Dr. Hans Markus Wulf, Hamburg

Neue EU-Vorgaben zur IT-Sicherheit – Geht Brüssel zu weit mit der Regulierung?

Der Autor
ist Partner, Rechtsanwalt und Fachanwalt für Informationstechnologierecht sowie IT- und Datenschutzexperte bei der wirtschaftsberatenden Kanzlei Heuking.

Mit der NIS-2-Richtlinie, der DORA-Verordnung (Digital Operational Resilience Act) und dem Cyber Resilience Act (CRA) wird die EU-Cybersicherheitsgesetzgebung in den kommenden Monaten auf den Kopf gestellt. Alle drei Gesetzgebungsvorhaben zielen auf die Erhöhung der digitalen Sicherheit, wobei nur der CRA eine nicht-sektorspezifische Regulierung aller vernetzten Produkte vorsieht.

Im Oktober 2024 muss die NIS-2-Richtlinie in nationales Recht umgesetzt worden sein. Auch mittelständische Unternehmen unterliegen dann den scharfen KRITIS-Vorgaben, sofern es sich um wesentliche und wichtige Einrichtungen gemäß Anhang I und II der Richtlinie, wie z. B. Managed-Services-Provider oder bestimmten Maschinenbauunternehmen, handelt. Ab Inkrafttreten des Umsetzungsgesetzes müssen diese erweiterte IT-Sicherheitsanforderungen erfüllen, etwa Risikobewertungen durchführen, besondere technische und organisatorische Maßnahmen treffen, ein Meldesystem einrichten oder sich behördlich registrieren; Erleichterungen sind allerdings teilweise vorgesehen.

Die DORA-Verordnung gilt ab Januar 2025 als lex specialis zur NIS-2-Richtlinie mit neuen IT-Sicherheitsvorschriften für regulierte Finanz- und Versicherungsunternehmen sowie deren IKT-Dienstleister (Informations- und Kommunikationstechnologie). Sie müssen umfassende Vorgaben zum IKT-Risikomanagement umsetzen, die insbesondere die Sicherstellung der digitalen Betriebsstabilität, diverse Prozesse zum Risikomanagement, deren Dokumentation und regelmäßige Audits der IKT-Systeme betreffen. Für das IKT-Outsourcing sind Risikoanalysen, vertragliche Mindeststandards sowie weitere Vorgaben für Anbieter mit Sitz in Drittstaaten vorgesehen. Auch IKT-Drittdienstleister, die etwa Cloud-Dienste oder Software an Finanzunternehmen anbieten, müssen aufgrund der – eigentlich sektorspezifischen – Verordnung Maßnahmen zum IKT-Risikomanagement treffen. Zwar folgt DORA einem risikobasierten Ansatz, die EU-Kommission verabschiedet jedoch sukzessive technische Regulierungsstandards (RTS) und Implementierungsstandards (ITS), die spezifische technische Vorgaben regeln, die teilweise über die gängigen ISO-Standards hinausgehen. Viele der Anforderungen entsprechen den bestehenden Regularien, etwa der BAIT oder den übergeordneten MaRisk der BaFin, werden nun aber erstmals in Gesetzesform gegossen.

In Kürze wird auch der CRA verabschiedet, der als horizontale Regulierung nach einer Übergangsfrist alle Hersteller, Betreiber, Importeure und Händler von vernetzten Produkten verpflichten wird. Primär werden Hersteller u. a. verpflichtet, vorherige Risiko- und Konformitätsbewertungen durchzuführen, Meldepflichten und Schwachstellenanalysen umzusetzen oder einen vollständigen Schutz vor Manipulation sowie regelmäßige Sicherheitsupdates der implementierten Software sicherzustellen.

Ihren Zielen werden die Gesetzesvorhaben nur teilweise gerecht. Zwar entspricht der erweiterte Anwendungsbereich von NIS-2 der wachsenden Bedrohungslage durch Cyberrisiken, allerdings kann er für mittlere Unternehmen zu einer Überforderung führen und es ist fraglich, ob schon bei 50 Mitarbeitern Bußgelder von bis zu 2 % des weltweiten Jahresumsatzes gerechtfertigt sind. Nehmen die Behörden nun Rücksicht auf diese Unternehmen, können Defizite bei der Umsetzung und eine Aufweichung zu Lasten der Cybersicherheit die Folge sein. Auch wenn die neuen Anforderungen grundsätzlich sinnvoll sind, wäre hier ein Festhalten an der Kritikalität als maßgebliches Kriterium geeigneter gewesen, als nach dem Prinzip „Gießkanne“ vorzugehen.

Auch bei DORA ist fraglich, ob die Verordnung den Spagat zwischen risikobasiertem Ansatz und den RTS und ITS hinbekommt. Zwar können letztere ggf. einfacher angepasst werden als die Verordnung selbst, allerdings sind die spezifischen Vorgaben nicht für alle Unternehmen gleichermaßen geeignet. Dieses Problem zieht sich durch die gesamte Verordnung. Auch hinsichtlich der Verträge mit IKT-Dienstleistern sind viele Spezialthemen zu regeln (z. B. Dienstleistungsgüte, Aktualisierungen oder Behördenkommunikation), die Vertragsverhandlungen komplexer und fehleranfälliger werden lassen. Nicht jedes Finanzunternehmen kann solche Klauseln durchsetzen, insbesondere gegenüber den großen US-Hyperscalern. Zusammen mit der weiten IKT-Definition kann dies aber auch die kleineren IT-Dienstleister beschränken. Es ist dennoch positiv zu werten, dass – angesichts des grenzüberschreitenden Charakters von IKT-Risiken – Inkohärenzen und Mehrkosten durch Alleingänge der Mitgliedstaaten beseitigt werden. Allerdings bleibt es durch RTS und ITS bei einer komplexen Rechtslage, die schwierig zu durchdringen und noch schwieriger umzusetzen ist.

Die neuen EU-Umsetzungspflichten zur IT-Sicherheit sind enorm und werden Unternehmen erheblich belasten, allerdings wird eine EU-weite Resilienz anders nicht zu erreichen sein.

Im Gegensatz dazu lassen die technologieneutralen Vorschriften im CRA viel Spielraum für Innovationen – jedenfalls solange die Behörden minimale Schwachstellen der Produkte durchgehen lassen. Denn tatsächlich werden Hersteller zumindest ein (Rest-) Risiko wohl fast immer bewusst in Kauf nehmen müssen. Der Fokus sollte deutlich auf Erkennung von Schwachstellen und deren Beseitigung liegen.

Es besteht die Hoffnung, dass Cybersecurity durch die Gesetzesvorhaben zu einem wesentlichen Teil der Unternehmenskultur wird. Die Union sollte jedoch im Blick behalten, dass der teils stark fragmentierte Ansatz den Blick fürs Wesentliche verstellt und Unternehmen sich in den zahlreichen Compliance-Dokumenten verlieren können. Die oftmals komplizierten Prozesse werden wohl zu mehr Outsourcing führen und so möglicherweise doch die Sensibilisierung für Cybersecurity schwächen.