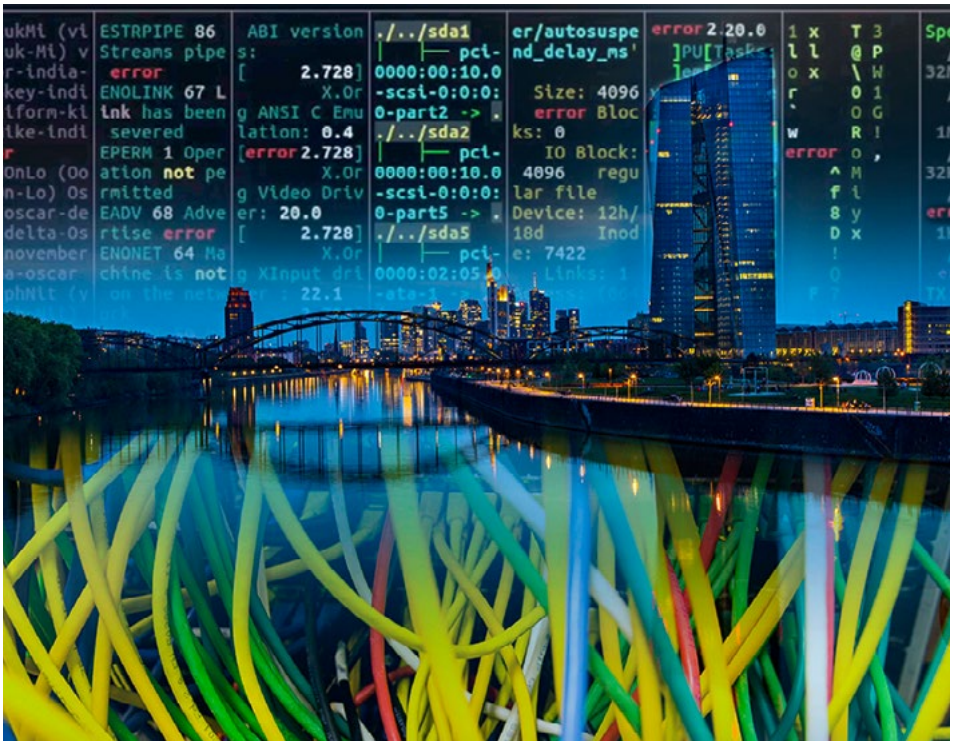
Compliance-Hammer durch das „NIS-2-Umsetzungsgesetz“

IT-Sicherheit, das ist Chef/innenaufgabe; diese Phrase kreist bereits seit einiger Zeit durch die Juristerei. Dem ist unter Heranziehung allgemeiner Compliance-Regelungen für die Leitungsebene in Unternehmen schon jetzt zuzustimmen. Richtig faustdick kommt es nun aber durch ein neues Gesetz.



© IMAGO / Jochen Tack

Finanzstandort Frankfurt: Der Schutz vor Cyberangriffen ist elementar.

Das sogenannte NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz wird das Recht der IT-Sicherheit in Deutschland revolutionieren und kommt mit Regelungen für Leitungspersonen daher, die ihresgleichen suchen. Das Gesetz liegt seit Mai 2023 als Synopse für einen Referentenentwurf vor. Aufgrund der NIS-2-RL, die bis Oktober 2024 in nationales Recht umgesetzt sein muss, ist aber sicher, dass der Entwurf in seinen Grundzügen so Gesetz werden muss.

Die NIS-2-RL (RL (EU) 2022/2555) wurde Ende 2022 verabschiedet und ersetzt eine Richtlinie zur Gewährleistung von Netzwerk- und Informationssicherheit (NIS-RL) aus dem Jahr 2017. Sie hat in Deutschland einen maßgeblichen Einfluss auf die Unternehmens- und Einrichtungskategorien der Kritischen Infrastrukturen, insbesondere im BSIG.

Hierbei wird es nun in Zukunft aber nicht bleiben. Aus den Sektoren Energie, Verkehr und Transport, Bankwesen, Finanzmarktinfrastrukturen, Gesundheitswesen, Trinkwasser, Abwasser, Ernährung, Digitale Infrastruktur sowie Siedlungsabfallentsorgung werden in Zukunft die kritischen Anlagen als Nachfolger der Kritischen Infrastrukturen, die besonders wichtigen und die „nur“ wichtigen Einrichtungen erfasst. Hinzukommen bestimmte Anbieter im Telekommunikations- sowie Internetbereich. Das Gesetz wird hauptsächlich Großunternehmen und mittlere Unternehmen entsprechend den bekannten europäischen Maßstäben betreffen. Es gelten dann jeweils abgestufte Pflichten. Am strengsten erwischt es weiterhin die kritischen Anlagen.

Neben umfassenden Risikomanagementvorschriften, die im Vergleich zur bisherigen Rechtslage deutlich konkretisiert und verschärft werden (bspw. Pflicht zum Business-Continuity-Management), sowie einer nunmehr als gestuft geplanten Meldepflicht bei Sicherheitsvorfällen (Erstmeldung, Zwischenmeldung, Abschlussmeldung) sind es vor allem die Sanktionsvorschriften sowie bislang nie dagewesene Compliance-Vorschriften für die Leitungspersonen der Unternehmen und Einrichtungen, die schon jetzt die Leitungsebenen der betroffenen Sektoren zu Maßnahmen bewegen sollten. Zudem kann sich der Beratungssektor auf einen deutlichen Arbeitsaufwand einstellen.

Das BSIG sieht aktuell zwar auch schon Bußgelder in Millionenhöhe vor, allerdings sind diese Sanktionsvorschriften in der Praxis bislang weitgehend unberücksichtigt geblieben. Stand Mai 2023 hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) seit 2015 erst ein Bußgeldverfahren eingeleitet. Die EU-Kommission hat im Richtlinienverfahren die laxe Bußgeldpraxis in den Mitgliedstaaten kritisiert. Daher wurden die Vorschriften verschärft. Sowohl für die besonders wichtigen als auch wichtigen Einrichtungen wird neben den Bußgeldrahmen in Millionenhöhe eine Bemessung anhand des weltweiten Konzernumsatzes, wie etwa aus der DSGVO bekannt und gefürchtet, eingerichtet werden. Für kritische Anlagen sollen Geldbußen bis 20 Mio. EUR möglich sein.

© Privat

Tilmann Dittrich, LL. M. (Medizinrecht), ist Rechtsreferendar im OLG-Bezirk Düsseldorf und Doktorand am Lehrstuhl von Prof. Dr. Helmut Frister an der Heinrich-Heine-Universität Düsseldorf.

Nun aber zu den angekündigten Compliance-Vorschriften, die teilweise über die Vorgaben der NIS-2-RL hinausgehen wollen. Hinsichtlich der Pflichten zum Risikomanagement soll für die Geschäftsleitung eine Billigungs- und Überwachungspflicht bestehen. Es soll keine komplette Delegation möglich sein, sondern stets zumindest eine Letztverantwortung bei der Leitungsebene verbleiben. Außerdem – ebenfalls mit erheblicher Praxisrelevanz für die Beratungsbranche – sollen sich Leitungspersonen in Schulungen das notwendige Fachwissen erarbeiten, um eben solche Risikomanagementprozesse auch bewerten zu können.

Der „Hammer“ ist aber die geplante überschießende Regelung, dass sich die Unternehmen und Einrichtungen bei Schäden durch Verstöße gegen diese Compliance-Pflichten zwingend an die Leitungspersonen halten müssen. Ein Verzicht auf oder Vergleich über Schadensersatzansprüche soll ausdrücklich ausgeschlossen sein. Möglicherweise müssen hierauf auch bestehende Versicherungslösungen überprüft werden, falls dies so Gesetz werden sollte. Ein letztes besonderes Compliance-Element soll die Möglichkeit sein, dass das BSI für die Umsetzung bestimmter Vorschriften einen Überwachungsbeauftragten (Compliance-Monitor) bestimmen kann.

Es gilt also für die Unternehmen und Einrichtungen, den Gesetzgebungsprozess aufmerksam zu beobachten. Spannend bleibt, ob die zwingende Inanspruchnahme der Leitungsebene bei Compliance-Verstößen tatsächlich so kommen wird. Bereits jetzt dürfte es sinnvoll sein, der „Schulbank-Pflicht“ zuvorzukommen und Leitungspersonen, sofern noch nicht geschehen, mit IT-Sicherheits-Kenntnissen auszustatten und bestehende Delegationen und Überwachungsprozesse auf den Prüfstand zu stellen. *Tilmann Dittrich*