Frankfurter Allgemeine Zeitung vom 24.09.2025, S. 16

Recht und Steuern

Neue Vorgaben für Cybersicherheit

Schon bald müssen Unternehmen die Brüsseler Vorgaben umsetzen. Noch herrscht viel Unsicherheit

Cyberangriffe gehören heute zu den größten Risiken für Unternehmen - egal ob Konzern oder Mittelständler. Sie legen Produktionslinien lahm, stehlen sensible Daten oder sabotieren kritische Infrastrukturen. Vor diesem Hintergrund will die EU mit der NIS-2-Richtlinie die Cybersicherheit europaweit auf ein einheitlich hohes Niveau heben. Mit mehreren Monaten Verspätung hat die Bundesregierung Ende Juli den Gesetzentwurf zur Umsetzung dieser Richtlinie beschlossen. Das Gesetz könnte noch in diesem Jahr in Kraft treten. Für betroffene Unternehmen bedeutet das: sofortige, bußgeldbewehrte Compliance - ohne Übergangsfrist. Doch viele wissen bis heute nicht, ob sie unter NIS 2 fallen.

Im Vergleich zur bisherigen Rechtslage gehören nicht mehr allein jene Branchen, welche zur sogenannten kritischen Infrastruktur zählen, zum Kreis der Verpflichteten. Erfasst werden von NIS 2 nunmehr - teilweise abhängig von bestimmten Schwellenwerten - beispielsweise auch Unternehmen, welche digitale Dienste erbringen, im Lebensmittelbereich tätig sind, zum verarbeitenden Gewerbe gehören oder Maschinen herstellen. Wurden bislang allein sieben Wirtschaftssektoren adressiert, sind es nunmehr 18 mit - nach Angaben des Bundesamts für Sicherheit in der Informationstechnik - etwa 29.000 betroffenen Unternehmen.

Die Anzahl der betroffenen Unternehmen kann jedoch auch wesentlich höher sein. Denn es ist weiterhin unklar, ob auch solche Unternehmen den erhöhten Cybersicherheitsanforderungen zu genügen haben, deren Hauptgeschäftstätigkeit nicht zu einem der regulierten Sektoren gehört, wohl aber eine Nebentätigkeit, wie etwa das Angebot einer Ladesäule für die Kundschaft oder das Betreiben einer Photovoltaikanlage. Zwar sollen nach dem Gesetzentwurf Tätigkeiten ausgeblendet werden, welche im Vergleich zur Hauptgeschäftstätigkeit "vernachlässigbar" sind. In welchen Fällen eine Tätigkeit "vernachlässigbar" ist, wird im Gesetzestext hingegen nicht weiter erläutert und in der Gesetzesbegründung nur vage umschrieben. Ohnehin ist zu bemerken, dass die offenbar vom Gesetzgeber gewollte Unterscheidung zwischen Haupt- und Nebentätigkeit von der Richtlinie gerade nicht vorgesehen ist. Es darf insofern bezweifelt werden, ob der Gesetzentwurf die Richtlinie ordnungsgemäß umsetzt.

Für Unternehmen in einem Konzernverbund dürfte sich ferner von vornherein die Annahme verbieten, allein deswegen nicht NIS 2 verpflichtet zu sein, weil sie die geforderten Schwellenwerte hinsichtlich der Mitarbeiteranzahl beziehungsweise des Jahresumsatzes und der Jahresbilanzsumme nicht erreichen. Denn ist ein Unternehmen in Bezug auf seine IT nicht unabhängig von der Konzernmutter, so werden jedenfalls deren Werte den eigenen hinzugerechnet.

Die Pflichten, welchen von NIS 2 betroffene Unternehmen zu genügen haben, sind mannigfaltig. So sind jene Unternehmen angehalten, sich beim Bundesamt für Sicherheit in der Informationstechnik zu registrieren sowie technische, operative und organisatorische Maßnahmen zu ergreifen, um die Risiken für ihre IT beherrschen und die Auswirkungen von möglichen Sicherheitsvorfällen verhindern

oder möglichst gering halten zu können. Auszurichten sind jene Maßnahmen an der Eintrittswahrscheinlichkeit eines Sicherheitsvorfalls und dessen potentielle Auswirkungen sowohl auf das Unternehmen als auch auf die Gesellschaft und die Wirtschaft insgesamt. Umfassende Schulungspflichten der Mitarbeiter genauso wie Melde- und Berichtspflichten bei Sicherheitsvorfällen flankieren diese Maßnahmen. Sofern Unternehmen zur kritischen Infrastruktur zählen oder sich bestimmten sensiblen Sektoren zuordnen lassen, trifft diese darüber hinaus eine proaktive Nachweispflicht, dass die von ihnen getroffenen Maßnahmen ausreichend sind.

JÖRG WÜNSCHEL

Der Autor ist Anwalt bei *GSK Stockmann*.