xmera

September 2017

IT-SICHERHEITSGESETZ ENERGIEVERSORGER & NEUREGELUNG

Ein umfassender Überblick über das IT-Sicherheitsgesetz einschließlich der aktuellen Neuregelung, den Pflichten, Rechten und drohenden Konsequenzen bei Pflichtverletzungen als Energieversorger

Inhaltsverzeichnis

Abbildungs- und Tabellenverzeichnis

Einleitung

Bereits 2015 trat das IT-Sicherheitsgesetz in Kraft. Seit dem nimmt das Thema IT-Sicherheit auch bei Energieversorgern Fahrt auf.

Gesetze, Verordnungen und Richtlinien regeln welche Energieversorger in den Regelungsbereich des IT-Sicherheitsgesetzes fallen. Hier den Überblick zu behalten ist mitunter gar nicht so einfach. Zudem wurden mit der letzten Neuregelung im Rahmen der NIS-Richtlinie, die am 30. Juni 2017 umgesetzt wurde, die Anforderungen an Energieversorger nochmals verschärft.

Diese Broschüre gibt Ihnen einen umfassenden Überblick über das IT-Sicherheitsgesetz einschließlich der aktuellen Neuregelungen, über Ihre Rechte und Pflichten und Konsequenzen bei Pflichtverletzungen als Energieversorger sowie über die relevanten Rechtsvorschriften.

Was ist das IT-Sicherheitsgesetz?

Eine formale Einordnung

Das Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme, bekannt als IT-Sicherheitsgesetz (IT-SiG), ist kein gewöhnliches Gesetz.

Das Besondere am IT-Sicherheitsgesetz ist, dass es ein Mantelgesetz ist. Mantelgesetze ändern andere Gesetze, schaffen sie neu oder heben sie auf. Dazu bedienen sie sich einer genau festgelegten Änderungstechnik, die über einen Änderungsbefehl einzelne Wörter, Satzteile oder Sätze verändert. Erst, wenn Sie die Änderungen mit dem bisherigen Wortlaut des Stammgesetzes vergleichen, ist es möglich die Auswirkungen des Mantelgesetzes zu verstehen.[1]

Wegen seines artikelorientierten Aufbaus wird das Mantelgesetz auch gerne Artikelgesetz genannt.

Eine inhaltliche Betrachtung

Das IT-Sicherheitsgesetz fasst alle Änderungen von Stammgesetzen, die an das Thema IT-Sicherheit angepasst werden sollen, zusammen. Für jedes betroffene Stammgesetz gibt es einen eigenen Artikel, in dem die Änderungen beschrieben werden.

Somit besteht das IT-Sicherheitsgesetz aus elf Artikeln. Davon beschreiben neun Artikel die Änderungen in acht Stammgesetzen.

[1] Vgl. Bundesministerium der Justiz (2008).

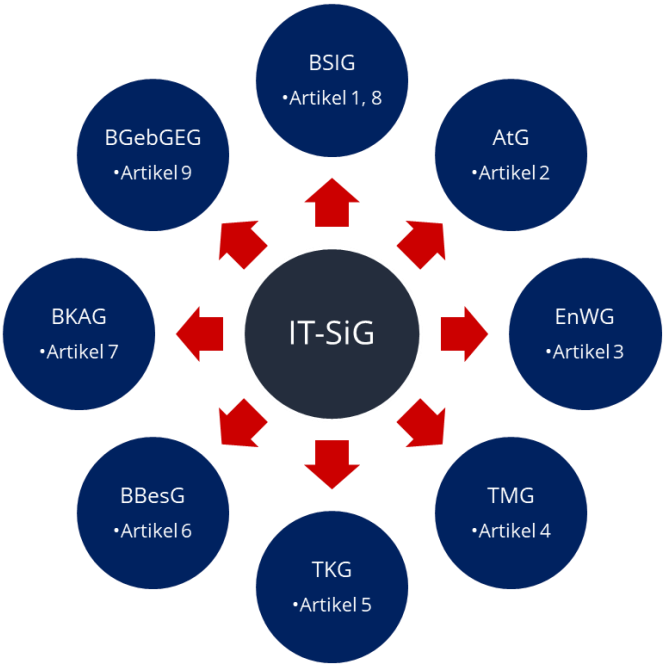

Abbildung 1: Im IT-Sicherheitsgesetz enthaltene Stammgesetze.

Die betroffenen Gesetze sind das BSI-Gesetz (BSIG), Atomgesetz (AtG), Energiewirtschaftsgesetz (EnWG), Telemediengesetz (TMG), Telekommunikationsgesetz (TKG), Bundesbesoldungsgesetz (BbesG), Bundeskriminalamtgesetz (BKAG) und das Gesetz zur Strukturreform des Gebührenrechts des Bundes (BGebGEG).

Die übrigen Artikel (10 und 11) regeln die Evaluierung einzelner Änderungen und das Inkrafttreten des Gesetzes selbst.

Was möchte der Gesetzgeber mit dem IT-Sicherheitsgesetz erreichen?

IT-Sicherheit als Pflicht im Zuge der Digitalisierung

Das IT-Sicherheitsgesetz ist das erste konkrete Ergebnis der Digitalen Agenda 2014 der Bundesregierung, die die strategischen Ziele der Cyber-Sicherheitsstrategie für Deutschland, festgelegt in 2011, verfolgt.

Mit Voranschreiten der Digitalisierung entstehen nicht nur Freiräume. In allen Bereichen der Gesellschaft wächst gleichzeitig auch die Abhängigkeit von informationstechnischen Systemen. Computer und Internet sind nicht mehr wegzudenken. Sie sind wertvolle Ressourcen, die wir schützen müssen.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) analysiert seit Jahren die Bedrohungssituation dieser Ressourcen. Angriffe im Cyberraum erfolgen demnach zielgerichteter, technologisch ausgereifter und komplexer.[2]

[2] Vgl. Die Bundesregierung der Bundesrepublik Deutschland (2015).

Mindestschutzniveau für besonders schutzbedürftige Strukturen

Das IT-SiG hat zum Ziel die Sicherheit informationstechnischer Systeme zu verbessern. Dazu hat es ein besonderes Augenmerk auf den Schutz von IT-Infrastrukturen, die sich als unverzichtbare Lebensadern unserer modernen und leistungsfähigen Gesellschaft darstellen.

IT-Infrastrukturen der Sektoren Energie, Wasser, Informationstechnik und Telekommunikation, Ernährung, Gesundheit, Finanz- und Versicherungswesen, Transport und Verkehr, Medien und Kultur sowie Staat und Verwaltung sind besonders kritisch für die Gesellschaft und damit auch besonders schutzbedürftig.

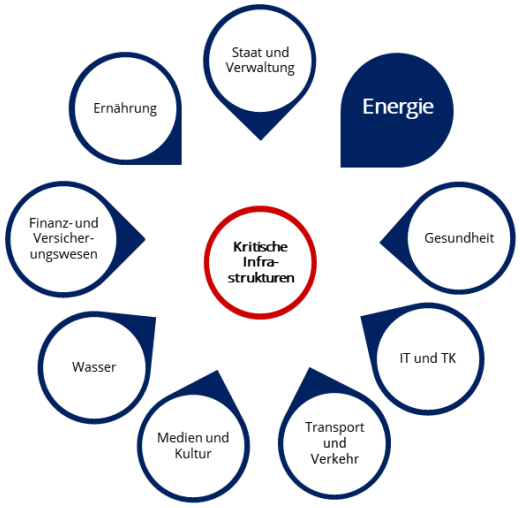

Abbildung 2: Kritische Infrastrukturen.

Das IT-Sicherheitsniveau der sogenannten Kritischen Infrastrukturen ist sehr verschieden.[3] Um hier einen einheitlichen Standard gewähren zu können, verpflichtet das IT-Sicherheitsgesetz Betreiber Kritischer Infrastrukturen dazu ein Mindestniveau an IT-Sicherheit einzuhalten und IT-Sicherheitsvorfälle zukünftig zu melden.

Welchen Einfluss hat die NIS-Richtlinie auf die Regelungen zur IT-Sicherheit?

Die NIS-Richtlinie ist eine EU-Richtlinie. Sie fordert Maßnahmen zur Stärkung der Cyber-Sicherheit in der europäischen Union.

Dazu soll der Aufbau nationaler Kapazitäten für die Cyber-Sicherheit gefördert werden. Mitgliedsstaaten sollen intensiver zusammenarbeiten. Für Kritische Infrastrukturen und Anbieter digitaler Dienste werden Mindestsicherheitsanforderungen und eine Meldepflicht bestimmt.

[3] Vgl. Die Bundesregierung der Bundesrepublik Deutschland (2015).

Die NIS-Richtlinie ist am 8. August 2016 in Kraft getreten. Bis zum 10. Mai 2018 muss sie in nationales Recht umgesetzt worden sein.

Aufgrund des seit Juli 2015 bestehenden IT-Sicherheitsgesetzes waren viele der Forderungen der NIS-Richtlinie in Deutschland bereits erfüllt. Mit dem NIS-Richtlinien-Umsetzungsgesetz konnte daher die EU-Richtlinie schon am 30. Juni 2017 umgesetzt werden.

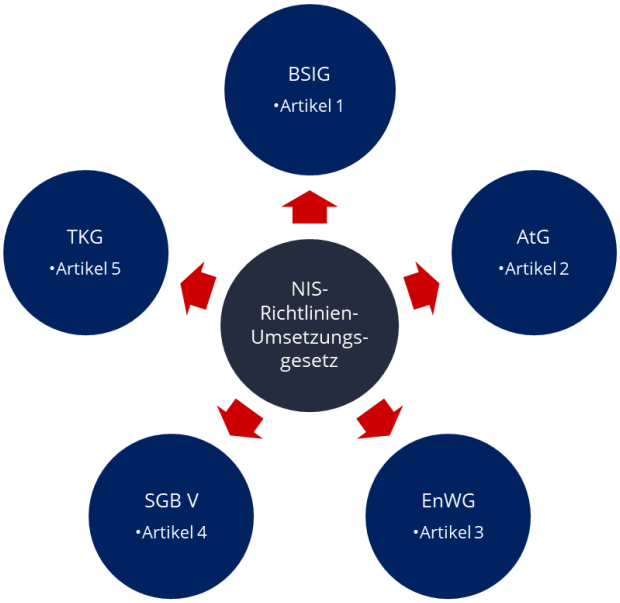

Abbildung 3: Im NIS-Richtlinien-Umsetzungsgesetz enthaltene Stammgesetze.

Das NIS-Richtlinien-Umsetzungsgesetz ändert das BSI-Gesetz (BSIG), Atomgesetz (AtG), Energiewirtschaftsgesetz (EnWG), Fünfte Buch des Sozialgesetzbuches (SGB V) und Telekommunikationsgesetz (TKG).

Die NIS-Richtlinie wurde am 19. Juli 2016 im Amtsblatt der Europäischen Union veröffentlicht. Das NIS-Richtlinien-Umsetzungsgesetz wurde am 29. Juni 2017 im Bundesgesetzblatt veröffentlicht.

Beide Rechtstexte können Sie in der xmera : library downloaden.

Die durch die NIS-Richtlinie entstandenen Neuregelungen für den Energiesektor wurden bei allen weiteren Ausführungen in diesem Beitrag berücksichtigt.

An wen richtet sich das IT-Sicherheitsgesetz?

Der Gesetzgeber spricht mit dem IT-Sicherheitsgesetz vier Adressaten an: Betreiber Kritischer Infrastrukturen, Betreiber von Webangeboten, Telekommunikationsunternehmen und das Bundesamt für Sicherheit in der Informationstechnik.

Nicht alle Unternehmen der obigen Sektoren zählen automatisch zu den Kritischen Infrastrukturen (KRITIS). In der Rechtsverordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-KritisV), die in ihrer ersten Fassung am 3. Mai 2016 in Kraft getreten ist, wird anhand von quantitativen Kriterien festgelegt, welche Unternehmen als Kritische Infrastruktur eingestuft werden. Einschätzungen zu Folge werden ca. 2.000 Unternehmen betroffen sein.

Zu den Betreibern von Webangeboten gehören Online-Marktplätze, Online-Suchmaschinen und Cloud-Computing-Dienste. Telekommunikationsunternehmen nehmen eine besondere Rolle ein, da sie durch ihre Dienste den Zugang zum Internet ermöglichen. Das Bundesministerium für Sicherheit in der Informationstechnik ist Hauptakteuer in Sachen IT-Sicherheit in der Bundesrepublik und erhält zusätzliche Befugnisse und Pflichten.

Welche Energieversorger sind vom IT-Sicherheitsgesetz betroffen?

Für fast Alles benötigen wir Energie in Form von Strom, Wärme oder Treibstoff. Der Kritis-Sektor Energie umfasst daher die Bereiche Strom, Gas, Kraftstoff/Heizöl und Fernwärme.

Als Energieversorgung versteht die BSI-KritisV nahezu alle Stufen der energiewirtschaftlichen Wertschöpfungskette. Dazu gehören die Stufen Erzeugung/Förderung, Speicherung/Lagerung, Handel, Transport, Verteilung und Messung.

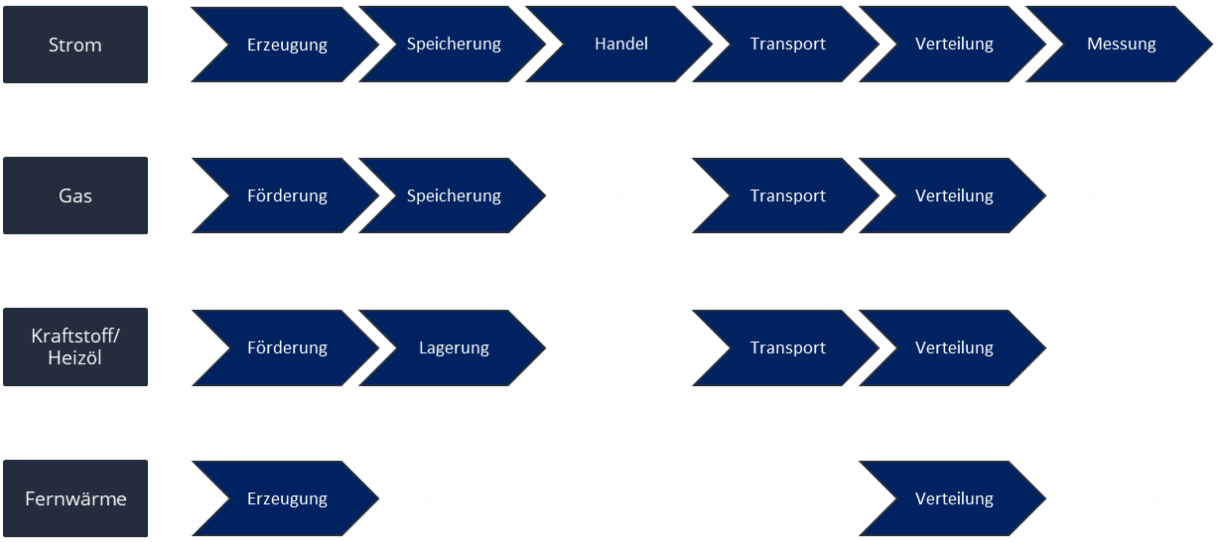

Abbildung 4: Die Wertschöpfungskette des KRITIS-Sektors Energie.

Ein Energieversorger ist im Sinne der Verordnung ein Dienstleister, der die Allgemeinheit mit Strom, Gas, Kraftstoff/Heizöl oder Fernwärme versorgt. Die Versorgung ist dann gegeben, wenn ein Unternehmen des Energiesektors mindestens in einer der

Wertschöpfungsstufen tätig ist.

Für Energieversorger ergeben sich aus dem BSIG sechs Einordnungsmöglichkeiten.

Gruppe	1	2	3	4	5	6
Bezeich-nung	Kernkraft	Netz EnWG	Anlage EnWG	Sonstige KRITIS-Netze	Sonstige KRITIS-Anlagen	Übrige Versorger
Definition	Betreiber von Kernkraft-werken.	Betreiber von Energie-versorgungs-netzen i.S.d. § 11 Abs. 1a EnWG.	Betreiber von Energiean-lagen i.S.d. § 11 Abs. 1b EnWG.	KRITIS-Betreiber von Energie-versorgungs-netzen, die nicht zur Gruppe 2 gehören.	KRITIS-Betreiber von Energiean-lagen, die nicht zur Gruppe 1 oder 3 gehören.	Energie-versorger, die nicht zu den Gruppen 1 bis 5 gehören.

Tabelle 1: Einordnungsmöglichkeiten Energieversorger.

Jede der Gruppen 1 bis 5 fällt in den Regelungsbereich des IT-Sicherheitsgesetzes. Die bindenden Rechtsvorschriften variieren jedoch von Gruppe zu Gruppe. Wodurch sich auch Rechte, Pflichten und Konsequenzen bei Pflichtverletzungen unterscheiden.

Lediglich Gruppe 6 fällt nicht in den Regelungsbereich des IT-Sicherheitsgesetzes.

Welche Rechtsvorschriften sind für Energieversorger bindend?

Im Zentrum aller Stammgesetze, die durch das IT-Sicherheitsgesetz geändert oder tangiert werden, steht das BSI-Gesetz. Ein Blick in das BSI-Gesetz ist daher für alle Unternehmen des Energiesektors Pflicht.

Die §§ 8a, 8b BSIG haben in einigen Bereichen des Energiesektors keine oder eingeschränkte Gültigkeit, weil für sie spezialgesetzliche Regelungen gelten.

> Eine Übersicht über branchenspezifische Sicherheitsstandards (B3S) finden Sie unter https://www.bsi.bund.de/DE/Themen/Industrie_KRITIS/IT-SiG/Was_tun/Stand_der_Technik/B3S_BAKs/B3S_BAKs.html?nn=7588870

Spezialgesetzliche Regelungen gibt es für Gruppe 1- *Kernkraft*, Gruppe 2-*Netz EnWG* und Gruppe 3-*Anlagen EnWG*.

Welche Gesetze vorrangige Regelungen zur IT-Sicherheit beinhalten oder bei der Einordnung in eine der Gruppen helfen, zeigt die nachfolgende Tabelle auf.

Gruppe	1	2	3	4	5
Bezeichnung	Kernkraft	Netz EnWG	Anlage EnWG	Sonstige KRITIS-Netze	Sonstige KRITIS-Anlagen
Rechtsvor-schriften	BSIG BSI-KritisV EnWG AtG	BSIG BSI-KritisV EnWG IT-Sicherheits-katalog	BSIG BSI-KritisV EnWG KWKG IT-Sicherheits-katalog	BSIG BSI-KritisV	BSIG BSI-KritisV EEG 2017 MsbG UVPG
IT-Sicherheit	§ 11 Abs. 1b EnWG § 7c Abs. 2 Nr. 1 AtG § 44b AtG	§ 11 Abs. 1a EnWG § 11 Abs. 1c EnWG	§ 11 Abs. 1b EnWG § 11 Abs. 1c EnWG	§ 8a BSIG § 8b BSIG	§ 8a BSIG § 8b BSIG
Einordnung	§ 7 Abs. 1 AtG Anhang 1 Teil 1-3 BSI-KritisV	§ 3 EnWG Anhang 1 Teil 1-3 BSI-KritisV	§ 3 EnWG § 2 KWKG Anhang 1 Teil 1-3 BSI-KritisV	Anhang 1 Teil 1-3 BSI-KritisV	§ 4 EEG 2017 § 2 MsbG Anlage 1 UVPG Anhang 1 Teil 1-3 BSI-KritisV

Tabelle 2: Rechtsvorschriften Energieversorger.

Die Gruppe *Kernkraft* findet Regelungen zur IT-Sicherheit im EnWG, da sie Erzeugungsanlagen betreiben. Sofern es vorrangige Regelungen im Atomgesetz (AtG) gibt, haben sie diese anzuwenden. Insbesondere die Meldepflicht für IT-Sicherheitsvorfälle wurde mit Inkrafttreten des IT-Sicherheitsgesetzes in § 44b AtG aufgenommen.

Die Gruppe *Netz EnWG* besteht aus Betreibern von Strom- oder Gasversorgungsnetzen. Die entsprechenden Legaldefinitionen sind in § 3 EnWG nachzulesen. Das Energiewirtschaftsrecht regelt die Anforderungen an die IT-Sicherheit in § 11 Abs. 1a EnWG. Die Meldepflicht wird durch § 11 Abs. 1c EnWG geregelt.

Zur Gruppe *Anlagen EnWG* gehören Energieanlagenbetreiber, die den Legaldefinitionen von § 3 EnWG oder § 2 Kraft-Wärme-Kopplungsgesetz (KWKG) entsprechen und als KRITIS-Betreiber einzuordnen sind. Für sie wurden die IT-Sicherheitsanforderungen in § 11 Abs. 1b EnWG festgelegt. Die Meldepflicht wird auch hier durch § 11 Abs. 1c EnWG geregelt.

KRITIS-Betreiber von Energieversorgungsnetzen, die keine Strom- oder Gasnetze im Sinne des EnWG sind, gehören zur Gruppe *Sonstige KRITIS-Netze*. Für sie gibt es bislang keine spezialrechtlichen Vorschriften. Daher finden Energieversorger dieser Gruppe alle bindenden Regelungen im BSI-Gesetz.

Für Betreiber der Gruppe *Sonstige KRITIS-Anlagen*, die keine Kernkraftwerke oder Anlagen im Sinne des Energiewirtschaftsrechts betreiben, gelten ebenfalls die Regelungen des BSI-Gesetzes. Bei der Einordnung in diese Gruppe helfen Definitionen des Erneuerbare-Energien-Gesetzes (EEG 2017), Messstellenbetriebsgesetz (MsbG) und Gesetz über die Umweltverträglichkeitsprüfung (UVPG).

Für alle Gruppen wird die Zugehörigkeit zu den Kritischen Infrastrukturen über Anhang 1 Teil 1-3 BSI-KritisV bestimmt.

Alle genannten Rechtvorschriften finden Sie in der xmera : library zum Downloaden.

Einen Überblick über die gesetzlichen Bestimmungen einschließlich der Änderungshistorie mit Vorher- und Nachhertexten seit Bestehen des IT-Sicherheitsgesetz finden Sie im xmera : lawbook.

Welche Rechte, Pflichten und Konsequenzen gelten für betroffene Energieversorger?

Je nach Gruppenzugehörigkeit ergeben sich durch die verschiedenen bindenden Rechtsvorschriften weitestgehend auch unterschiedliche Rechte und Pflichten. Auch bei Pflichtverletzungen wird nicht jeder Energieversorger gleich behandelt. Es kommt auf die zugrunde liegenden Gesetze an.

Gruppe	1	2	3	4	5
Bezeichnung	Kernkraft	Netz EnWG	Anlage EnWG	Sonstige KRITIS-Netze	Sonstige KRITIS-Anlagen
Pflichten	Einrichtung eines Managementsystems zur Sicherstellung der nuklearen Sicherheit (§ 7c Abs. 2 Nr. 1).	Umsetzung der Anforderungen des IT-Sicherheitskataloges (§ 11 Abs. 1a EnWG).	Umsetzung der Anforderungen des (noch nicht vorliegenden) IT-Sicherheitskataloges (§ 11 Abs. 1b EnWG) .	Umsetzung von IT-Sicherheitsmaßnahmen nach Stand der Technik (§ 8a BSIG) bis Mai 2018.	Umsetzung von IT-Sicherheitsmaßnahmen nach Stand der Technik (§ 8a BSIG) bis Mai 2018.
	Umsetzung der Anforderungen des IT-Sicherheitskataloges (§ 11 Abs. 1b EnWG) für KRITIS-Betreiber solange es keine vorrangigen Vorgaben im AtG gibt.	Zertifizierung des ISMS bis 31. Januar 2018 (IT-Sicherheitskatalog gem. § 11 Abs. 1a EnWG).		Nachweis alle zwei Jahre gegenüber dem BSI (§ 8a BSIG) ab Mai 2018.	Nachweis alle zwei Jahre gegenüber dem BSI (§ 8a BSIG) ab Mai 2018.
	Registrierung einer Kontaktstelle beim BSI (§ 8b BSIG) bis November 2016 durch KRITIS-Betreiber.	Registrierung einer Kontaktstelle beim BSI (§ 8b BSIG) bis November 2016 durch KRITIS-Betreiber.	Registrierung einer Kontaktstelle beim BSI (§ 8b BSIG) bis November 2016 .	Registrierung einer Kontaktstelle beim BSI (§ 8b BSIG) bis November 2016.	Registrierung einer Kontaktstelle beim BSI (§ 8b BSIG) bis November 2016.
	Meldung von IT-Sicherheitsvorfälle (§ 44b AtG) an das BSI seit 25. Juni 2015.	Meldung von IT-Sicherheitsvorfällen (§ 11 Abs. 1c EnWG) an das BSI seit November 2016 für KRITIS-	Meldung von IT-Sicherheitsvorfällen (§ 11 Abs. 1c EnWG) an das BSI seit Mai 2016.	Meldung von IT-Sicherheitsvorfällen (§ 8b BSIG) an das BSI seit Mai 2016.	Meldung von IT-Sicherheitsvorfällen (§ 8b BSIG) an das BSI seit Mai 2016.

		Betreiber. **Neuregelung :** Meldung von IT-Sicherheitsvorfällen (§ 11 Abs. 1c EnWG) an das BSI seit 30. Juni 2017 durch Nicht-KRTITIS-Betreiber. Meldung eines Ansprechpartners für IT-Sicherheit bei BNetzA bis 30. November 2015 (IT-Sicherheitskatalog gem. § 11 Abs. 1a EnWG).			
Rechte	Informationsversorgung durch BSI für KRITIS-Betreiber. Beratung und Unterstützung durch das BSI für KRITIS-Betreiber.	Informationsversorgung durch BSI für KRITIS-Betreiber. Beratung und Unterstützung durch das BSI für KRITIS-Betreiber.	Informationsversorgung durch BSI. Beratung und Unterstützung durch das BSI.	Informationsversorgung durch BSI. Beratung und Unterstützung durch das BSI.	Informationsversorgung durch BSI. Beratung und Unterstützung durch das BSI.
Bußgelder	Für KRITIS-Betreiber können bis 50.000 EUR Bußgeld bei nicht ordnungsgemäßer Registrierung einer Kontaktstelle anfallen.	Für KRITIS-Betreiber können bis 50.000 EUR Bußgeld bei nicht ordnungsgemäßer Registrierung einer Kontaktstelle anfallen.	Für KRITIS-Betreiber können bis 50.000 EUR Bußgeld bei nicht ordnungsgemäßer Registrierung einer Kontaktstelle anfallen.	Bis 100.000 EUR bei Zuwiderhandlung einer vollziehbaren Anordnung i.Z.m. der Beseitigung von Sicherheitsmängeln.	Bis 100.000 EUR bei Zuwiderhandlung einer vollziehbaren Anordnung i.Z.m. der Beseitigung von Sicherheitsmängeln.

	Alle übrigen Bußgelder gem. § 14 BSIG entfallen.	Alle übrigen Bußgelder gem. § 14 BSIG entfallen.	Alle übrigen Bußgelder gem. § 14 BSIG entfallen.	Bis 50.000 EUR bei Verletzung übriger Pflichten gem. §§ 8a, 8b BSIG.	Bis 50.000 EUR bei Verletzung übriger Pflichtengem. §§ 8a, 8b BSIG.

Tabelle 3: Pflichten, Rechte und Bußgelder Energieversorger.

Pflichten

Energieversorger, die der Gruppe *Kernkraft* angehören, zählen zu den Energieanlagenbetreibern im Sinne des § 11 Abs. 1b EnWG, wenn sie KRITIS-Betreiber sind. Die darin geregelten Pflichten haben sie jedoch nur umzusetzen, wenn das Atomgesetz keine eigenen Pflichten zur IT-Sicherheit formuliert.

Unter § 7c Abs. 2 Nr. 1 AtG werden Betreiber von Kernkraftwerken zur Einrichtung eines Managementsystems, das die nukleare Sicherheit sicherstellt, verpflichtet. Hierunter ließe sich auch die Einführung eines Informationssicherheitsmanagementsystems (ISMS) verstehen.

Expliziter ist dagegen § 44b AtG. Er regelt die Meldepflicht für IT-Sicherheitsvorfälle, die seit 25. Juni 2015 an das BSI gemeldet werden müssen. KRITIS-Betreiber mussten zudem nach § 8b Abs. 3 BSIG bis November 2016 eine Kontaktstelle benennen.

Die Pflichten von Energieversorgern der Gruppe *Netz EnWG* sind dagegen dezidiert formuliert. Sie ergeben sich aus dem EnWG und dem IT-Sicherheitskatalog gemäß § 11 Abs. 1a EnWG.

Bis zum 30. November 2015 mussten Energieversorgungsnetzbetreiber der BNetzA einen Ansprechpartner benennen. Diese Pflicht geht aus dem IT-Sicherheitskatalog hervor, der zudem die Einführung eines ISMS gemäß der Umsetzungsstandards DIN ISO/IEC 27001, DIN ISO/IEC 27002 und DIN ISO/IEC TR 27019 fordert. Das ISMS muss bis zum 31. Januar 2018 zertifiziert worden sein.

Bis November 2016 waren KRITIS-Netzbetreiber dazu angehalten eine Kontaktstelle beim BSI registrieren zu lassen. Diese Pflicht ergib sich aus § 8b Abs. 3 BSIG. Seit November 2016 müssen KRITIS-Betreiber IT-Sicherheitsvorfälle gemäß § 11 Abs. 1c EnWG melden.

Neuregelung durch NIS-Richtlinien-Umsetzungsgesetz: Seit 30. Juni 2017 sind auch Nicht-KRITIS-Netzbetreiber dazu verpflichtet IT-Sicherheitsvorfälle an das BSI zu melden. Diese Neuerung wurde in § 11 Abs. 1c EnWG verankert.

> ! In unserem Beitrag Meldepflicht doch nicht für alle Energieversorger relevant? durchleuchten wir die neue Meldepflicht mit all ihren Anforderungen und Unklarheiten an die Meldekriterien.

Für Energieversorger der Gruppe *Anlagen EnWG* sind IT-Sicherheitsanforderungen bislang lediglich in ihren Wurzeln angelegt. Zwar werden Energieanlagenbetreiber im Sinne des Energiewirtschaftsrechts dazu verpflichtet die Anforderungen des IT-

Sicherheitskataloges gemäß § 11 Abs. 1b EnWG umzusetzen. Doch bis dato liegt dieser Sicherheitskatalog nicht vor.

Die Meldepflicht von IT-Sicherheitsvorfällen an das BSI dagegen besteht seit Mai 2016 und ist in § 11 Abs. 1c EnWG nachzulesen. Zudem mussten Energieanlagenbetreiber gemäß § 8b Abs. 3 BSIG bis November 2016 eine Kontaktstelle beim BSI registrieren lassen.

Energieversorger der Gruppen *Sonstige KRITIS-Netze* und *Sonstige KRITIS-Anlagen* haben als KRITIS-Betreiber dieselben Pflichten. Sie fallen direkt unter das BSIG und haben daher Maßnahmen zur Wahrung der IT-Sicherheit von IT-Systemen, -Komponenten und –Prozessen nach Stand der Technik umzusetzen. Diese Pflicht regelt § 8a BSIG, woraus ebenso hervorgeht, dass die Umsetzung bis Mai 2018 erfolgen und nachgewiesen werden muss. Im Weiteren muss ein geeigneter Nachweis alle zwei Jahre vorgezeigt werden.

Auch für *Sonstige KRITIS-Netze* und *Sonstige KRITIS-Anlagen* besteht durch § 8b BSIG eine Meldepflicht von IT-Sicherheitsvorfällen an das BSI. Beide Gruppen müssen seit Mai 2016 entsprechende Vorfälle melden. Bis November 2016 musste zudem eine Kontaktstelle beim BSI registriert werden.

Rechte

KRITIS-Energieversorger, unabhängig von jeder weiteren Einordnung, werden gemäß § 8b Absatz 2 Nr. 4 BSIG vom BSI mit Informationen zu Sicherheitslücken, Schadprogrammen, versuchten Angriffen auf die Sicherheit der Informationstechnik, potentiellen Auswirkungen von Angriffen und dem aktuellen Lagebild zur IT-Sicherheit der Kritischen Infrastrukturen versorgt.

Außerdem können sie gemäß § 3 Abs. 1 Nr. 18 BSIG Beratungsleistungen und Unterstützung des BSI bei der Beseitigung von herausgehobenen IT-Sicherheitsvorfällen in Anspruch nehmen.

Herausgehobene Fälle sind beispielsweise Angriffe auf besonderem technischem Niveau. Hat der Angriff eine Verletzung der IT-Sicherheit zur Folge, die die Öffentlichkeit besonders betrifft, liegt nach § 5a Abs. 2 BSIG ebenfalls ein herausgehobener Fall vor.

Für Nicht-KRITIS-Energieversorger sieht das BSIG diese Rechte nicht vor.

Bußgelder

Das BSI-Gesetz definiert in § 14 BSIG ordnungswidrige Handlungen bezüglich der in den §§ 8a, 8b BSIG geregelten Pflichten von Kritischen Infrastrukturen.

Geldbußen bis 50.000 EUR können verhängt werden, wenn vorsätzlich oder fahrlässig gegen die Meldepflicht, die Registrierung einer Kontaktstelle oder die Umsetzung von IT-

Sicherheitsmaßnahmen verstoßen wird. Dabei reicht es schon aus, dass eine Pflicht nicht richtig, nicht vollständig oder nicht rechtzeitig erfüllt wird.

Bis 100.000 EUR Bußgeld werden fällig, wenn vorsätzlich oder fahrlässig einer vollziehbaren Anordnung im Zusammenhang mit der Beseitigung von Sicherheitsmängeln zuwidergehandelt wird.

Nicht-KRITIS-Energieversorger (Strom- und Gasnetzbetreiber gemäß § 11 Abs. 1a EnWG und Nicht-KRITIS-Betreiber von Kernkraftwerken) sind grundsätzlich nicht von den Bußgeldern des § 14 BSIG betroffen, da sie ausschließlich den spezialrechtlichen Regelungen folgen.

Für KRITIS-Betreiber der Gruppen *Kernkraft*, *Netze EnWG* oder *Anlagen EnWG* können lediglich bei nicht ordnungsgemäßer Registrierung einer Kontaktstelle Geldstrafen durch das BSI verhängt werden. Die übrigen Ordnungswidrigkeiten beziehen sich auf Pflichten des BSI-Gesetzes, die für die genannten Gruppen keine Anwendung finden.

Welche Rolle nimmt das BSI ein?

Das BSI möchte als nationale IT- und Cyber-Sicherheitsbehörde die IT-Sicherheit einerseits durch präventive Sicherheitsmaßnahmen erhöhen. Andererseits möchte es aber auch dabei unterstützen aktuelle Bedrohungen und Angriffe erfolgreich abzuwehren.

Dazu überträgt das IT-Sicherheitsgesetz dem BSI mehr Verantwortung und erweitert seinen operativen Aufgabenbereich. Beispielsweise ist das BSI befugt IT-Produkte und Software auf Sicherheitslücken zu untersuchen.

Zudem hat es die Aufgabe eingehende Meldungen zu IT-Sicherheitsvorfällen zu bewerten und zu analysieren. Ziel ist, mittels der eingehenden Informationen ein Warnsystem aufzubauen, um KRITIS-Betreiber möglichst früh über potentielle Bedrohungen und geeignete Gegenmaßnahmen in Kenntnis zu setzen.[4]

Diese Aufgabe erfüllt das IT-Lagezentrum des BSI. Dafür ist es für KRITIS-Betreiber und Bundesbehörden täglich 24 Stunden erreichbar.

Im Rahmen des NIS-Richtlinien-Umsetzungsgesetzes ist für 2017 geplant, KRITIS-Betreiber auf Wunsch vor Ort durch Mobile Incident Response Teams (MIRT) des BSI zu unterstützen, wenn sie von einem IT-Sicherheitsvorfall betroffen sind.[5]

[4] Vgl. Bundesamt für Sicherheit in der Informationstechnik (2017).
[5] Vgl. Bundesamt für Sicherheit in der Informationstechnik (2016); Die Bundesregierung der Bundesrepublik Deutschland (2016).

Welche Aufgaben hat die Bundesnetzagentur in Sachen IT-Sicherheit für Energieversorger?

Die Kernaufgabe der Bundesnetzagentur (BNetzA) im Energiebereich ist die Energieregulierung. Mit Einführung des IT-Sicherheitsgesetzes wurden der Bundesnetzagentur neue Aufgaben zugeteilt.

Gemäß dem Energiewirtschaftsgesetz ist die BNetzA verantwortlich für die nach § 11 Abs. 1a, 1b EnWG geforderten IT-Sicherheitskataloge. Der Katalog der Sicherheitsanforderungen gemäß § 11 Abs. 1a EnWG wurde bereits erarbeitet und im August 2015 veröffentlicht. Der Katalog der Sicherheitsanforderungen gemäß § 11 Abs. 1b EnWG dagegen ist bis dato noch nicht fertiggestellt.

Zudem ist die Bundesnetzagentur berechtigt die Einhaltung der IT-Sicherheitsanforderungen der Kataloge zu überprüfen.

Werden IT-Sicherheitsvorfälle von Energienetzbetreibern oder Energieanlagenbetreiber, die unter das EnWG fallen, gemeldet, wird die BNetzA vom BSI unverzüglich darüber informiert.

So können Energieversorger zukünftig Regelungen zur IT-Sicherheit mitgestalten

UP KRITIS

Die Initiative UP KRITIS (Umsetzungsplan KRITIS) fördert die Zusammenarbeit zwischen Wirtschaft und Staat in Deutschland bereits seit 2007.

Ziel der Initiative ist, branchenspezifische Sicherheitsanforderungen kooperativ zu erarbeiten, die Widerstandsfähigkeit der Kritischen Infrastrukturen zu verbessern und Gesetzesvorgaben aktiv zu begleiten.[6]

Teilnehmer des UP KRITIS können in Deutschland ansässige Organisationen von KRITIS-Betreibern, Fach- und Branchenverbände als auch zuständige Behörden werden. Eine aktive Mitarbeit in den Branchenarbeitskreisen (BAK) und Themenarbeitskreisen (TAK) erfordert die Aufnahme als Partner im UP KRITIS.

Für Energieversorger sind der BAK Strom, BAK Gas und BAK Mineralöl interessant. Die TAKs umfassen beispielsweise Themen wie Audits und Standards, Operativer Informationsaustausch oder Industrial Control Systems.

Mit der Anmeldung zur Teilnahme am UP KRITIS ist auf Wunsch auch die Registrierung als Teilnehmer der Allianz für Cyber-Sicherheit möglich.

[6] Vgl. UP KRITIS (2014).

Allianz für Cyber-Sicherheit

Die Initiative Allianz für Cyber-Sicherheit wurde gemeinsam vom BSI und BITKOM (Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V.) gegründet.

Ziel der Allianz für Cyber-Sicherheit ist, eine zeitnahe und valide Informationsversorgung beispielswiese über aktuelle Cyber-Bedrohungen oder die aktuelle Cyber-Sicherheitslage anzubieten.

Teilnehmen kann jede deutsche Organisation, somit auch Nicht-KRITIS-Energieversorger. KRITIS-Energieversorger können als INSI (Institution mit besonderem staatlichem Interesse) aufgenommen werden. Ihnen wird ein erweitertes Informationsangebot zur Verfügung gestellt.

Organisationen können sich als Teilnehmer oder aktiver Partner bei der Allianz für Cyber-Sicherheit einbringen. Verbände, Gremien, Medienorgane o.ä. können als Multiplikator aktiv mitwirken. Beiträge von Partnern und Multiplikatoren sind exklusiv und kostenlos für Teilnehmer.

Zum UP KRITIS finden Sie unter http://www.kritis.bund.de/SubSites/ ausführliche Informationen.

Mehr Informationen zur Allianz für Cyber-Sicherheit erhalten Sie unter https://www.allianz-fuer-cybersicherheit.de.

Wo ist das IT-Sicherheitsgesetz als PDF Download verfügbar?

Am 24. Juli 2015 wurde das IT-SiG im Bundesgesetzblatt veröffentlicht. Am Tag drauf ist es in Kraft getreten.

Sie können das IT-Sicherheitsgesetz als PDF-Dokument direkt beim Bundesministerium des Innern herunterladen.

Empfehlenswerter sind jedoch die zugehörigen Stammgesetze in ihrer aktuellen Fassung. Sie enthalten auch die Neuregelungen des NIS-Richtlinien-Umsetzungsgesetz.

Für Sie als Energieversorger haben wir alle Downloadlinks zu relevanten Rechtstexten im Rahmen der IT-Sicherheit in unserer xmera : library gesammelt.

Im xmera : lawbook können Sie Gesetzesänderungen wortgetreu verfolgen.

Zusammenfassung

Sicherheit beschäftigt die Menschheit schon solange es Menschen gibt. Genauso lange werden Sicherheitsstandards an aktuelle Entwicklungen immer wieder angepasst. Die Digitalisierung ist eine dieser Entwicklungen, die eine Anpassung notwendig macht. Mit dem IT-Sicherheitsgesetz wurde ein entscheidender Schritt für mehr Digitalisierung gemacht.

Der Gesetzgeber verfolgt hierbei drei Ziele: Kritische Infrastrukturen sollen vor Angriffen auf ihre IT-Infrastruktur geschützt werden, die Versorgungssicherheit in Deutschland soll stets gewährleistet sein und Gefahren sollen frühzeitig erkannt werden.

Die Energieversorgung ist eine der Kritischen Infrastrukturen. Einige Unternehmen der Energieversorgung werden mit dem IT-Sicherheitsgesetz verpflichtet bis 2018 geeignete IT-Sicherheitsmaßnahmen umzusetzen. IT-Sicherheitsvorfälle müssen schon jetzt gemeldet werden.

Pflichten, Rechte und Konsequenzen bei Pflichtverletzungen werden jedoch nicht für alle betroffenen Energieversorger gleich geregelt. Für Energieversorgungsnetzbetreiber im Sinne des Energiewirtschaftsrechts sind die IT-Sicherheitsregelungen in Form von spezialgesetzlichen Vorschriften am weitesten ausgearbeitet worden.

Ähnliche Regelungen können für Energieanlagenbetreiber gemäß § 11 Abs. 1b EnWG erwartet werden.

Ob in den Bereichen Kraftstoff/Heizöl und Fernwärme branchenspezifische Regelungen folgen werden, bleibt abzuwarten.

Sicher dagegen ist, mit dem IT-Sicherheitsgesetz wurde der Grundstein für ein neues Sicherheitsbewusstsein gelegt.

Literaturverzeichnis

Bundesamt für Sicherheit in der Informationstechnik (2017): Schutz Kritischer Infrastrukturen durch IT-Sicherheitsgesetz und UP KRITIS, Bonn .

Bundesamt für Sicherheit in der Informationstechnik (2016): Das IT-Sicherheitsgesetz, Kritische Infrastrukturen schützen, Bonn.

Bundesministerium der Justiz (2008): Bundesanzeiger, Bekanntmachung des Handbuchs der Rechtsförmlichkeit, 3. Auflage, Köln.

Die Bundesregierung der Bundesrepublik Deutschland (2015): Entwurf eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz), Deutscher Bundestag, 18. Wahlperiode, Drucksache 18/5121, Köln.

Die Bundesregierung der Bundesrepublik Deutschland (2016): Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Jan Korte, Frank Tempel, Annette Groth, weiterer Abgeordneter und der Fraktion DIE LINKE - Drucksache 18/9334 - , Deutscher Bundestag, 18. Wahlperiode, Drucksache 18/9445, Köln.

UP KRITIS (2014): UP KRITIS, Öffentlich-Private Partnerschaft zum Schutz Kritischer Infrastrukturen – Grundlagen und Ziele -, Bonn.

Impressum

Herausgeber
xmera e.K.

Hainbuchenstr. 13
45881 Gelsenkirchen

Autorin
Liane Hampe

T 0209 590 888 63
F 0209 947 085 07
E liane.hampe@xmera.de
W https://xmera.de

Stand
September 2017

Bildnachweis
Abbildungen: Eigene Darstellungen der xmera.

Titelbild: https://stockata.de

x m e r a : werte schützen