Kritisch in jeder Hinsicht: der Referentenentwurf des IT-Sicherheitsgesetzes 2.0

Categories : Compliance, Digitalisierung, Energie, Gas, Strom, Telekommunikation, Verkehr, Wasser

Tagged as : Chief Information Security Officer, Cyber-Angriff, Cybersicherheit, Gemeinwohlrelevanz, Informationssicherheitscompliance, IT-Sicherheitsgesetzes 2.0, kritische Infrastruktur, Strafrecht, Zvilrecht

Date : 28. November 2019

Digitalisierung und Cyberkriminalität gehen oft Hand in Hand. Das zeigen die Kriminalstatistiken: 2018 wurde bei 271.864 Straftaten das Internet als Tatmittel genutzt. Wenn Cyberkriminelle ihre Attacken gegen kritische Infrastruktur richten, dann können sie damit unermessliche Schäden anrichten. Um das zu verhindern, ist der Gesetzgeber aktiv geworden. Kürzlich hat das Bundesinnenministerium (BMI) dazu einen Referentenentwurf für ein IT-Sicherheitsgesetz 2.0 vorgelegt.

Dieser gibt die Grundlage für die Ansprüche an die IT-Sicherheits-Compliance.

Schutz kritischer Infrastruktur als Compliance-Aufgabe

Als typische kritische Infrastrukturen gelten die Energieerzeugung und die Energienetzen. Dass der Roman „Blackout“ längst keine Science Fiction mehr ist, zeigen die Angriffe auf deutsche Energieversorger, wie z.B. die Stadtwerke Rosenheim (wir berichteten). Dazu kommen weitere Bereiche, deren Funktionieren für das Gemeinwohl unverzichtbar ist: Wasser, Ernährung, Informationstechnik und Telekommunikation, Gesundheit, Finanz- und Versicherungswesen, Transport und Verkehr, Staat und Verwaltung.

Wir alle sind vom Funktionieren dieser Bereiche abhängig. Ein Cyber-Angriff kann Unternehmen und deren Kunden nachhaltig beschädigen. Deshalb muss erwartet werden, dass diese Unternehmen, das ihnen Mögliche tun, um ihre Cybersicherheit zu gewährleisten. Dies ist Teil der Compliance und Managementaufgabe. Die jeweilige Führungskraft muss also im Falle eines solchen Angriffs nachweisen, alles getan zu haben, um Schäden vom Unternehmen abzuwenden. Kann sie das nicht (z.B. weil das Thema nicht in den Compliance-Strukturen abgebildet wird), kann das ernsthafte Konsequenzen haben.

Die Verantwortlichkeit für Maßnahmen zum Schutz des Unternehmens gegen Cyber-Angriffe liegt beim CEO bzw. auch beim Aufsichtsrat. Es reicht heute nicht mehr aus, einen Chief Information Security Officer (CISO) einzustellen, Aufträge in die Organisationseinheit zu geben und lediglich auf die Mitarbeiter zu vertrauen. Die juristische Entwicklung führt heutzutage zum direkten Verantwortlichen, sowohl in zivilrechtlicher wie auch in strafrechtlicher Hinsicht.

IT-Sicherheitsgesetz 2.0: Was ist „kritisch“?

Aber auch Unternehmen, die aktuell noch nicht als kritische Infrastruktur gelten, könnten es demnächst werden. Denn der Referentenentwurf des IT-Sicherheitsgesetzes 2.0 dehnt den Anwendungsbereich des Gesetzes massiv aus.

Erfasst werden soll der Bereich Medien und Kultur, die Rüstungsindustrie und alle Aktiengesellschaften, die den Status des „prime standard“ genießen, also unter § 48 der Börsenordnung der Frankfurter Wertpapierböse fallen und im DAX, MDAX, SDAX oder TecDax gelistet sind. Sie werden per se als

ökonomisch bedeutsam eingeordnet und deswegen dem Gesetz unterworfen.

Der Entwurf des IT-Sicherheitsgesetzes 2.0 adressiert damit einen Großteil der deutschen Wirtschaft. Gleichzeitig erweitert er die Handlungsmöglichkeiten des Bundesamt für Sicherheit und Informationstechnik (BSI) künftig massiv.

Dass Unternehmen, die kritische Infrastruktur bewirtschaften, in den heutigen Zeiten und unter der heutigen Sicherheitslage ein gewisses Maß an Selbstbestimmtheit aufgeben müssen und man von ihnen ein hohes Maß an Cyber-Sicherheit mehr verlangen kann, das leuchtet ein. Denn sie sind gemeinwohlrelevant. Ob das aber auch für jedes Unternehmen gilt, das „nur“ ökonomisch wichtig ist? Diese Frage zu stellen, ist ein Luxus, den die Verantwortlichen für die Informationssicherheitscompliance dann nicht mehr haben. Was dann zu berücksichtigen ist, soll aber später an dieser Stelle geklärt werden. „Bleiben Sie wachsam!“

Ansprechpartner: Prof. Dr. Ines Zenke/Dr. Christian Dessau

Experten IT-Sicherheitsgesetz: Alexander Bartsch/Nadine Voß