LEGAL UPDATE IT- UND DATENSCHUTZRECHT
München und Berlin, 20.11.2023

Aktuelles IT-Sicherheitsrecht – Auswirkungen der NIS-2-Richtlinie auf Unternehmen

Thomas Altmann, Dr. Andrea Kirsch

In seinem am 02.11.2023 veröffentlichen Bericht zur Lage der IT-Sicherheit in Deutschland bezeichnet das Bundesamt für Sicherheit in der Informationstechnik (BSI) die Bedrohungslage erneut als besorgniserregend. Wenige Tage später gingen Mitteilungen über einen gegen einen kommunalen IT-Dienstleister in Nordrhein-Westfalen gerichteten Cyberangriff durch die Medien. Eine Woche später: Ein Ransomwareangriff auf eine Tochtergesellschaft der chinesischen Großbank ICBC mit Auswirkungen auf die internationalen Finanzmärkte. Bedauerlicherweise handelt es sich dabei nicht um Einzelfälle.

Bereits seit Längerem spielt das Thema IT-Sicherheit zum Glück nicht nur in den Medien eine Rolle, sondern wird verstärkt auch von der EU adressiert. In diesem Zusammenhang versucht der europäische Gesetzgeber zum wiederholten Mal dort nachzubessern, wo die Mitgliedstaaten der EU bislang keine umfassenden Regelungen hin zu einer verpflichtenden IT-Sicherheitscompliance getroffen haben. So wurde am 27.12.2022 die NIS-2-Richtlinie (Richtlinie über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union) veröffentlicht, die am 16.01.2023 in Kraft getreten ist. Der Grundstein für die Stärkung der IT-Sicherheit wurde bereits im Jahr 2016 mit der (ersten) NIS-Richtlinie gelegt. Sie legte Mindestsicherheitsanforderungen für Betreiber wesentlicher Dienste und digitale Dienstleister fest, die auf nationaler Ebene durch das IT-Sicherheitsgesetz umgesetzt wurden. Im Zuge dessen wurde insbesondere auch die BSI-KritisVO um die Vorgaben des EU-Richtliniengebers erweitert.

Die NIS-2-Richtlinie, die Teil der Bemühungen der Europäischen Union zur Stärkung der Cybersicherheit ist, hat weitreichende Auswirkungen auf die Unternehmenslandschaft. Während bislang primär die sog. kritischen Infrastrukturen, also Systeme und Einrichtungen, deren Ausfall oder Beeinträchtigung erhebliche Auswirkungen auf die öffentliche Versorgung und Sicherheit hätte, im Fokus standen, geht die NIS-2-Richtlinie in ihrer Reichweite deutlich über den Schutz kritischer Infrastrukturen hinaus.

Von der NIS-2-Richtlinie werden weit mehr als die bislang rund 2000 Unternehmen betroffen sein, die zu den „kritischen Infrastrukturen“ gehören. Bereits mittlere Unternehmen mit mindestens 50 Mitarbeitern und EUR 10 Millionen Jahresumsatz können bei Zugehörigkeit zu einem von 18 festgelegten Sektoren zur Umsetzung der rechtlichen Vorgaben verpflichtet sein. Die Anzahl betroffener Unternehmen in

Deutschland dürfte bei rund 30.000 liegen. Unter den betroffenen Sektoren befinden sich unter anderem folgende Bereiche: Energie, Verkehr, Gesundheitswesen, Digitale Infrastrukturen, aber auch das verarbeitende Gewerbe und die Herstellung von Waren.

Hinweise dazu, ob ein Unternehmen vom Anwendungsbereich der NIS-2-Richtlinie erfasst ist, bietet die unter folgendem Link abrufbare **Checkliste:**
https://forms.office.com/e/A4brtRAd5n

Auswirkungen auf Unternehmen

Um den Anforderungen der NIS-2-Richtlinie gerecht zu werden, müssen betroffene Unternehmen ihre Sicherheitspraktiken und -infrastrukturen an die von der Richtlinie geforderten Standards anpassen. Dazu gehören unter anderem die Implementierung von angemessenen Sicherheitsvorkehrungen und die Gewährleistung einer angemessenen Überwachung und Reaktion auf Cyberbedrohungen. Des Weiteren müssen Unternehmen interne Mechanismen zur Risikobewertung und zum Krisenmanagement etablieren, um mögliche Sicherheitsvorfälle effektiv zu bewältigen.

Eine Ähnlichkeit zur Datenschutzgrundverordnung (DSGVO) besteht hinsichtlich der Meldepflichten bei Sicherheitsvorfällen und der Möglichkeit, bei Verstößen Bußgelder in erheblicher Höhe festzusetzen. Der Bußgeldrahmen reicht bis zu EUR 10 Millionen beziehungsweise 2% des weltweiten Jahresumsatzes des betroffenen Unternehmens. Die Besonderheit der NIS-2-Richtlinie: Sie sieht eine persönliche Haftung der Leitungsorgane gegenüber dem Unternehmen vor, wobei jedenfalls nach der Gesetzesbegründung des Entwurfs des Gesetzes zur Umsetzung der NIS-2-Richtlinie (NIS2UmsuCG) die Haftung auch Bußgeldforderungen umfasst.

Der Entwurf des NIS2UmsuCG wartet außerdem noch mit einer weiteren bußgeldbewehrten Pflicht auf: Betroffene Unternehmen werden in die Pflicht genommen, selbst zu prüfen, ob sie in den Anwendungsbereich des Gesetzes fallen. Ist dies der Fall, muss eine Meldung gegenüber dem BSI erfolgen.

Fazit und Ausblick

Bei dem aktuellen Entwurf des NIS2UmsuCG handelt es sich um ein Artikelgesetz, das verschiedene bestehende Gesetze, wie insbesondere das Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSIG) abändert.

Die Mitgliedstaaten müssen die NIS-2-Richtlinie bis zum 17.10.2024 in nationales Recht umgesetzt haben. Nach aktuellen Planungen soll dies in Deutschland - just in time - zum 01.10.2024 erfolgen. Dies bedeutet, dass Unternehmen nur noch begrenzt Zeit haben, um ihre Prozesse und Sicherheitsmaßnahmen an die gestiegenen Anforderungen anzupassen. Übergangsfristen für die Umsetzung sieht der Entwurf des NIS2UmsuCG grundsätzlich nicht vor.

Daher sollten gegebenenfalls notwendige Maßnahmen bereits frühzeitig umgesetzt werden. Dies gilt umso mehr, als die Etablierung von entsprechenden Strukturen, die Stärkung der Resilienz der eingesetzten Systeme und weitere unternehmensinterne Schritte zur Umsetzung eines angemessenen Informationssicherheitsniveaus nicht von heute auf morgen möglich sind.

Hinweis
Dieser Überblick dient ausschließlich der allgemeinen Information und kann konkreten Rechtsrat im einzelnen Fall nicht ersetzen. Sprechen Sie bei Fragen bitte Ihre gewohnten Ansprechpartner und Ansprechpartnerin bei GÖRG bzw. den Autor Thomas Altmann unter +49 89 3090667-86 oder TAltmann@GOERG.de oder die Autorin Dr. Andrea Kirsch unter +49 30 884503-243 oder AKirsch@goerg.de an. Informationen zum Autor finden Sie auf unserer Homepage www.goerg.de.

Wir verwenden das generische Maskulinum und sehen von einer Nennung aller Geschlechtsidentitäten ab, damit dieser Text besser lesbar ist, und meinen damit ausdrücklich jeden in jeder Geschlechtsidentität.

Unsere Standorte

GÖRG Partnerschaft von Rechtsanwälten mbB

BERLIN
Kantstr. 164, 10623 Berlin
Tel. +49 30 884503-0
Fax +49 30 882715-0

HAMBURG
Alter Wall 20 - 22, 20457 Hamburg
Tel. +49 40 500360-0
Fax +49 40 500360-99

FRANKFURT AM MAIN
Ulmenstr. 30, 60325 Frankfurt am Main
Tel. +49 69 170000-17
Fax +49 69 170000-27

KÖLN
Kennedyplatz 2, 50679 Köln
Tel. +49 221 33660-0
Fax +49 221 33660-80

MÜNCHEN
Prinzregentenstr. 22, 80538 München
Tel. +49 89 3090667-0
Fax +49 89 3090667-90