THE AUDIT COMPANY

KRITIS – Kritische Infrastrukturen

IT-Sicherheitsgesetz und BSI-KritisV gemäß §8a BSIG

Das Bedrohungspotenzial aus dem Cyberraum ist beträchtlich. Besonders anfällig sind so genannte Kritische Infrastrukturen (KRITIS). Hier hätte ein Ausfall oder eine Beeinträchtigung der Versorgungsdienstleistungen dramatische Folgen für Wirtschaft, Staat und Gesellschaft.

Als wichtigste Grundlage zum Schutz gilt das **IT-Sicherheitsgesetz***, das zum 25. Juli 2015 in Kraft getreten ist. Mit diesem Gesetz wird u. a. das Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz/BSIG) ergänzt.

Zur Umsetzung des IT-Sicherheitsgesetzes ist am 3. Mai 2016 der erste Teil der Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (**BSI-Kritisverordnung – BSI-KritisV**) in Kraft getreten, der Organisationen aus den Sektoren **Energie, Wasser, Informationstechnik und Telekommunikation** sowie **Ernährung** betrifft. Mit der seit 30. Juni 2017 vorliegenden **Änderungsverordnung BSI-KritisV** wird die Vorgabe des § 10 BSIG nunmehr abschließend umgesetzt. Sie bestimmt transparente Kriterien, anhand derer Betreiber Kritischer Infrastrukturen aus den Sektoren **Gesundheit, Finanz- und Versicherungswesen sowie Transport** und **Verkehr** prüfen können, ob sie unter die Regelungen des IT-Sicherheitsgesetzes fallen und somit von der Umsetzung betroffen sind. Daneben wurden erforderliche Ergänzungen und Klarstellungen zu den bereits getroffenen Festlegungen aus dem ersten Teil der BSI-KritisV vorgenommen.

Die Änderungen der BSI-KritisV ergänzen den bisherigen Teil 1 der Verordnung. Nun werden für sieben der neun KRITIS-Sektoren objektive Schwellenwerte bestimmt, ab denen für Betreiber und Anlagen Nachweispflichten gemäß **§ 8a des BSIG** gegenüber dem BSI gelten.

Das BSIG bestimmt in § 8a, dass Betreiber Kritischer Infrastrukturen ihre kritischen IT-Systeme, IT-Komponenten und IT-Prozesse durch angemessene Vorkehrungen nach dem Stand der Technik gegen Störungen der Verfügbarkeit, Vertraulichkeit, Authentizität und Integrität schützen müssen. Zudem müssen sie dem BSI eine Kontaktstelle benennen und erhebliche Störungen ihrer IT melden (§ 8b), sofern diese Auswirkungen auf die Verfügbarkeit kritischer Dienstleistungen haben.

Die Erfüllung der Anforderungen nach § 8a muss von den betroffenen Betreibern mindestens alle zwei Jahre gegenüber dem BSI nachgewiesen werden. Der Nachweis kann durch die Einführung und die Prüfung sogenannter „**B**ranchen**s**pezifische **S**icherheits**s**tandards“ (B3S) erfolgen, die von KRITIS-Betreibern und ihren Verbänden erarbeitet werden können.

Es ist davon auszugehen, dass sich betroffene Betreiber nach den entsprechenden Branchenstandards prüfen lassen – und von der „prüfenden Stelle“ Nachweise über deren Kompetenz verlangen. Eine reine ISO 27001-Zertifizierung ist nicht ausreichend, da hierbei die branchenspezifischen Anforderungen fehlen.

Für die „prüfende Stelle“ und deren Auditoren empfiehlt das BSI eine sogenannte „**Spezielle Prüfverfahrens-Kompetenz für §8a BSIG**“ als Nachweis der eingesetzten Auditoren und Experten. Die DQS GmbH ist als Prüfstelle anerkannt; eine Reihe ihrer Auditoren haben diese Prüfverfahrenskompetenz nach § 8a BSIG bereits nachgewiesen und sind beim BSI gelistet.

(https://www.bsi.bund.de/DE/Themen/Industrie_KRITIS/IT-SiG/Was_tun/Nachweise/Liste_Pruefer/Liste_Pruefer.html)

Sprechen Sie mit uns.
Wir stehen Ihnen gern zur Verfügung:

André Säckel
DQS Produktmanager
informationssicherheit@dqs.de

** IT-SiG: Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme*

THE AUDIT COMPANY

Kritische Infrastrukturen nach Sektoren und Fristen

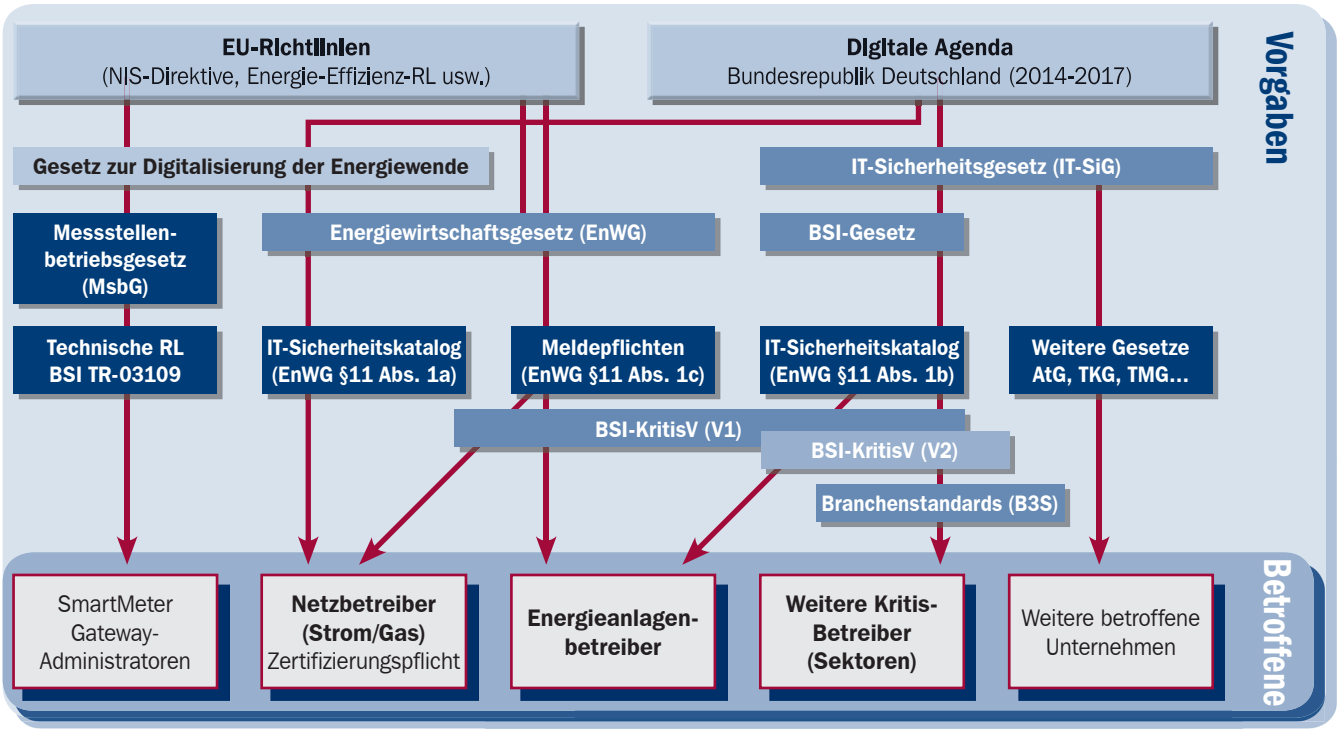
Sektoren	Bereiche	BSI-KritisV	Frist gemäß BSI-KritisV
Energie	Elektrizität, Gas, Mineralöl	Teil I vom 3. Mai 2016	Mai 2018*
Informationstechnik und Telekommunikation	Informationstechnik und Telekommunikation	Teil I vom 3. Mai 2016	Mai 2018*
Wasser	öffentliche Wasserversorgung, öffentliche Abwasserbeseitigung	Teil I vom 3. Mai 2016	Mai 2018*
Ernährung	Ernährungswirtschaft, Lebensmittelhandel	Teil I vom 3. Mai 2016	Mai 2018*
Finanz- und Versicherungswesen	Banken, Börsen, Versicherungen, Finanzdienstleister	Änderungsverordnung vom 30. Juni 2017	Juni 2019**
Gesundheit	medizinische Versorgung, Arzneimittel und Impfstoffe, Labore	Änderungsverordnung vom 30. Juni 2017	Juni 2019**
Transport und Verkehr	Luftfahrt, See- und Binnenschifffahrt, Straßen- und Schienenverkehr, Logistik	Änderungsverordnung vom 30. Juni 2017	Juni 2019**
Staat und Verwaltung	Regierung und Verwaltung, Parlament, Justizeinrichtungen, Notfall-/Rettungswesen inkl. Katastrophenschutz		
Medien und Kultur	Rundfunk, gedruckte / elektronische Presse, Kulturgut, symbolträchtige Bauwerke		

Quelle: www.bsi.de

* *Mai 2018:* *Betroffene Unternehmen aus dem ersten Korb haben zwei Jahre nach Veröffentlichung der BSI-KritisV Zeit nachzuweisen, dass sie ihre IT nach dem Stand der Technik angemessen abgesichert haben.*

** *Juni 2019:* *Betroffene Unternehmen aus dem zweiten Korb haben zwei Jahre nach Veröffentlichung der Änderungsverordnung (BSI-KritisV (2)) Zeit nachzuweisen, dass sie ihre IT angemessen nach dem Stand der Technik abgesichert haben.*

Gesetzliche Grundlagen



BSI-KritisV

Schwellenwerte für Korb 2

Die Verordnung zur Bestimmung Kritischer Infrastrukturen (BSI-KritisV) nach dem BSI-Gesetz legt fest, welche Organisationen und Anlagen in Deutschland als Kritische Infrastrukturen gelten und besonders schützenswert sind. Es handelt sich dabei um Einrichtungen und Organisationen mit wichtiger Bedeutung für das staatliche Gemeinwesen. Das IT-Sicherheitsgesetz verpflichtet deren Betreiber, Sicherheitsstandards zum Schutz der IT-Systeme, IT-Komponenten und IT-Prozesse einzuführen, um durch angemessene Vorkehrungen unempfindlich gegenüber Störungen der Verfügbarkeit, Vertraulichkeit, Authentizität und Integrität zu sein.

Es geht dabei um branchenübliche Maßnahmen bis hin zur nachhaltigen Implementierung geeigneter Strukturen in das Managementsystem, beispielsweise nach ISO/IEC 27001. Der erste Teil der BSI-KritisV, der sogenannte Korb 1, ist Anfang Mai 2016 in Kraft getreten und legt die Schwellenwerte für die Sektoren Energie, Informationstechnik und Telekommunikation, Wasser, Ernährung sowie Medien und Kultur fest. Mit der seit 30. Juni 2017 vorliegenden Änderungsverordnung zur BSI-KritisV wird die Vorgabe des §10 BSI-Gesetzes nunmehr abschließend umgesetzt. Sie bestimmt die Schwellenwerte für die Sektoren aus Korb 2: Gesundheit, Transport/Verkehr sowie Finanzen/Versicherungen. Angaben zum Sektor Staat und Verwaltung stehen nach wie vor aus.

Betreiber Kritischer Infrastrukturen haben zwei Jahre Zeit, die vom Gesetz definierten Anforderungen zu erfüllen. Stichtag für die Umsetzung aus Korb 2 ist der 30. Juni 2019. Davon ausgenommen ist das Einrichten der Meldestelle und deren Benennung beim BSI, das bis zum 31. Dezember 2017 erfolgt sein muss. Bei Nichterfüllung der definierten Anforderungen sind Bußgelder bis zu einer Höhe von 100.000 Euro für das verantwortliche Management möglich. Entsprechende Umsetzungsnachweise können durch Sicherheitsaudits, Prüfungen oder Zertifizierungen erfolgen. Dafür sind entweder anerkannte Normen und Standards oder alternativ vom Bundesamt für Sicherheit in der Informationstechnik (BSI) anerkannte branchenspezifische Standards (B3S) zugelassen.

Als beim BSI gelistete prüfende Stelle haben sowohl die DQS GmbH als auch deren ISMS-Auditoren die „Prüfverfahrenskompetenz nach § 8a BSIG“ nachgewiesen.

BSI-KritisV, Korb 2

Betreiber Kritischer Infrastrukturen aus Korb 2 können anhand der festgelegten Schwellenwerte prüfen, ob sie unter die Regelungen des IT-Sicherheitsgesetzes fallen und somit von der Umsetzung betroffen sind. Auszug:

Schwellenwerte Finanzen/Versicherungen

- *Autorisierungssysteme für Bargeldabhebungen und Systeme zur Anbindung an ein Autorisierungssystem: > 15 Mio. Transaktionen/Jahr*
- *Clearing- und Settlement-Systeme: > 18 Mio. Transaktionen/Jahr*
- *Kontoführungssysteme: > 15 Mio. Transaktionen/Jahr*
- *Cash-Center und Systeme zur Bargeldlogistik: > 93,5 Mio. Banknoten/Jahr*
- *Kartengestützter Zahlungsverkehr: > 21 Mio. Transaktionen/Jahr*
- *Konventioneller Zahlungsverkehr: > 100 Mio. dienstleistungsbezogene Transaktionen/Jahr*
- *Systeme zur Verrechnung und Abwicklung von Wertpapier- und Derivat-Geschäften: > 850.000 Transaktionen/Jahr*
- *Systeme in Verbindung mit Lebensversicherungen: > 500.000 Leistungsfälle/Jahr*
- *Systeme in Verbindung mit Krankenversicherungen: > 2 Mio. Leistungsfälle/Jahr*

Schwellenwerte Transport/Verkehr

- *Abfertigungsanlagen und Flughäfen: > 20 Mio. Passagiere/Jahr bzw. 750.000 t Fracht/Jahr*
- *Flugsicherung und Luftverkehrskontrolle: > 17.500 Flugbewegungen/Jahr*
- *Güter- und Zugbildungsbahnhöfe: > 23.000 Züge/Jahr*
- *Schienennetze, Stellwerke und Leitzentralen im ÖSPNV: > 125 Mio. beförderte Personen/Jahr oder > 500.000 Einwohner in der überwachten Region*
- *Logistikzentren und Umschlaganlagen: > 17 Mio. t Güter/Jahr*

Schwellenwerte Gesundheit

- *Krankenhäuser: > 30.000 stationäre Patienten/Jahr*
- *Medizinprodukte (Produktionsstätten/Abgabestellen): > 90,6 Mio. Euro Umsatz/Jahr*
- *Produktionsstätten, Betriebs-/Lagerräume, Vertriebsanlagen für verschreibungspflichtige Arzneien und Apotheken: > 4,65 Mio. Packungen/Jahr*
- *Labore, Transport- und Kommunikationssysteme zur Auftrags-/Befundübermittlung: > 1,5 Mio. Aufträge/Jahr*
- *Blutspende-Einrichtungen: > 34.000 Produkte/Jahr*

informationssicherheit@dqs.de