Mit Netz und doppeltem Boden

Verordnungen sorgen für Schutz in der Informationstechnik

Jürgen H. Stroscher
Ext. Datenschutzbeauftragter (TÜV ®,UDIS zert ©)

In der heutigen digitalen Welt ist die Sicherheit im Internet von größter Bedeutung. Um Menschen, Unternehmen und Institutionen resilienter zu machen und gleichzeitig ein einheitliches Sicherheitslevel zu schaffen, hat die EU Regularien eingeführt.

Kleine und mittelständische Unternehmen (KMU) sind das Rückgrat der europäischen und das Herzstück unserer regionalen Wirtschaft. Insbesondere sie sind von den neuen EU-Regeln betroffen. Das hat sowohl schwierige als auch positive Auswirkungen. Doch wie wirken sie sich aus? Im nachstehenden Beitrag finden Sie eine Zusammenfassung der wichtigsten Neuerungen.

Kritis Verordnung und BSI-Gesetz

Die Verordnung zu Kritischen Infrastrukturen (Kritis) in Verbindung mit dem BSI Gesetz – aktuell noch im Entwurf – liefert den Rahmen für Unternehmen, die als Betreiber kritischer Infrastrukturen eingestuft werden. Der Kreis wurde im Entwurf erheblich erweitert: So können Unternehmen mit mehr als 50 Mitarbeitenden oder zehn Millionen Euro Umsatz und einer Bilanzsumme ab zehn Millionen Euro betroffen sein. Unternehmen müssen nun Maßnahmen ergreifen, um die Sicherheit und Resilienz ihrer IT-Infrastrukturen zu gewährleisten. Sicherheitsvorfälle müssen dem Bundesamt für Sicherheit (BSI) gemeldet werden, daher ist ein Zehn-Punkte-Plan für den Krisenfall notwendig. Die Einhaltung der Kritis-Standards können erhebliche Investitionen in Sicherheitstechnologien und Fachpersonal bedeuten. Kritis-Unternehmen sind zum Beispiel Anbieter digitaler Dienste, Internet Service Provider, Luftsicherheit und Unternehmen des öffentlichen Interesses.

IT-Sicherheitsgesetz 2.0

In Verbindung mit der Kritis-V soll das nationale IT-Sicherheitsgesetz 2.0 die Cybersicherheit und die Sicherheit informationstechnischer Systeme in Deutschland erhöhen. Wie genau sich das Gesetz auswirkt, hängt von der Branche ab sowie davon, ob eine Organisation als Kritis-Unternehmen oder Unternehmen im besonderen öffentlichen Interesse (UBI) eingestuft ist. Einfluss hat es dann auf die jeweiligen Meldepflichten, den Nachweis von Sicherheitsmaßnahmen sowie die Zertifizierungspflicht. On top müssen sie von ihren Zulieferern ebenfalls ein gewisses Maß an IT-Sicherheit fordern. Bei Nichteinhaltung können hohe Bußgelder verhängt werden.

NIS-2-Richtlinie

Die NIS-2-Richtlinie ist eine EU-Verordnung über die Sicherheit von Netz- und Informationssystemen. Sie zielt darauf ab, ein hohes gemeinsames Sicherheitsniveau in der EU zu schaffen. Die deutsche Realisierung soll im NIS-2-Umsetzungsgesetz geregelt werden. Auch hier ist die Kritis-Regulierung betroffen: Für etwa 30.000 Unternehmen in Deutschland steigen die Security-Pflichten.
Details zur Umsetzung werden allerdings erst dann vollständig klar sein, wenn die Richtlinie wie aktuell geplant im April 2024 verkündet wird.

Cybersecurity Act (CSA)

Mit der Umsetzung des Cybersecurity Acts (CSA) hat die EU bereits 2019 ein Zertifizierungssystem für Cybersicherheit eingeführt, das das Vertrauen in die Sicherheit von digitalen Produkten und Diensten erhöhen soll. Zudem sollen die europäische Cybersicherheitsindustrie unterstützt und die Wettbewerbsfähigkeit der EU auf dem globalen Markt verbessert werden.

Alle ausführlichen Gesetze, Verordnungen und Regularien finden Sie in unserem E-Paper.

Foto: privat

> Um Menschen, Unternehmen und Institutionen resilienter zu machen und gleichzeitig ein einheitliches Sicherheitslevel zu schaffen, hat die EU Regularien eingeführt.

KI-Verordnung

Der Artificial Intelligence Act (KI-Verordnung) regelt die Anforderungen und den Einsatz von Produkten, die sich künstlicher Intelligenz (KI) bedienen. Der Gesetzesvorschlag zielt darauf ab, den Einsatz von KI innerhalb der EU zu regulieren. Die KI-Verordnung wird ein breites Spektrum von Akteuren betreffen, die an Entwicklung, Einsatz und Nutzung von KI-Systemen in der EU beteiligt sind. Unternehmen und Organisationen, die KI-Systeme in der EU nutzen oder betreiben, müssen sicherstellen, dass sie die in der Verordnung festgelegten Anforderungen und Pflichten einhalten. KI-Systeme müssen so gestaltet sein, dass sie die Anforderungen des Datenschutzrechts einhalten. Der Verordnungsentwurf wird derzeit noch verhandelt, wann eine Einigung erreicht wird, ist noch nicht absehbar.

KI-Haftungsrichtlinie

Vor dem Hintergrund der KI-Verordnung sollten potenziell betroffene Unternehmen schon jetzt die geplante EU-KI-Haftungsrichtlinie im Blick haben, die darauf abzielt, klare Regeln für die Haftung bei Schäden durch KI festzulegen. Sie beinhaltet eine mögliche Umkehr der Beweislast, wobei Hersteller oder Betreiber von KI-Systemen nachweisen müssen, dass ihre Technologie nicht für Schäden verantwortlich ist. Die Richtlinie strebt zudem nach Transparenz und Nachvollziehbarkeit von KI-Entscheidungen, passt sich in das Produkthaftungsrecht ein und verfolgt einen risikobasierten Ansatz. Ihr Hauptziel ist es, den Verbraucherschutz zu stärken und eine einheitliche Regelung im EU-Raum zu schaffen.

Cyber Resilience Act (CRA)

Der Cyber Resilience Act (CRA) ist eine Verordnung, die im Rahmen der Bemühungen der EU zur Stärkung ihrer Fähigkeit zum Schutz vor Cyberangriffen und zur Verbesserung der Cybersicherheit entwickelt wurde. Betroffen sind alle Produktions- und Entwicklungsunternehmen.

Ausführliche Informationen und einen Event-Tipp des TechHub e.V. finden Sie auf Seite 23.

Datenschutzgrundverordnung (DSGVO)

Nicht zu vergessen ist die Datenschutzgrundverordnung (DSGVO), die im Mai 2018 in Kraft getreten ist und einen Paradigmenwechsel in der Datennutzung mit sich gebracht hat. Sie fordert von Unternehmen, die personenbezogene Daten von EU-Bürgern verarbeiten, die Einhaltung strenger Datenschutzprinzipien. Das führt zu einem bewussteren Umgang mit Datenschutz bei Unternehmen und Verbrauchern und fördert die Implementierung robuster Datenschutz- und Sicherheitsmaßnahmen. Die DSGVO bringt aber auch globale Auswirkungen mit sich, weil alle – auch nicht-europäische Unternehmen – die mit EU-Bürgerdaten arbeiten, diese Richtlinien befolgen müssen.

Die dargestellten Verordnungen und Richtlinien der Europäischen Union im Bereich Cyber- und IT-Sicherheit stellen wesentliche Schritte dar, um auf die Herausforderungen und Bedrohungen der digitalisierten Welt zu reagieren, bilden jedoch zugleich nur einen Ausschnitt der von der EU anvisierten Rechtsakte in diesen und angrenzenden Bereichen ab. Durch die Einführung dieser umfassenden Regelwerke wird nicht nur die Sicherheit und Resilienz gegenüber Cyberbedrohungen erhöht, sondern auch das Vertrauen in digitale Dienste gestärkt. Langfristig tragen diese Maßnahmen zu einem sichereren und vertrauenswürdigen digitalen Binnenmarkt bei, der die digitale Souveränität der EU stärkt und ihre Bürger schützt.

Jürgen H. Stroscher, www.drimalski.de/blog

KI untersteht übrigens genauso den allgemeinen DSGVO-Regelungen. So hat zum Beispiel ein Betroffener nach Art. 22 DSGVO das Recht, eine KI-Entscheidung durch einen Menschen überprüfen zu lassen, wenn die Entscheidung erhebliche Folgen für ihn hat.