitstellung von Inhalten, öffentliche elektronische Kommunikationsnetze und elektronische Kommunikationsdienste,...); öffentliche Verwaltung; Weltraum.
- *Wichtige Einrichtungen:* Post- und Kurierdienste; Abfallwirtschaft; Chemikalien; Lebensmittel; Herstellung anderer Medizinprodukte, von Computern, Elektronik und Kraftfahrzeugen sowie Maschinenbau; Anbieter digitaler Dienste (Onlinemarktplätze, Onlinesuchmaschinen und Plattformen der sozialen Netzwerke).

Sowohl die kritischen als auch die wichtigen Einrichtungen müssen u. a. folgende Cybersecurity-Maßnahmen treffen:

- Erlass und Umsetzung von Richtlinien für Risiken und Informationssicherheit
- Umsetzung von Maßnahmen zur Prävention, Detektion und Bewältigung von Cybersecurity-Vorfällen (Sicherheitspannen)
- Ergreifen von Maßnahmen zum Business Continuity Management (BCM) inkl. Backup- bzw. Krisenmanagement
- Gewährleistung der Sicherheit bei der Beschaffung von IT- und Netzwerksystemen
- Beachtung von Vorgaben für Kryptografie bzw. Verschlüsselung

- Umsetzung angemessener Maßnahmen zur Zugangskontrolle
- Einsatz sicherer Sprach-, Video- und Textkommunikation
- Einsatz gesicherter Notfallkommunikationssysteme

Durch die NIS2-Richtlinie wird der Aspekt der Cybersecurity zukünftig in der gesamten Lieferkette zu berücksichtigen sein. Außerdem sollen die Aufsicht und die Zusammenarbeit zwischen den Behörden und den von NIS2 betroffenen Betreibern innerhalb der EU vertieft werden. Die Sanktionen bei Verstößen gegen die NIS2-Vorgaben sollen durch die einzelnen EU-Mitgliedsstaaten selbst geregelt werden. Allerdings wird von Seiten des EU-Gesetzgebers bestimmt, dass die Sanktionen wirksam, verhältnismäßig und abschreckend sein müssen. Gegen kritische Einrichtungen sollen Geldbußen mit einem Höchstbetrag von mindestens 10 Mio. Euro oder von mindestens 2 Prozent des gesamten weltweit erzielten Vorjahresumsatzes verhängt werden können. Bei Sanktionen gegen wichtige Einrichtungen soll der Höchstbetrag mindestens 7 Mio. Euro oder 1,4 Prozent des Vorjahresumsatzes betragen.

Praxistipp

Neben dem CRA und NIS2 beinhaltet die Strategie der EU noch weitere Gesetze, die den Umgang mit digitalen Daten regeln sollen. Dazu zählen insbesondere der Data Governance Act (DGA) zur Förderung der Weiterverwendung von Daten des öffentlichen Sektors, der Digital Markets Act (DMA) und der Digital Services Act (DSA) zur Regulierung großer Onlineplattformen, der Artificial Intelligence Act (AIA) zur Regulierung von Künstlicher Intelligenz (KI) oder auch der Data Act (DA) zur besseren Weiterverwendung von Unternehmensdaten. Bei diesen Rechtsakten handelt es sich nicht um bloße Zukunftsmusik, denn der DMA ist bereits seit dem 1. November 2022 in Kraft. Der DGA wird ab dem 24. September 2023 anwendbar sein, der DSA bereits ab dem 2. Mai 2023.

- Michael Rohrlisch hat als Rechtsanwalt und Fachautor seinen

Kanzleisitz in Würselen, Nähe Aachen. Seine beruflichen Schwerpunkte liegen auf dem Gebiet des Onlinerechts sowie des gewerblichen Rechtsschutzes. Weitere Infos zu den Themen aus den Rechtsbeiträgen sowie Gesetze und Gerichtsentscheidungen bietet er unter www.rechtssicher.info an.