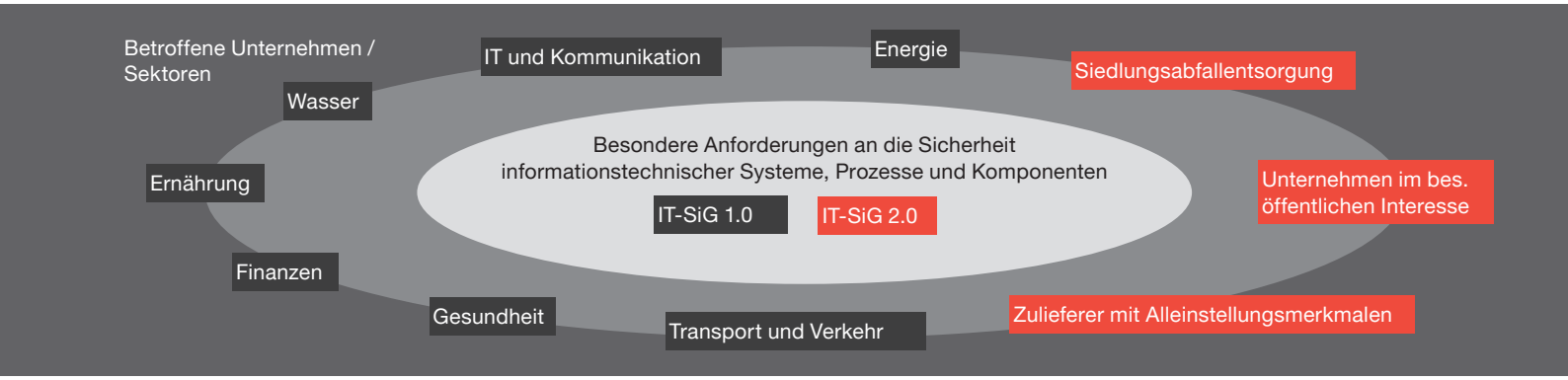
IT-Sicherheitsgesetz 2.0: Ein Paukenschlag mit Ansage – nicht nur für KRITIS-Betreiber

Auf einen Blick: Warum nun dringender Handlungsbedarf für Unternehmen besteht

Executive Summary

- Das **IT-Sicherheitsgesetz 2.0** verfolgt das Ziel die IT-Systeme und digitalen Infrastrukturen Deutschlands sicherer zu machen. Ein Fokus dabei ist der Schutz der Bevölkerung vor dem Ausfall kritischer Infrastrukturen.
- Das IT-SiG 2.0 ist ein **Artikelgesetz**, das neben dem BSI-Gesetz auch das Energiewirtschaftsgesetz, das Telemediengesetz und weitere Gesetze ändert und ergänzt.
- Das IT-SiG 2.0 wurde am 07. Mai 2021 durch den Bundesrat verabschiedet, am 18. Mai durch den Bundespräsidenten unterzeichnet und am **27. Mai 2021 im Bundesgesetzblatt verkündet**. Weitere Spezifizierungen der konkreten Anforderungen werden folgen.
- Sofern Unternehmen im Geltungsbereich des Gesetzes liegen, sind sie mit einer sehr kurzen **Umsetzungsfrist der Anforderungen von nur einem Tag** konfrontiert.
- Neben der **Definitionserweiterung betroffener Unternehmen** führt zudem die **Absenkung** einiger **Schwellenwerte** zur Beurteilung kritischer Anlagen dazu, dass mehr Unternehmen im Geltungsbereich des Gesetzes liegen.
- Eine Neuheit ist, dass nun auch kleinere Unternehmen mit den Anforderungen des Gesetzes konfrontiert sein können, sofern sie in **besonderen Zuliefererbeziehungen** zu KRITIS Unternehmen oder Unternehmen im besonderen öffentlichen Interesse stehen.
- Zudem wurde die Anzahl der Tatbestände sowie die Höhe der **Bußgelder** (bis zu 2 Mio. EUR) erhöht.
- Es besteht **dringender Handlungsbedarf** für Unternehmen. Diese müssen nun prüfen, ob sie aufgrund ihrer Anlagen oder Verflechtungen der Wertschöpfungsketten die KRITIS Anforderungen erfüllen müssen und, falls zutreffend, welche akuten Anpassungserfordernisse bestehen.



Die Kernverpflichtungen für Unternehmen im Überblick

Im Kern fordert das IT-SiG 2.0 die Einführung eines Informationssicherheits-Managementsystems (ISMS) sowie die regelmäßige Auditierung dieses Systems durch eine unabhängige, zugelassene Stelle. Welche Anforderungen Unternehmen, die neu im Geltungsbereich des Gesetzes sind, konkret erfüllen müssen, wird durch weitere Rechtsverordnungen spezifiziert.

1. Organisatorische und technische Vorkehrungen zum Schutz der IT-Systeme, Komponenten, Prozesse
2. IT „Stand der Technik“ (Sicherheitskennzeichen, etc.)
3. Bidirektionale Meldewege zum BSI: Einrichtung einer Kontaktstelle
4. Angriffserkennungssysteme
5. Meldepflicht bei erheblichen Störungen der Leistungserbringung
6. Anzeigepflicht bei Einsatz kritischer Komponenten an das Bundesamt für Sicherheit in der Informationstechnik
7. Vertikalverantwortung für Zulieferer
8. Auditierung alle zwei Jahre

pwc

IT-Sicherheitsgesetz 2.0: Kopfschmerzen durch Compliance?

Wer ist betroffen?

I. KRITIS-Sektor Siedlungsabfallentsorgung
Die hier betroffenen Anlagen zur Sammlung, Beseitigung und Verwertung sowie die entsprechenden Schwellenwerte sind noch offen.

II. Unternehmen im besonderen öffentlichen Interesse (UNBÖFI)
Dies sind Unternehmen, die nicht Betreiber kritischer Infrastrukturen sind, jedoch als besonders schützenswert gelten und daher besondere Maßnahmen umzusetzen haben. Es handelt sich um drei Kategorien:

1. Rüstung, Waffen und Verschlusssachen-IT nach Außenwirtschaftsverordnung (AWV).
2. UNBÖFI welche von volkswirtschaftlicher Bedeutung sind und aufgrund ihrer inländischen Wertschöpfung zu den größten Unternehmen gehören (Top 100). Hier bleibt noch die entsprechende Rechtsverordnung abzuwarten an der sich entsprechende Kriterien und der relevante Geltungsbereich ableiten lassen.
3. UNBÖFI die in den Bereich der Gefahrstoffe fallen (Unternehmen die unter die Störfallverordnung fallen, respektive Betriebsbereiche der oberen Klasse).

III. Unternehmen die vorher nicht KRITIS relevant waren es aber aufgrund von niedrigeren Schwellenwerten jetzt sind
Energie Stromerzeugung, Informationstechnik und Telekommunikation Housing, IT-Hosting IXP, Transport und Verkehr Luftverkehr

IV. Neue KRITIS relevante Anlagen in den Sektoren Energie
Gastransport und -speicherung, Gashandel, Rohölförderung und Rohölproduktenherstellung, Mineralölförderung, Anlagen zur Steuerung in der Fernwärmeversorgung, Gesundheit Labor, Transport und Verkehr Luftverkehr, See- und Binnenschifffahrt, Informationstechnik und Telekommunikation Steuerung von Domains, Finanzen und Versicherungen Einbringung von Aufträgen in den Handel

V. Zulieferer
Wenn sie von wesentlicher Bedeutung für KRITIS-Betreiber oder für UNBÖFI sind.

Wie kann PwC unterstützen?

Scoping: Ermittlung, ob und welche Bereiche der Gesellschaft durch das IT-SiG 2.0 betroffen sind.

GAP-Analyse & Aufbau ISMS: Review bestehender Sicherheitsmaßnahmen und Begleitung des Aufbau eines Informationssicherheit-Managementsystems

ISMS-Zertifizierung: Zertifizierungs-Audit, ggf. mit anschließender Zertifizierung zur Nachweiserbringung gegenüber dem BSI.

Warum PwC?

> 400 Experten bei PwC Cyber Security & Privacy in Deutschland

Führende Beratungs- und Prüfungsgesellschaft für Cyber Security (Forrester Wave 2019).

PwC ist zertifizierter IT-Sicherheitsdienstleister des Bundes.

PwC ist Unterstützer des BSI in der Entwicklung von Standards.

PwC Mitarbeiter sind aktive Mitglieder der DIN Arbeitskreise.

Vereinbaren Sie mit unseren Experten ein Erstgespräch:

Derk Fischer
Partner
Cyber Security & Privacy
Tel.: +49 211 981-2192
derk.fischer@pwc.com

Joachim Mohs
Partner
Cyber Security & Privacy
Tel.: +49 40 6378-1838
joachim.mohs@pwc.com

Hendrik Gollnisch
Manager
Cyber Security & Privacy
Tel.: +49 30 2636-1500
hendrik.gollnisch@pwc.com