Zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-SiG 2.0)

Das zweite Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme, das sog. IT-SiG 2.0, trat am 28. Mai 2021 in Kraft und hat weitreichende Auswirkungen auf verschiedenste Unternehmen. So werden z.B. mehr Unternehmen unter die Definition "kritische Infrastruktur" fallen und haben daraus folgend die Pflicht sich selbst als solche zu identifizieren.

Das IT-SiG 2.0

Bei dem "zweiten Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme" handelt es sich um ein Artikelgesetz. Solche Gesetze ändern gleichzeitig mehrere andere Gesetze. Das IT-SiG wirkt sich auf insgesamt acht verschiedene Gesetze aus; unter anderem das BSI-, Atom- und Telekommunikationsgesetz. Neben der Erhöhung der Sicherheit digitaler Infrastrukturen bei KRITIS-Betreibern soll das IT-Sicherheitsgesetz somit auch Verbesserung der IT Systeme bei Bundesverwaltungen und sog. Unternehmen im besonderen öffentlichen Interesse (UNBÖFI) zur Folge haben.
Letztere sind eine Neuerung im Gesetz und bestehen aus drei verschiedenen Gruppen:

- Unternehmen die Güter gemäß §60 Abs.1 Nr. 1 und 3 AWV herstellen oder entwickeln, z.B. Rüstungsunternehmen
- Unternehmen von großer volkswirtschaftlicher Bedeutung und ihre wesentlichen Zulieferer
- Unternehmen, die mit Gefahrenstoffen der oberen Klasse gem. Störfallverordnung arbeiten

Im Bereich KRITIS zählt nun die Siedlungsabfallentsorgung als eigener KRITIS-Sektor und die Betreiber müssen die von ihnen genutzten kritischen Komponenten dem BSI anzeigen. Kritische Komponenten sind IT-Produkte in KRITIS-Anlagen, deren Ausfall die Funktion der Anlage erheblich beeinträchtigen würde. Daneben sind weitere Pflichten für die Betreiber hinzugekommen.
Das BSI ist die IT- und Cyber-Sicherheitsbehörde des Bundes, weswegen das BSI-Gesetz auch von den Änderungen des IT-SiG 2.0 betroffen ist. Das Gesetz verpflichtet das BSI dazu verschiedene Aufgaben und Befugnisse wahrzunehmen. Diese werden durch das neue IT-SiG erweitert. Zu diesen zählen unter anderem:

- die 12 monatige Verarbeitung und Speicherung von Protokolldaten zur Abwehr von Gefahren für die Kommunikationstechnik des Bundes
- Port-scans bei Schnittstellen öffentlich erreichbarem IT-Systemen des Bundes, von KRITIS-Betreibern und UNBÖFI durchzuführen
- Unternehmen selbstständig als KRITIS-Betreiber identifizieren

Was ist "kritische Infrastruktur"?

Für die Versorgung unserer Bevölkerung stellen technische Systeme und Einrichtungen eine unverzichtbare Grundlage dar. Viele Bereiche unserer Gesellschaft sind von der ununterbrochenen Funktionalität dieser abhängig. So würde beispielweise die Produktion von Lebensmitteln oder die Aufbereitung und Bereitstellung von Trinkwasser ohne moderne Technik nicht mehr funktionieren. Organisationen und Einrichtungen die unverzichtbare Dienste für unsere Bevölkerung erbringen, werden als kritische Infrastruktur (KRITIS) bezeichnet. Diese werden in 10 KRITIS-Sektoren (vorher 9) eingeteilt.

Die Verordnung zur Bestimmung kritischer Infrastrukturen (BSI-KritisV) greift diese Sektoren auf und definiert betroffene Anlagen sowie Schwellenwerte, die überschritten werden müssen, um als KRITIS eingestuft zu werden. Die Betreiber der kritischen Infrastrukturen sind zur Einhaltung von Sicherheitsstandards verpflichtet, welche sich aus dem IT-SiG 2.0 ergeben.
Ziel der KRITIS-Einstufung ist die Erhöhung der Widerstandsfähigkeit gegen Bedrohungen. Mögliche Versorgungsengpässe sollen so verhindert und die öffentliche Sicherheit gewährleistet werden.

Zusätzliche und neue Pflichten der Unternehmen

KRITIS-Betreiber

Die KRITIS-Betreiber unterliegen neuen zusätzlichen Pflichten. Neben der Pflicht kritische Komponenten dem BSI anzuzeigen, ist es nun obligatorisch die sog. Garantieerklärung der Vertrauenswürdigkeit des Herstellers einzuholen und dem BSI vorzulegen, um kritische Komponenten einsetzen zu dürfen. Hierbei ist zu beachten, dass es dem BSI in bestimmten Fällen erlaubt ist, den Einsatz kritischer Komponenten zu untersagen.
Zudem ist die Angriffserkennung neuerdings verpflichtend für KRITIS-Betreiber. Dies bedeutet, dass technische und organisatorische Sicherheitsvorkehrungen getroffen werden müssen, die Bedrohungen im laufenden Betrieb anhand von Mustern erkennen und vermeiden.
Der zweite Referentenentwurf der BSI-Kritisverordnung stellt außerdem ein deutliches Absenken mehrerer Schwellenwerte, sowie die Einstufung vieler weiterer Anlagen als kritisch in Aussicht. Dies würde eine merkliche Zunahme der Unternehmen zur Folge haben, die unter die kritische Infrastruktur fallen.

UNBÖFI

Unternehmen des besonderen öffentlichen Interesses werden durch das IT- Sicherheitsgesetz dazu verpflichtet, sich eigenständig als solches zu identifizieren und folglich auch bei dem BSI zu registrieren. Im Rahmen der Meldung ist eine Selbsterklärung erforderlich, die unteranderem eine Zertifizierung für IT-Sicherheit (beispielweise durch die ISO 27001 oder den BSI IT-Grundschutz) nachweist. Des weiteren sind Nachweise über regelmäßige Audits sowie die Implementierung von Sicherheitsmaßnahmen durch die Unternehmen zu erbringen. Ausgenommen von der Registrierung sowie Übermittlung einer Selbsterklärung sind Unternehmen der oberen Klasse der Störfallverordnung.
Eine weitere Pflicht stellt das unverzügliche Melden von Sicherheitsvorfällen dar.

Diese Neuerungen werden für die betroffenen Unternehmen zu Handlungsbedarf führen.

Hinsichtlich des IT-SiG 2.0 und dem aus ihm resultierenden Handlungsbedarf beraten wir Sie gern!

IFIS-FR
Inh. Dipl.-Ing. (FH) Bernd Frenz
Im Finigen 6
28832 Achim

E-Mail: anfrage@ifis-fr.de
Fon: +49 (0) 4202 95 411 47
Fax: +49 (0) 4202 95 411 48