RETHINKING LAW

INTERVIEW

„Die persönliche Haftung macht die NIS-2-Richtlinie zur Chefsache"

Die NIS-2-Richtlinie der EU soll angesichts einer zunehmenden Bedrohung durch Cyberattacken die Cybersicherheit der europäischen Wirtschaft stärken und auf ein einheitlich hohes Niveau bringen. Knapp 30.000 Unternehmen sind davon betroffen und müssen jetzt in ihre Ausstattung investieren. Datenschutzrechts-Experte Dr. Patrick Grosmann erklärt, was auf Unternehmen zukommt.

PG — Dr. Patrick Grosmann
VD — Viola C. Didier

VD Herr Dr. Grosmann, welche wesentlichen Änderungen bringt das neue Gesetz für die IT-Sicherheit in deutschen Unternehmen mit sich?

PG Statt wie bisher nur ca. 4.500 von der NIS-1-Richtlinie betroffene Unternehmen werden in Deutschland zukünftig ca. 30.000 Unternehmen in den Anwendungsbereich der NIS-2-Richtlinie fallen. Anders als bisher sind dabei nicht nur Betreiber kritischer Infrastrukturen betroffen.

VD Sondern?

PG Die NIS-2-Richtlinie gilt für diverse Branchen, weit über den Betrieb von kritischen Infrastrukturen hinaus. Die betroffenen Unternehmen werden in „wichtige" und „besonders wichtige" Einrichtungen kategorisiert – diese Unterscheidung spiegelt sich in den jeweiligen Pflichten, die durch Unternehmen zu erfüllen sind.

VD Wie werden die neuen Regelungen die Pflichten der Unternehmen hinsichtlich IT-Sicherheit im Vergleich zu den bisherigen Regelungen erweitern?

PG Die NIS-2-Richtlinie legt erhöhte Sicherheitsanforderungen fest: Dies umfasst etwa die Verpflichtung zur regelmäßigen Durchführung von Sicherheitstests und Risikobewertungen. Die aus meiner Sicht zentrale Pflicht der NIS-2-Richtlinie ist die Pflicht zur Einführung von Risikomanagementmaßnahmen. Auch wenn sich die konkret zu treffenden Risikomanagementmaßnahmen nach dem jeweils konkreten Unternehmenszuschnitt richten, soll an dieser Stelle ein einheitlicher IT-Sicherheitsstandard geschaffen werden. Neu ist insoweit, dass die NIS-2-Richtlinie für ca. 30.000 Unternehmen einen einheitlichen Mindeststandard der Risikomanagementmaßnahmen in Sachen IT-Sicherheit schafft.

VD Welche Branchen und Unternehmensgrößen sind konkret von den neuen IT-Sicherheitsanforderungen betroffen?

PG Das nationale Umsetzungsgesetz[1], das u.a. diverse Neuerungen des BSI-Gesetzes (BSIG) mit sich bringen wird, erfasst insgesamt 14 Sektoren. Diese kann man grob in die Bereiche Energie, Wasser, Verkehr, IT und digitale Infrastruktur, Bank- und Finanzwesen, Gesundheit, öffentliche Verwaltung, Industrie und Produktion aufschlüsseln.
Abhängig von der konkreten Einrichtungsart unterfallen die meisten Unternehmen der NIS-2-Richtlinie nur, wenn sie mehr als 50 Mitarbeitende beschäftigten oder einen Jahresumsatz

1 Bezug genommen wird hier auf den Gesetzesentwurf der Bundesregierung vom 22.07.2024 zum „NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz".

von mehr als 10 Millionen Euro aufweisen. Je nach Konstellation können bei der Berechnung auch „Partnerunternehmen“ oder „verbundene Unternehmen“ zumindest anteilig hinzugerechnet werden. Gleichzeitig kann auch nur ein Teil der Mitarbeiter und des Umsatzes berücksichtigt werden, wenn nur ein Teil des Unternehmens NIS-2-relevante Tätigkeiten ausübt.
Von den Schwellenwerten gibt es Ausnahmen: Einige besonders relevante Einrichtungsarten fallen unabhängig eines Schwellenwerts unter die NIS-2-Richtlinie.
Deutlich wird: Die Bestimmung der NIS-2-Betroffenheit ist komplex und bildet die erste relevante Hürde des Umgangs mit der Richtlinie.

VD Wie sollten Unternehmen ihre Mitarbeiter in Bezug auf IT-Sicherheit jetzt schulen?

PG Die Sensibilisierung von Mitarbeitern zur IT-Sicherheit ist unabhängig der NIS-2-Richtlinie besonders wichtig – dies zeigen die diversen IT-Sicherheitsvorfälle, die letztlich auf ein menschliches Fehlverhalten zurückzuführen sind.
Die NIS-2-Richtlinie sieht nun vor, dass Mitarbeiter und ausdrücklich auch die Geschäftsleitung zur IT-Sicherheit zu schulen sind. Aus meiner Sicht ist es wichtig, die Schulungen nicht bloß als Bürde zu verstehen: Schulungen sollten so konzipiert werden, dass die Mitarbeiter mit deren Arbeitsrealität abgeholt werden und Interesse geweckt wird. Dabei helfen regelmäßige Präsenzschulungen, bei denen tatsächlich die (volle) Aufmerksamkeit der Mitarbeiter gewonnen wird.

VD Welche Konsequenzen drohen Geschäftsleitern, die die IT-Sicherheitsanforderungen nicht ausreichend umsetzen?

PG Unternehmen sind bei der Verletzung von der NIS-2-Richtlinie Bußgeldern und potenziellen Schadensersatzforderungen ausgesetzt. Besondere Vorsicht ist für Geschäftsleiter geboten: Diese sehen sich einem Haftungsrisiko ausgesetzt, wenn aufgrund eines schuldhaften Verstoßes gegen die NIS-2-Richtlinie Schäden entstanden sind.
Darüber hinaus drohen bei Verstößen gegen die NIS-2-Richtlinie je nach Schwere des Verstoßes Bußgelder von bis zu 10 Millionen Euro oder 2 % des weltweiten Jahresumsatzes.

VD Was bedeutet die persönliche Haftung der Geschäftsleitung für die IT-Sicherheit in der Praxis?

PG Ähnlich wie bei der DSGVO ist zu erwarten, dass die persönliche Haftung der Geschäftsleitung dafür sorgt, dass die Erfüllung der NIS-2-Richtlinie zur „Chefsache“ gemacht wird. Damit bekommt die NIS-2-Richtlinie eine erhöhte Management-Attention – aus meiner Sicht lässt sich hoffen, dass dies insgesamt einen positiven Effekt auf die IT-Sicherheit in der EU hat.

VD Welche zusätzlichen Befugnisse erhält das Bundesamt für Sicherheit in der Informationstechnik (BSI) durch das neue Gesetz?

PG Durch die Gesetzesänderung kommt es zu einer Ausweitung der bereits bestehenden Aufgaben und Befugnisse des BSI. Das BSI wird umfangreiche Aufsichts- und Überwachungsmaßnahmen der Pflichten nach der NIS-2-Richtlinie übernehmen. Die Behörde ist zudem für die Entgegennahme der Registrierungen betroffener U nternehmen sowie der Meldungen nach einem IT-Sicherheitsvorfall zuständig. Außerdem kann das BSI die Geschäftsleitung temporär ihrer Position entheben.

Das komplette dreiseitige Interview ist abrufbar unter https://research.owlit.de/lx-document/ZURE1465886, für ZURe-Abonnenten kostenfrei, ansonsten kostenpflichtig.

Datenschutzrechtliche Meldepflicht
Mit der DSGVO hat der Gesetzgeber die Verpflichtung eingeführt, Verletzungen des Schutzes personenbezogener Daten der zuständigen Aufsichtsbehörde unverzüglich, möglichst aber binnen 72 Stunden zu melden.