Positionierung des Sächsischen Verbandes für Sicherheit in der Wirtschaft (SVSW) zum

Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz)

Dresden, 24.06.2015

Ausgehend von der Zielsetzung des Bundesinnenministers Dr. Thomas de Maiziére, der anlässlich seiner Ansprache zur ersten Lesung des IT-Sicherheitsgesetzes im Deutschen Bundestag im Dezember 2014 konstatierte: „Wir wollen die deutschen IT-Systeme zu den sichersten in der Welt machen." liegt jetzt das durch den Bundestag am 12.06.2015 verabschiedete IT-Sicherheitsgesetz vor. Die abschließende Prüfung durch den Bundesrat hat lediglich formalen Charakter.

Bei dem IT-Sicherheitsgesetz handelt es sich um ein sog. Artikelgesetz, d.h. es ändert Artikel in bestehenden Gesetzen. Schwerpunktmäßig werden das BSI-Gesetz, das Atomgesetz, das Energiewirtschafts-Gesetz, das Telekommunikations-Gesetz, das Telemedien-Gesetz sowie das Bundeskriminalamts-Gesetz erweitert.

Der SVSW begrüßt diese Änderungen als ersten wichtigen Schritt, um die durch Cyberkriminalität jährlich steigenden Schäden in Deutschland kurzfristig einzudämmen und mittelfristig zu reduzieren.

Nach aktuellen Studien entsteht in Deutschland ein jährlicher Schaden von ca. 50 Mrd. € (Quelle: BITKOM, Frontal21). Jedes zweite deutsche Industrieunternehmen ist in den letzten zwei Jahren attackiert worden. Aus einer Studie von Symantec aus dem Januar 2015 folgt, dass ca. 30% aller Cyberangriffe auf Unternehmen mit bis zu 250 Mitarbeitern durchgeführt werden (Handelsblatt 16.3.2015).

Im Mittelpunkt des IT-Sicherheitsgesetzes steht der Schutz der sog. Kritischen Infrastruktur. Wesentliche Punkte sind die Meldepflicht von schweren IT-Störungen und die Verpflichtung, diese Infrastrukturen in einem zweijährigen Turnus nach Sicherheitskriterien zu überprüfen. Zusätzlich werden Anforderungen an die Infrastrukturen von TK-Anbietern und Telemediendienstleistern verschärft.

Das BSI wird mit diesem Gesetz als zentrale Behörde verankert und wandelt sich dabei von einer Beratungs- und Auskunftsbehörde (z.B. für den BSI-Grundschutz) in eine Aufsichtsbehörde, ähnlich der Bundesaufsicht für Finanzdienstleistungen. Das BSI erhält die Vollmacht, bei Ordnungswidrigkeiten Geldbußen bis zu 100.000 € zu verhängen. Zu den Ordnungswidrigkeiten zählen die Nichteinhaltung der wesentlichen Anforderungen ebenso wie das Versäumnis, angezeigte Sicherheitsmängel zu beseitigen.

Nach der Etablierung des nationalen Cyberabwehrzentrums im Juni 2011 werden dem BSI damit erheblich erweiterte Kompetenzen zugewiesen. So erhält es das Recht, sämtliche Auditierungs-, Prüfungs- und Zertifizierungsunterlagen einzusehen. Es kann die Behebung von Sicherheitsmängeln verlangen und hat dabei auch das Untersuchungsrecht sowie die Anforderungsbefugnis gegenüber IT-Herstellern.

Nachdem nun Klarheit über die Ausgestaltung des Gesetzes herrscht, ist der nächste Schritt, die neuen Anforderungen umzusetzen.

„Der SVSW sieht in den Gesetzesänderungen die Chance, durch die Formulierung von Prüfungsanforderungen den Unternehmern Klarheit über das geforderte Maß an Sicherheit zu verschaffen.“, so Klaus Hoogestraat, Vorsitzender des SVSW. „Unsere Aufgabe als Verband wird es sein, den Mittelstand bei der Umsetzung des Gesetzes gezielt zu unterstützen, und als starker Partner dafür zu sorgen, dass die Umsetzung die Unternehmen wirtschaftlich und organisatorisch nicht überfordert.“

Besonders Sachsen mit seiner überaus mittelständisch ausgeprägten Wirtschaft und zahlreichen Weltmarktführern benötigt auf Grund der eher kleinen Unternehmensgrößen praktikable, einfache aber wirkungsvolle Maßnahmen, die dem gesetzlichen Rahmen entsprechen.

„Wir werden vergleichbar der Autozulieferindustrie erleben, dass die Erhöhung des Sicherheitsniveaus in der IT auch von externen Dienstleistern, die für die Kritische Infrastruktur arbeiten, gefordert werden wird. Die Umsetzung des Gesetzes wird also weitere Kreise ziehen, als bisher angenommen.“, sagt Klaus Hoogestraat weiter.

Der SVSW rät daher auch diesen Unternehmen, sich frühzeitig um die Umsetzung von geeigneten Sicherheitsmaßnahmen zu kümmern. Nur so wird sichergestellt, dass die Unternehmen mittelfristig auf nationaler wie internationaler Ebene wettbewerbsfähig bleiben.

Stichwort „Kritische Infrastruktur – Wer gehört dazu?“

- **Informationstechnik / Telekommunikation**, z.B. Telekommunikationsprovider, Mobilfunkanbieter;
- **Gesundheit**, z.B. Krankenhäuser, Rettungsdienste
- **Ernährung**, z.B. Lebensmittelkonzerne und -händler
- **Finanzdienstleister**, z.B. Banken, Versicherungen
- **Energie**, z.B. Stadtwerke, Verteilnetzbetreiber
- **Wasser**, z.B. Wasserwerk- und Klärwerkbetreiber
- **Transport und Verkehr**, z.B. Flughafen- und Bahnbetreiber.