NIS2: „In keinem anderen Gesetz existiert eine so starke Geschäftsführerhaftung“

„Die Bedrohungslage ist so hoch wie nie! Die Einschläge werden häufiger und ausgefuchster“, beschrieb Dr. Paul Vogel die aktuelle Entwicklung im Bereich Cybercrime. Gemeinsam mit Andreas Daum erläuterte er in einem Webinar im Rahmen der Noerr Digital Talks unter anderem die Hintergründe und Auswirkungen der NIS2-Richtlinie.

© IMAGO / aalphoto

NIS 2: Cybersicherheitsmaßnahmen sind jetzt Sache des Top-Managements.

Man könne fast schon von einer Cybercrime-Schattenwirtschaft sprechen, sagte Vogel. Dem begegne der europäische Gesetzgeber mit verschiedenen Mitteln; dazu gehören

1. die DORA-Verordnung (Digital Operational Resilience Act), mit der die Cybersicherheit für Finanzinstitute und Versicherer adressiert werde,
2. der Cyber Resilience Act (CRA), der auf Produktebene Cyberresilienz regele,
3. die CER-Richtlinie (Critical Entities Resilience) über kritische Einrichtungen, die vom deutschen Gesetzgeber mit dem KRITIS-Dachgesetz umgesetzt werden müsse, und schließlich
4. die NIS2-Richtlinie, die der deutsche Gesetzgeber mit dem NIS2-Umsetzungs- und Cybersicherheitsgesetz als neues BSI-Gesetz umsetze.

Das Besondere an NIS2: „Wer unter diese Richtlinie fällt, hat ein Mindestmaß an Cybersicherheitsmaßnahmen umzusetzen. Das kann nicht mehr delegiert werden, sondern ist Sache des Top-Managements“, stellte Vogel gleich zu Beginn klar.

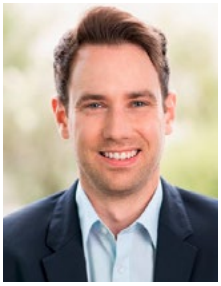
Erfasst seien nur mittlere und große Unternehmen (mehr als 50 Mitarbeiter oder 10 Mio. Euro Jahresumsatz) im Sinne der KMU-Regeln. Zu beachten sei jedoch, dass unter Umständen auch Mitarbeiterzahlen aus einem Konzernverbund mit einberechnet werden müssen. Die Prüfung hierzu müssten Unternehmen an sich selbst vornehmen. „Das BSI kann hier möglicherweise unterstützen, das wird aber bei perspektivisch bis zu 30.000 zu regulierenden Unternehmen in Deutschland schwierig werden“, räumte Vogel ein.

Die Pflichten für Unternehmen erläuterte Daum: Sie reichen von der Registrierung des Unternehmens beim BSI über Risikomanagementmaßnahmen, den Nachweis darüber an das BSI, die Meldepflicht im Fall eines Vorfalls an das BSI bis hin zu Informationspflichten über Inhalt, Umfang, Dauer des Vorfalls gegenüber dem BSI und der Mitteilungspflicht gegenüber den Kunden – und das auch, wenn es nicht um Kundendaten geht. Wichtig zu wissen sei, dass bereits der Verdacht eines Vorfalls zur Meldung verpflichte. Die Devise müsse also sein, eher einmal zu viel zu melden, als darauf zu verzichten.

Als wesentliche Daumenschrauben räume das Gesetz dem BSI die Möglichkeit ein, Maßnahmen anzuordnen, die so weit gehen, dass dem Verantwortlichen der Geschäftsführung sogar die Führung der Geschäfte untersagt werde, das BSI sich so quasi selbst zum Geschäftsführer aufschwingen und die Maßnahmen im Unternehmen durchsetzen könne. Die Gefahr, dass es soweit komme, sei aber gering, denn dazu müsste sich ein Unternehmen den ausdrücklichen Anordnungen des BSI widersetzen.

Daneben gebe es die üblichen Bußgelder von bis zu 10. Mio. Euro oder 2 Prozent des gesamten weltweiten Jahresumsatzes.

Die schmerzhafteste Durchsetzungsmaßnahme der NIS2-Richtlinie sei allerdings die Geschäftsführerhaftung: „Das Gesetz gibt der Geschäftsführung auf, sich aktiv um die Risikomanagementmaßnahmen zu kümmern, sie also umzusetzen und zu überwachen. Diese Pflichten können nicht einfach an die IT-Abteilung oder die Rechtsabteilung delegiert werden“, stellte Daum klar. Selbstverständlich solle die Geschäftsführung nicht selbst die Risikoanalyse durchführen und sämtliche Bereiche des Unternehmens auf Cybersecurity durchleuchten, Schwachstellen identifizieren und entsprechende Maßnahmen anordnen und umsetzen. „Das ist sicherlich nicht gemeint, denn dann würde die Geschäftsführung nichts anderes mehr tun“, so Daum.



© Noerr

Andreas Daum, LL.M. (LSE), RA, ist spezialisiert auf die rechtliche Beratung in den Bereichen Data Economy und Cybersecurity sowie im Zusammenhang mit komplexen IT-Projekten.

© Noerr

Dr. Paul Vogel, LL.M. Eur., RA, ist Mitglied der Praxisgruppe Data, Tech & Telecoms und des Noerr Cyber Risks-Teams. Er berät zum Datenschutz- sowie Cybersecurity-Recht.

Die aktivere Rolle sei indes im Zusammenhang mit der Schulungspflicht zu sehen, die in der NIS2-Richtlinie auch für die Geschäftsführung vorgesehen sei. Es gehe also darum, dass die Geschäftsführung bei den Risikomanagementmaßnahmen eine informierte Entscheidung treffen könne. „Die Geschäftsführung muss wissen, wo die Schwachstellen des Unternehmens sind und wie sie darauf reagieren kann. Das ist nicht nur eine einmalige punktuelle Pflicht, sondern eine Dauerpflicht“, erklärte Daum. Die Risikomanagementmaßnahmen müssten somit auch von der Geschäftsführung überwacht und entsprechend angepasst werden. Werde diese Pflicht nicht eingehalten, hafte die Geschäftsführung persönlich, etwa für klassische Schäden bei einem Cybersicherheitsvorfall wie z.B. den Betriebsausfall im Unternehmen oder die Wiederherstellungskosten, wenn die Hardware nicht mehr fehlerfrei wiederhergestellt werden könne und die komplette Neubeschaffung der IT erforderlich werde. Schließlich könne auch ein entsprechendes Bußgeld darunterfallen.

Einen kleinen Lichtblick gebe es jedoch: In einem vorigen Entwurf war der Verzicht der Ansprüche der Gesellschaft gegen den Geschäftsführer nur im Insolvenzfall des Geschäftsführers möglich. Diese Passage sei gestrichen worden. Dennoch: „Es gibt in keinem anderen Gesetz eine so starke Pflicht, dass Geschäftsführer persönlich haften“, warnte Daum. *chk*

Mehr zu NIS2, Cyber-Schutzpflichten und deren Umsetzung im operativen Geschäft sowie der Rolle von Compliance dabei erfahren Sie auch bei der Deutschen Compliance Konferenz 2025, am 13. und 14. Mai 2025 in Frankfurt am Main.