Zur Cybersicherheit verpflichtet

Auf die Absicherung der IT-Infrastruktur wird immer noch zu wenig Wert gelegt. Ein neues Gesetz auf Basis der NIS-2-Richtlinie soll dies ändern und mehr Unternehmen in die Pflicht nehmen. Geschäftsführern, die die IT-Sicherheit schleifen lassen, droht eine strengere Haftung.

Bild: ©Konsta/stock.adobe.com

Zum Thema Cyberattacken ist eigentlich schon alles gesagt: Es gibt aktuell keine größere Bedrohung für die deutsche Wirtschaft. Und trotzdem sind die Schutzmaßnahmen, die getroffen werden, nicht ausreichend. Die europäische Richtlinie zur Stärkung der Cybersicherheit, kurz NIS-2, zielt deshalb auf einen erheblich größeren Adressatenkreis als der Vorgänger NIS-1: rund 30.000 Unternehmen zusätzlich werden wohl ab Oktober unter das deutsche Umsetzungsgesetz fallen – und zwar ohne Übergangsfrist.

Zielgruppe schwer zu bestimmen

Wer betroffen ist, entscheidet sich nach der Zugehörigkeit zu bestimmten Sektoren und anhand von Schwellenwerten bei Unternehmensgröße und Umsatz. Anders als bei NIS-1, wo es nur eine Anlage I mit KRITIS-Unternehmen gab, gibt es bei NIS-2 nun zusätzlich eine Anlage II. Diese listet Sektoren wie Entsorgung, Chemie, Lebensmittel und verarbeitendes Gewerbe auf und nennt für den Sektor Transport und Verkehr ausdrücklich Post- und Kurierdienste. In diesen Sektoren sind alle „wichtigen Einrichtungen" betroffen, das sind Unternehmen ab 50 Beschäftigten oder ab 10 Millionen Euro Jahresumsatz.
Logistikanbieter sind im aktuellen Gesetzentwurf (noch) nicht ausdrücklich erwähnt. „Logistik- und Fulfillment-Unternehmen werden aber mindestens mittelbar betroffen sein, weil deren Auftraggeber im Zuge ihrer gesetzlich vorgeschriebenen Sicherheitsmaßnahmen auf ihre gesamte Lieferkette achten müssen", gibt Rechtsanwalt Jens Ferner, Rechtsanwalt und Fachanwalt für IT-Recht in Alsdorf, zu bedenken. Die E-Commerce-Logistik dürfte aufgrund ihres reichen Schatzes an Endkundendaten besonders attraktiv für Cyber-Angriffe sein, und damit auch die Auftraggeber, etwa große Online-Händler, unter Druck setzen.

Pflichten und Sanktionen

Die Europäische Union will ein einheitliches hohes Cyber-Sicherheitsniveau in allen Mitgliedstaaten etablieren. Die Unternehmen im Fokus von NIS-2 haben deshalb ein IT-Risikomanagement zu etablieren und zu überwachen. Sie müssen sich registrieren lassen und dem Bundesamt für Sicherheit in der Informationstechnik (BSI) Sicherheitsvorfälle innerhalb kurzer Fristen melden. Regelmäßige Audits sowie Schulungen sind nachzuweisen und die Kunden über einen Vorfall zu informieren.
Die erweiterten Befugnisse der Kontrollbehörden beziehen sich auf Datenzugriffe, Vor-Ort-Kontrollen, Sicherheitsscans der Systeme usw.
Bei Gesetzesverstößen wird es happig: „Mit dem neuen IT-Sicherheitsrecht kommt auch ein neues Sanktionensystem, das aufwecken muss", sagt IT- und Strafrechtler Ferner. Denn der Bußgeldrahmen sieht 100.000 bis 10 Millionen Euro oder bis zu zwei Prozent des weltweiten Jahresumsatzes vor. Angesichts der Höhe der Bußgelder riskiert ein Geschäftsführer eines Mittelständlers bei Pflichtverstößen die Insolvenz des Betriebs.
Und gerät womöglich selbst in die persönliche Haftung. „Wenn ein Geschäftsleiter eines betroffenen Unternehmens den gesetzlichen Pflichten nicht nachkommt, haftet er nicht nur persönlich für entstandene Schäden und Bußgelder", berichtet Anwalt Ferner über die Pläne des Gesetzgebers. „Vielmehr soll das Unternehmen ihm gegenüber weder auf diesen Anspruch verzichten noch einen Vergleich darüber treffen können." Es sei fraglich, ob eine D&O-Versicherung dies abdecke. Ferner warnt: „Die hier entstehenden faktischen Sanktionen für Geschäftsleiter sind immens und noch lange nicht in allen Köpfen angekommen."

Zur Autorin

Anja Falkenstein ist als Rechtsanwältin in Karlsruhe tätig und schreibt zu Themen an der Schnittstelle Logistik/Recht.