# Cybersecurity Compliance Management: Rechtliche Anforderungen an Cybersicherheit strategisch umsetzen

## Ein Beitrag von Dr. Carlo Piltz Stefan Hessel und Karin Potel

### Cybersicherheit als Chance und Risiko

Die Nutzung von digitalen Technologien ist ein zentraler Erfolgsfaktor für Unternehmen und in nahezu allen Branchen auch für ein Überleben am Markt notwendig. Dies führt zu einer zunehmenden Digitalisierung und Vernetzung von Produkten (z.B. im Bereich der IoT), aber auch von Produktionsanlagen (u.a. Industrie 4.0 oder Smart Factory). Datennutzung und -austausch sind dabei längst nicht mehr auf einzelne Unternehmen beschränkt, sondern erfolgen in zunehmendem Maß über ganze Lieferketten hinweg.

Durch die zunehmende Vernetzung steigt die Abhängigkeit der Akteure. Ein IT-Sicherheitsvorfall bei einem einzelnen Zulieferer kann die gesamte Lieferkette oder sogar die Sicherheit eines Produkts am Markt betreffen. Unternehmen sollten daher bestrebt sein, präventiv ihre Unternehmensstrukturen auf mögliche Risiken und Bedrohungen zu überprüfen und zu sichern. Die Angriffsmöglichkeiten sind dabei vielseitig. Gefahren drohen auf technischer Ebene unter anderem durch Schadsoftware, Identitätsdiebstahl, Social Engineering oder Advanced Persistent Threats, die zur gezielten Informationsgewinnung eingesetzt werden.

Doch fehlende IT-Sicherheit stellt auch auf rechtlicher Ebene wegen einer zunehmenden Regulierung ein Risiko dar. Durch immer engere Vorgaben zur Umsetzung von IT-Sicherheit können selbst bei kleineren Abweichungen – auch außerhalb des Datenschutzrechts – hohe Bußgelder oder Vertragsstrafen im Raum stehen. Kommt es tatsächlich zu einem IT-Sicherheitsvorfall, stehen darüber hinaus regelmäßig auch Gewährleistungs- und Schadensersatzansprüche von Kunden oder Betroffenen im Raum. Unternehmen, die am Markt bestehen und erfolgreich digitalisieren wollen, müssen also neben einer technischen Umsetzung auch den rechtlichen Anforderungen gerecht werden. Dies ist jedoch weit weniger einfach als gedacht, denn weder auf nationaler Ebene noch auf europäischer Ebene existiert ein einheitliches Gesetz, das allgemeine Sicherheitsanforderungen verpflichtend für Unternehmen definiert. Der rechtliche Rahmen setzt sich stattdessen aus einer Vielzahl von Einzelregelungen zusammen. Diese gelten teils allgemein für Unternehmen, teils nur für bestimmte Branchen oder Produkte.

## Cybersecurity Compliance Management reduziert rechtliche Risiken

Notwendig ist daher ein unternehmens- und produktbezogenes Cybersecurity Compliance Management, das die geltenden gesetzlichen Anforderungen und Verpflichtungen eines Unternehmens zunächst identifiziert und die anschließende Umsetzung begleitet. Teil der im Rahmen des Cybersecurity Compliance Management zu betrachtenden Vorgaben kann beispielsweise der Schutz von Geschäftsgeheimnissen und Know-how vor Wirtschaftsspionage sein. Auch hierbei gewinnt die Digitalisierung z.B. bei der Nutzung und dem Schutz von maschinengenerierten Daten an Bedeutung. Darüber hinaus drängen aktuell vermehrt IT-sicherheitsrechtliche Aspekte sowie seit der Einführung der Datenschutzgrund-Verordnung (DSGVO) Datenschutzrisiken in den Vordergrund. Nach Art. 24 Abs. 1 i.V.m. Art. 32 Abs. 1 DSGVO sind Unternehmen bei der Verarbeitung von personenbezogenen Daten dazu verpflichtet, diese angemessen zu schützen. Ein konkreter Maßnahmenkatalog wird durch die DSGVO jedoch nicht definiert, vielmehr fällt die Auswahl angemessener Maßnahmen in den Verantwortungsbereich der Unternehmen. Bedingt durch die digitale Transformation der Automobilbranche, gelten auch für Hersteller und Zulieferer immer weiter gehende Reglementierungen. Anforderungen zur IT-Sicherheit können sich darüber hinaus beispielsweise auch aus steuerrechtlichen Vorschriften wie der Abgabenordnung (AO) ergeben. Nicht zu unterschätzen sind auch mittelbare Verpflichtungen zur IT-Sicherheit, die sich beispielsweise aus Produkthaftungsansprüchen oder dem Mängelgewährleistungsrecht, das gerade eine starke Reformierung durch die Digitale-Inhalte-Richtlinie erfährt, ergeben.

Daneben finden sich abhängig von Branche oder Produkt auch spezialgesetzliche Vorgaben bei wirtschaftlichen Tätigkeiten, die an ein erhöhtes Risiko anknüpfen. Der Gesetzgeber erachtet insoweit den Schutz durch die allgemeinen Vorschriften nicht als ausreichend und verlangt daher in besonders gefährdeten Bereichen die Erfüllung von höheren Mindeststandards und kontrolliert diese enger.

Ein Beispiel hierfür sind die gesetzlichen Vorgaben für Betreiber kritischer Infrastrukturen, die nach § 8a Abs. 1 S. 1 BSIG "angemessene organisatorische und technische Vorkehrungen" zu treffen haben, soweit es sich um funktionskritische Elemente handelt. Sie unterliegen darüber hinaus gem. § 8a Abs. 3 BSIG einer engeren Kontrolle durch das Bundesamt für Informationssicherheit (BSI). Im Bereich der kritischen Infrastrukturen wird es mit dem IT-Sicherheitsgesetz 2.0, das sich derzeit im Gesetzgebungsprozess befindet, eine ganze Reihe von relevanten und weitreichenden Änderungen ergeben.

Ein weiteres Beispiel – diesmal aus dem Bereich Healthcare – sind digitale Gesundheitsanwendungen (DiGA) bzw. Gesundheits-Apps auf Rezept für die seit dem Inkrafttreten des Digitale-Versorgung-Gesetzes (DVG) am

19.12.2019 ebenfalls besondere Regelungen geschaffen wurden. DiGA bedürfen einer Genehmigung durch das Bundesinstitut für Arzneimittel und Medizinprodukte (BfArM), die nach § 139e Abs. 2 S. 2 SGB V den Nachweis erfordert, dass die digitale Gesundheitsanwendung "Datensicherheit nach dem Stand der Technik" gewährleistet. Zur näheren Bestimmung hat das Bundesministerium für Gesundheit gemäß § 139e Abs. 9 SGB V die Digitale-Gesundheitsanwendungen-Verordnung (DiGAV) erlassen. Durch die DiGAV werden die Regelungen der DSGVO, z.B. bei Datenübermittlungen in Drittländer, verschärft und über § 4 Abs. 1 DiGAV in Verbindung mit Anlage 1 umfangreiche Anforderungen zur IT-Sicherheit gestellt.

## Fazit und erste Schritte zur Cybersecurity Compliance

Aufgrund der derzeit komplizierten Rechtslage und teilweise versteckter bzw. indirekter Verpflichtungen zur IT-Sicherheit ist die Reduzierung rechtlicher Cyber-Risiken für Unternehmen eine wachsende Herausforderung. Unternehmen sollten diesem Risiko durch die Etablierung eines Cybersecurity Compliance Management begegnen. Hierfür setzen wir gemeinsam mit unseren Mandanten in der Regel die folgenden Schritte um:

- Anwendbare Gesetze und Verpflichtungen für Unternehmen und Produkt identifizieren
- Vorgaben für Cybersecurity ableiten
- Risikoabwägungen durchführen
- Einheitliches IT-Sicherheitskonzept erstellen, anpassen und dokumentieren
- Rechtliche Wechselwirkungen berücksichtigen (z.B. Meldepflichten, aber auch Geheimnisschutz)
- IT-Sicherheitskonzept rechtlich absichern (z.B. durch Vertraulichkeitsverpflichtungen, aber auch Legal Incident Response)
- Kontinuierliches Monitoring nach neuen Vorschriften (Früherkennung) und regelmäßige Kontrolle der Umsetzung

[März 2021]



**Unternehmenskontakt**: Melanie Schaumann I Head of Marketing & Communications I T > +49 30 / 2332895 0 I E melanie.schaumann@reuschlaw.de