Neues IT-Sicherheitsrecht – Updates in vielen Unternehmen dringend notwendig

Die CrowdStrike-Panne hat gezeigt: In Sachen Cybersicherheit in Unternehmen ist an vielen Stellen noch Luft nach oben. Die durch die Panne eingetretenen Betriebsstörungen haben bereits nach kurzer Zeit wirtschaftliche Schäden verursacht. Um solche Vorfälle möglichst zu verhindern bzw. ein effektives Vorgehen im Falle eines Cyber-Incidents sicherzustellen, wurde auf EU-Ebene Ende 2022 eine Richtlinie über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union (NIS-2-Richtlinie) beschlossen. Der Entwurf eines deutschen Umsetzungsgesetzes enthält weitreichende Pflichten für einen großen Kreis von Unternehmen. Ob dieser Entwurf vor dem Hintergrund des Ampel-Aus noch vor den Neuwahlen im Frühjahr 2025 beschlossen wird oder ob uns in der neuen Legislaturperiode ein neuer Entwurf erwartet, bleibt abzuwarten. Fest steht jedoch: Der Schutz vor Cybersicherheitsvorfällen ist auch schon jetzt wichtiger denn je. Mit einer Umsetzung der NIS-2-Richtlinie ist auch zeitnah zu rechnen, zumal die EU-Kommission wegen der verzögerten Umsetzung bereits ein Vertragsverletzungsverfahren gegen Deutschland eingeleitet hat. Mit der Vorbereitung auf neue Pflichten kann nicht früh genug begonnen werden.

Am 19. Juli 2024 führte ein fehlerhaftes Update beim Cybersicherheitsdienstleister CrowdStrike zu weltweiten Ausfällen von IT in Unternehmen. Fast 50 % der betroffenen Unternehmen mussten in der Folge ihren Betrieb zeitweise einstellen. Server sind ausgefallen, Flüge wurden gestrichen und Beschäftigte nach Hause geschickt. Die Störungen wurden teilweise als „gravierend für die deutsche Wirtschaft“ bezeichnet. Das geht aus einer Befragung einiger der betroffenen Unternehmen durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) und dem Digitalverband Bitkom hervor.

Als Reaktion auf diesen Cybersicherheitsvorfall ergriffen die befragten Unternehmen verschiedene Maßnahmen. Darunter die Erstellung bzw. Verbesserung ihres IT-Notfallplans, die

Durchführung von Schulungen aber auch technische Maßnahmen wie Updates und Backups. 20 % der Unternehmen gaben an, in Zukunft ihre Kriterien bei der Auswahl von IT-Sicherheitsanbietern zu verändern. Einzelne Unternehmen wechselten ihre IT-Sicherheitsanbieter bereits.

Nicht nur diese Crowdstrike-Panne zeigt, wie dringend in vielen Unternehmen Anpassungsbedarf beim Thema Cybersicherheit besteht. Auch der aktuelle BSI-Lagebericht 2024 hat erneut deutlich gemacht, dass die Sicherheitslage besorgniserregend ist. Aus gutem Grund werden daher bald für viele Unternehmen IT-Sicherheitsmaßnahmen gesetzlich verpflichtend. Die Umsetzung der NIS-2-Richtlinie befindet sich in Deutschland derzeit in Arbeit. Im Entwurf eines Umsetzungsgesetzes, das im Wesentlichen eine Neufassung des Gesetzes über das Bundesamt für Informationssicherheit (BSIG) ist, finden sich zahlreiche neue Sicherheitspflichten. Wesentlich ist die Sicherstellung angemessener Risikomanagementmaßnahmen, mit denen Systemstörungen vermieden und Auswirkungen von Sicherheitsvorfällen möglichst gering gehalten werden. Diese sind von der Geschäftsleitung zu überwachen. Dazu kommen Registrierungspflichten und Meldepflichten bei Sicherheitsvorfällen. Bei Verstößen drohen hohe Bußgelder.

Adressiert werden zudem insgesamt deutlich mehr Unternehmen, denn bisher richtete sich das BSIG nur an Betreiber kritischer Infrastrukturen, sog. KRITIS. In Zukunft können auch mittlere bis große Unternehmen von den Regelungen betroffen sein, sofern sie in den einschlägigen Sektoren tätig sind. Sie werden in „besonders wichtige“ und „wichtige Einrichtungen“ aufgeteilt. Neben den Sektoren spielen auch Mitarbeiterzahl sowie Jahresumsatz eine Rolle bei der Bestimmung, welche Pflichten genau gelten. Beispielsweise gelten nach dem BSIG-Entwurf Unternehmen, die in bestimmten Sektoren tätig sind, schon ab 50 Mitarbeitern oder einem Jahresumsatz von über zehn Mio. Euro als „wichtige Einrichtungen“. An dem deutlich weiteren Anwendungsbereich wird sich auch durch einen neuen Entwurf in einer neuen Legislaturperiode nichts ändern, denn diesen schreibt die NIS-2-Richtlinie verpflichtend vor. Die vielen Betroffenheitsanalysen, die wir für unsere Mandanten durchführen, zeigen eines deutlich: Es sind nicht nur Unternehmen betroffen, deren Ausfall vom Durchschnittsbürger als „gesellschaftlich kritisch“ angesehen wird. Durch die weiten

Definitionen, die auf die statistische Klassifizierung der Wirtschaftszweige abstellen, sind auch etliche in der allgemeinen Wahrnehmung als weniger kritische Bereiche eingeschätzte Sektoren erfasst, etwa alle Bereiche des Maschinenbaus oder jegliche Verwalter von IT-Systemen („Managed Service Providers“).

Sicherheitspflichten beziehen sich nun insbesondere auch auf die Lieferkette. Die Risikomanagementmaßnahmen eines von der NIS-2-Richtlinie erfassten Unternehmens müssen auch die „Sicherheit der Lieferkette“ umfassen (Art. 21 Abs. 2 lit. d) NIS-2-Richtlinie). Daher sollte sichergestellt werden, dass auch für beliefernde Unternehmen Sicherheitsanforderungen (vertraglich) geregelt werden, sog. „Cyber-Supply Chain Risk Management“.

Doch wie ist das in der Praxis umsetzbar? Primär bedarf es einer Bedarfsanalyse und der Verteilung von Zuständigkeiten im Unternehmen. Gegebenenfalls müssen vorhandene Sicherheitssysteme überarbeitet werden. Vor allem aber muss zukunftsorientiert gedacht werden: langfristige Cybersecurity-Strategien und regelmäßige Sicherheitsaudits sind unerlässlich, um die sich ständig entwickelnden rechtlichen Rahmenbedingungen einhalten zu können. Je nach Größe des Unternehmens können dabei Arbeitsgruppen erstellt, externe Berater hinzugezogen oder Rechts- und IT-Abteilungen erweitert werden. Es muss klar sein, wie im Falle von Cyberangriffen zu reagieren ist, bevor es zu einem Angriff kommt, damit schnell die notwenigen Abhilfemaßnahmen wirksam getroffen und größere Schäden verhindert werden können.

Für alle weiteren Fragen rund um das Datenschutzrecht stehen Ihnen gerne zur Verfügung

Dr. Kristina Schreiber
+49 221 65065-337
kristina.schreiber@loschelder.de

Dr. Simon Kohm
+49 221 65065-200
simon.kohm@loschelder.de

Dennis Pethke, LL.M.
+49 221 65065-337
dennis.pethke@loschelder.de

Rebecca Moßner
+49 221 65065-465
rebecca.mossner@loschelder.de

Impressum

LOSCHELDER RECHTSANWÄLTE
Partnerschaftsgesellschaft mbB
Konrad-Adenauer-Ufer 11
50668 Köln

Tel. +49 (0)221 65065-0, Fax +49 (0)221 65065-110
info@loschelder.de
www.loschelder.de