

# Gefahr erkannt, Recht gebannt

## Europas Kampf gegen Cyberbedrohungen

Stefan Hessel und Christoph Callewaert, reuschlaw



Einer dynamischen Bedrohungslage im Bereich der Cybersicherheit stand bisher eine eher statische Rechtslage gegenüber. Neue europäische Rechtsakte sollen nun jedoch die Cybersicherheitsarchitektur neu ausrichten und verbindliche Vorgaben für Unternehmen und digitale Produkte festlegen. Für die betroffenen Unternehmen gehen damit erhöhte Compliance-Anforderungen einher, die mit Blick auf die kurzen Umsetzungsfristen frühzeitig angegangen werden sollten.

## I. Status quo: Dynamische Bedrohungslage, statische Rechtslage

Die Digitalisierung und Vernetzung von Produkten und Unternehmen schreitet kontinuierlich voran. Nahezu täglich kommen neue internetfähige Produkte auf den Markt oder werden in die Prozesse von Unternehmen implementiert. Während die Vernetzung und Konnektivität einerseits zahlreiche Chancen und Möglichkeiten zur Prozessoptimierung bietet, bleiben andererseits auch Risiken nicht aus: Das Bundesamt für Sicherheit in der Informationstechnik (BSI) geht in seinem Bericht zur Lage der IT-Sicherheit in Deutschland 2022 von insgesamt 116 Millionen Schadprogrammen im vergangenen Jahr aus [1]. Fast täglich berichten die Medien über Cyberangriffe auf Unternehmen und damit verbundene Produktionsausfälle entlang ganzer Lieferketten. Nach Angaben der EU-Kommission entstanden im Jahr 2021 allein durch Ransomware-Angriffe weltweit Schäden in Höhe von rund 20 Milliarden Euro [2]. Unter Cybersicherheitsexperten ist längst bekannt: Es ist keine Frage des „Ob“, sondern lediglich des „Wann“, ein Unternehmen von einem Cyberangriff betroffen ist.

Dieser dynamischen Bedrohungslage stand bisher eine recht statische Rechtslage gegenüber: Auch wenn vereinzelt sektorspezifische und nationale rechtliche Vorschriften für bestimmte regulierte Bereiche, wie beispielsweise für die Betreiber sogenannter „Kritischer Infrastrukturen“ bestehen, fehlt es insgesamt an flächendeckenden, horizontalen und insbesondere europäischen Regelungen für die Cybersicherheit – denn Cyberkriminalität macht nicht an Landesgrenzen halt.

---

**Es ist keine Frage des „Ob“, sondern lediglich des „Wann“, ein Unternehmen von einem Cyberangriff betroffen ist.**

## II. Die neue europäische Cybersicherheitsarchitektur

Die EU-Kommission hat den bestehenden Handlungsbedarf erkannt und sich eine neue europäische Cybersicherheitsarchitektur zum Ziel gesetzt, die das Cybersicherheitsniveau und die Widerstandsfähigkeit der EU gegenüber Cyberangriffen erhöhen soll. Das Fundament dieser Architektur bilden im Wesentlichen die Novellierung der Network and Information Security Directive (NIS-2-Richtlinie) [3] und der geplante Cyber Resilience Act (CRA) [4].

### 1. Unternehmensbezogene Anforderungen der NIS-2 Richtlinie

Die bereits am 16. Januar 2023 in Kraft getretene NIS-2-Richtlinie ersetzt die bisherige NIS Richtlinie und enthält unternehmensbezogene Cybersicherheitspflichten. Sie richtet sich an „wesentliche“ und „wichtige“ Einrichtungen aus insgesamt 18 Wirtschaftssektoren wie Energie, Verkehr, digitale Infrastruktur, verarbeitendes Gewerbe oder Anbieter digitaler Dienste. Unternehmen fallen bereits ab einem Schwellenwert von 50 Mitarbeitenden und einem Jahresumsatz von zehn Millionen Euro unter die Richtlinie. Einrichtungen, die aufgrund ihrer besonderen nationalen oder regionalen Bedeutung als kritisch eingestuft werden, werden unabhängig von Schwellenwerten ebenfalls einbezogen. Nach diesen Kriterien sind in Deutschland schätzungsweise 30.000 bis 40.000 Unternehmen von den Anforderungen der NIS-2-Richtlinie erfasst. Ein Großteil von ihnen ist sich der eigenen Betroffenheit noch nicht bewusst. Die Mitgliedstaaten müssen die Vorgaben der NIS-2-Richtlinie bis spätestens 17. Oktober 2024 in nationales Recht umsetzen.

„Cybersicherheit ist Chefsache“ – mit der NIS-2-Richtlinie wird diese langjährige Forderung des BSI nunmehr gesetzlich verbrieft: Die Geschäftsführung muss die getroffenen Maßnahmen im Bereich der Cybersicherheit genehmigen und überwachen – und haftet im Zweifelsfall für Verstöße [5]. Dies kann bei wesentlichen Einrichtungen sogar bis zum vorübergehenden Ausschluss der Geschäftsführung von ihren Führungsaufgaben reichen. Darüber hinaus muss die Geschäftsführung verpflichtend an Cybersicherheitsschulungen teilnehmen diese auch den Beschäftigten anbieten.



**Stefan Hessel**

Rechtsanwalt Stefan Hessel, LL.M. ist Salary Partner und Head of Digital Business bei reuschlaw in Saarbrücken.

#### Kontakt

stefan.hessel@reuschlaw.de

www.reuschlaw.de



### Christoph Callewaert

Rechtsanwalt Christoph Callewaert ist Associate bei reuschlaw in Saarbrücken.

### Kontakt

christoph.callewaert  
@reuschlaw.de

www.reuschlaw.de

Primäres Ziel der NIS-2-Richtlinie ist die Gewährleistung eines angemessenen Sicherheitsniveaus der Netz- und Informationssysteme der erfassten Einrichtungen. Alle unternehmerischen Entscheidungen sind hinsichtlich ihrer Auswirkungen auf die Netz- und Informationssysteme zu bewerten. Die Bewertung muss entsprechend dokumentiert werden. Im Rahmen der Risikobewertung identifizierte Risiken sind durch geeignete technische, operative und organisatorische Maßnahmen zu beherrschen. Die Richtlinie nennt hier einen bunten Strauß an Maßnahmen, wie beispielsweise Risiko- und Informationssicherheitsrichtlinien, vertragliche Regelungen in der Lieferkette, Verschlüsselung und Kryptographie, Systeme zur Notfallkommunikation oder ein Backupmanagement zur Wiederherstellung der Systeme nach einem Sicherheitsvorfall. Zu beachten ist jedoch das in der NIS-2-Richtlinie ausdrücklich erwähnte Verhältnismäßigkeitsprinzip: Welche Maßnahmen für welche Einrichtung angemessen sind, bedarf stets einer Einzelfallprüfung.

Um frühzeitig ein nationales und europäisches Bild von Schwachstellen oder Angriffsmustern zu erhalten, sieht die NIS-2-Richtlinie eng getaktete Meldepflichten für erhebliche Sicherheitsvorfälle vor. Ein Sicherheitsvorfall ist als erheblich einzustufen, wenn eine schwerwiegende Betriebsstörung der Dienste eingetreten ist oder einzutreten droht beziehungsweise finanzielle Verluste eingetreten sind oder einzutreten drohen. Ein Sicherheitsvorfall gilt auch dann als erheblich, wenn Dritte durch materielle oder immaterielle Schäden beeinträchtigt wurden oder werden können. Ist ein erheblicher Sicherheitsvorfall eingetreten, muss innerhalb von 24 Stunden eine Frühwarnung, innerhalb von 72 Stunden eine erste Bewertung und innerhalb eines Monats nach dem Sicherheitsvorfall ein Abschlussbericht an die zuständige Aufsichtsbehörde übermittelt werden.

## 2. Produktbezogene Anforderung des CRA

Mit dem CRA, der sich derzeit noch im Entwurfsstadium befindet, beabsichtigt die EU-Kommission einen horizontalen Rechtsrahmen mit umfassenden Cybersicherheitsanforderungen für alle Produkte mit digitalen Elementen und damit insbesondere für IoT-Geräte zu schaffen [6]. Hersteller sollen die Cybersicherheit digitaler Produkte bereits in der Design- und Entwicklungsphase berücksichtigen und über den gesamten Lebenszyklus oder einen

definierten Zeitraum aufrechterhalten. Für als besonders kritisch definierte Produkte wie Desktop- oder Mobilgeräte, Mikroprozessoren oder Smartcards sollen höhere Anforderungen gelten. Auch Importeure und Händler digitaler Produkte werden durch den CRA adressiert. Derzeit befindet sich der Entwurf der EU-Kommission in den sogenannten Trilogverhandlungen zwischen der EU-Kommission, dem EU-Parlament und dem Rat der EU.

Die grundlegenden Anforderungen sind in Abschnitt 1 des Anhangs I des CRA festgelegt. Danach müssen digitale Produkte unter anderem ohne bekannte ausnutzbare Schwachstellen ausgeliefert und geeignete Kontrollmechanismen zum Schutz vor unbefugtem Zugriff implementiert werden.

Eine zentrale Anforderung ist zudem die Möglichkeit, vom Hersteller entdeckte oder öffentlich bekannt gewordene Schwachstellen durch Sicherheitsupdates zu beheben (sogenannte „Updatability“): Hersteller sollen verpflichtet werden, für die erwartete Lebensdauer des jeweiligen Produkts oder für einen festgelegten Zeitraum sicherzustellen, dass erkannte Schwachstellen des Produkts wirksam geschlossen werden. Zum Nachweis der Konformität mit den Anforderungen des CRA müssen digitale Produkte künftig ein Konformitätsbewertungsverfahren durchlaufen.

Wie bei der NIS-2-Richtlinie spielt die Durchführung einer Risikobewertung eine zentrale Rolle: Hersteller sind künftig verpflichtet, eine Bewertung der Cybersicherheitsrisiken ihres digitalen Produkts durchzuführen.

Das Ergebnis der Bewertung ist zu dokumentieren und in allen Phasen der Herstellung zu berücksichtigen. Die Pflicht zur Risikobewertung setzt sich auch nach dem Inverkehrbringen des digitalen Produkts fort: Hersteller müssen effektive und regelmäßige Tests und Überprüfungen der Sicherheit des Produkts durchführen und Schwachstellen unverzüglich beheben, etwa durch die Bereitstellung von Sicherheitsupdates.

Wird Herstellern eine aktiv ausgenutzte Schwachstelle in einem von ihnen hergestellten digitalen Produkt bekannt, müssen sie die Europäische Cybersicherheitsagentur ENISA unverzüglich, in jedem Fall aber innerhalb von 24 Stunden nach Kenntniserlangung, informieren. Dadurch soll die ENISA in die Lage versetzt werden, schnell ein Lagebild über mögliche Sicherheitsrisiken zu erstellen.

### III. Auswirkungen für die Unternehmenspraxis

Mit Auswirkungen auf das Cybersecurity Compliance Management, die IT-Verträge, den Umgang mit Aufsichtsbehörden und die Anforderungen an Cybersicherungen stellt das neue Cybersicherheitsrecht Unternehmen gleich auf mehreren Ebenen vor große Herausforderungen [7]. Mit Blick auf die Dauer von unternehmensinternen Prozessimplementierungen und Produktentwicklungszyklen sollten Unternehmen aus den Sektoren der NIS-2-Richtlinie bzw. Hersteller, Importeure oder Händler digitaler Produkte frühzeitig ihre Betroffenheit von den künftigen Rechtsakten prüfen und gegebenenfalls individuell umzusetzende Vorgaben ableiten. Dabei ist auch eine „mittelbare Betroffenheit“ zu berücksichtigen: Von den neuen Vorgaben betroffene Unternehmen werden voraussichtlich nur dann Aufträge an Zulieferer und Dienstleister vergeben können, wenn deren Angebote den Anforderungen der künftigen Rechtsakte entsprechen.

Auch wenn die künftigen Rechtsakte unterschiedliche Anwendungsbereiche und Adressaten haben, lassen sich grundlegende Anforderungen an die Cybersicherheit identifizieren, die derzeit in IT-Verträgen häufig nicht angemessen berücksichtigt werden [8]. Dies betrifft insbesondere die Durchführung und Dokumentation einer Risikobewertung: Unternehmen sind bei der Risikobewertung regelmäßig auf Informationen aus der Lieferkette und von Herstellern eingesetzter Produkte angewiesen. Gleiches gilt für die Bereitstellung von Sicherheitsupdates und die Behebung von Schwachstellen: Die schnelle Bereitstellung von Updates erfordert in der Regel eine „Software Bill of Materials“ (SBOM), für die häufig Informationen von Drittherstellern benötigt werden. Aber auch Maßnahmen des Risikomanagements wie die Datensicherung und -wiederherstellung, die Erfüllung von Meldepflichten oder der Umgang mit Aufsichtsbehörden sollten in IT-Verträgen präzise geregelt werden.

Sowohl die NIS-2-Richtlinie als auch der Entwurf des CRA sehen bemerkenswert weitreichende Befugnisse der jeweiligen Aufsichtsbehörden vor: Die Maßnahmen reichen von Bußgeldern in Millionenhöhe über den Rückruf von Produkten bis hin zu einer vorübergehenden Entbindung der Unternehmensleitung von ihren Geschäftsführungsbefugnissen. Auch

wenn ähnlich wie bei der DSGVO in Bezug auf aufsichtsbehördliche Maßnahmen zunächst mit einer Art inoffizieller „Schonfrist“ zu rechnen ist, empfiehlt es sich, im Rahmen des Compliance Management zur Erfüllung der Managementpflichten insbesondere auf eine ausreichende Dokumentation der cybersicherheitsrechtlich relevanten Maßnahmen zu achten. Darüber hinaus sollte gerade vor der Geltung von Rechtsakten frühzeitig Kontakt mit den zuständigen Behörden aufgenommen werden, um deren Sichtweise in Bezug auf strittige beziehungsweise unklare Aspekte zu erfahren und gegebenenfalls auch deren Unterstützung bei der Umsetzung in Anspruch zu nehmen. Für Produkte kann hierzu vorbereitend insbesondere das freiwillige IT-Sicherheitskennzeichen des BSI in Erwägung gezogen werden [9].

Kommt es trotz der getroffenen Vorkehrungen zu einem Cybersicherheitsvorfall, drohen Schadenersatz- und Regressforderungen der Betroffenen. Aufgrund der Automatisierung und Skalierbarkeit von Verfahren durch Legal-Tech-Anwendungen können Cybersicherheitsvorfälle schnell Massenverfahren nach sich ziehen. Neben einer guten Dokumentation zahlt sich in diesen Fällen der Abschluss einer Cybersicherungsversicherung aus. Angesichts der stetig steigenden Risiken steigen allerdings auch die Anforderungen an die Versicherbarkeit von Unternehmen und die zu erfüllenden Sicherheitsprüfungen. Um „böse“ Überraschungen hinsichtlich der versicherten Risiken zu vermeiden, sollten entsprechende Policen rechtlich geprüft, und ein Maßnahmenplan für die Kommunikation mit dem Versicherer bereitgehalten werden. ■

#### Kurz und Bündig

Mit der NIS-2 Richtlinie und dem Entwurf des CRA kommen in naher Zukunft umfassende unternehmens- und produktbezogene cybersicherheitsrechtliche Anforderungen auf Unternehmen zu. Neben einer frühzeitigen Prüfung der Betroffenheit sollten Unternehmen insbesondere das Compliance Management und ihre IT-Verträge an die neuen Anforderungen anpassen. Nicht zuletzt aufgrund der weitreichenden Befugnisse der Aufsichtsbehörden sollte zudem auf eine ausreichende Dokumentation geachtet werden.



Weitere Infos und Literaturangaben zum Artikel finden Sie unter folgendem Link: <https://bit.ly/46W85wk>