xmera

Oktober 2017

Meldepflicht doch nicht für alle Energieversorger relevant?

Ein umfassender Einblick in den § 11 Absatz 1c EnWG mit all seinen Anforderungen und Unklarheiten an die Meldekriterien, insbesondere für Nicht-KRITIS-Energieversorgungsnetzbetreiber.

Inhaltsverzeichnis

Abbildungsverzeichnis 2
Einleitung 3
Seit wann gibt es die Meldepflicht für Energieversorger? 3
Was ist für KRITIS-Energieversorger neu an der Meldepflicht? 4
Was bedeutet die Meldepflicht für Energieversorgungsnetzbetreiber? 4
Kontaktstelle 4
Meldestufen 5
Melde- und Informationsportal 5
Meldeaufwand 6
Welche IT-Sicherheitsvorfälle müssen gemeldet werden? 6
Gesetzestext 6
Definitionen der Schlüsselwörter und –begriffe 7
Störung 7
Störung der Schutzziele 8
Erhebliche Störung der Schutzziele 9
Beispiele für erhebliche Störungen der Schutzziele 9
Beispiele für nicht erhebliche Störungen der Schutzziele 10
Erheblichkeitskriterium 10
Erhebliche Beeinträchtigung für KRITIS-Betreiber 11
Erhebliche Beeinträchtigung für Nicht-KRITIS-Energieversorgungsnetzbetreiber 11
Ausfall 12
Meldesystematik 12
Welche Art von Angriffen ist zu befürchten? 13
Wie ist das IT-Sicherheitsniveau der Energieversorger einzuschätzen? 14
Sicherheitsbewusstsein 14
IT-Sicherheitsmaßnahmen-Index 14
Zusammenfassung 15
Literaturverzeichnis 16
Impressum 18

Abbildungsverzeichnis

Abbildung 1: Meldesystematik § 11 Absatz 1c EnWG..... 13

Einleitung

Erst vor rund dreieinhalb Monaten wurde die Meldepflicht für IT-Sicherheitsvorfälle auf alle Energieversorger ausgeweitet. Nach der derzeitigen Auslegung des Gesetzes durch das BSI ist jedoch unklar, ob die Meldepflicht wirklich auf alle der neu adressierten Nicht-KRITIS-Energieversorgungsnetzbetreiber durchschlägt.

Aktuell hängen Nicht-KRITIS-Energieversorgungsnetzbetreiber innerhalb des Meldeprozesses in der Luft. Eine Entscheidung, ob ein IT-Sicherheitsvorfall meldepflichtig ist, ist nicht sinnvoll möglich. In diesem Beitrag erklären wir Ihnen die Hintergründe.

Darüber hinaus erfahren Sie in diesem Beitrag was Erreichbarkeit für Ihr Funktionspostfach bedeutet, warum Sie Ihr ISMS um ein Schutzziel erweitern müssen, warum für KRITIS-Energieversorger mehr Störungen als zuvor meldepflichtig sind und was sich der Gesetzesgeber bei der Differenzierung der Störungen in § 11 Absatz 1c Nr. 1 und Nr. 2 gedacht hat.

Seit wann gibt es die Meldepflicht für Energieversorger?

Zu den Energieversorgern im Sinne des § 11 EnWG gehören Energieversorgungsnetzbetreiber und KRITIS-Energieanlagenbetreiber. Die Meldepflicht für IT-Sicherheitsvorfälle wird in § 11 Abs. 1c EnWG geregelt.

Der Absatz zur Meldepflicht wurde erstmals mit dem IT-SiG in 2015 eingeführt. KRITIS-Energieversorgungsnetzbetreiber und KRITIS-Energieanlagenbetreiber müssen bereits seit November 2016 entsprechende Störungen an das BSI melden.

Zwei Jahre später, mit Umsetzung der NIS-Richtlinie, wurde die Meldepflicht geändert. Seit dem 30. Juni 2017 sind auch Nicht-KRITIS-Energieversorgungsnetzbetreiber verpflichtet Informationen über IT-Sicherheitsvorfälle an das BSI zu weiterzuleiten.

Die Analyse und Bewertung der eingehenden Informationen zu IT-Sicherheitsvorfällen ist eine der neuen Aufgaben des BSI. Ziel ist es, ein Warnsystem für Cyber-Bedrohungen aufzubauen und regelmäßig die aktuelle Cyber-Sicherheitslage in Form von Lagebildern an Meldepflichtige zu kommunizieren.

Über diese Neuregelung haben wir bereits in unserem Beitrag IT-Sicherheitsgesetz Energieversorger & Neuregelung berichtet.

Was ist für KRITIS-Energieversorger neu an der Meldepflicht?

KRITIS-Energieversorgungsnetzbetreiber und KRITIS-Energieanlagenbetreiber sind schon fast seit einem Jahr dazu verpflichtet Störungen zu melden. Für sie sind die Regelungen zur Meldepflicht somit nichts Neues.

Doch wer einfach so weitermacht wie bisher könnte unwissentlich meldepflichtige IT-Sicherheitsvorfälle übersehen. Denn wie so häufig steckt der Teufel im Detail.

Die Meldepflicht ist in § 11 Abs. 1c EnWG geregelt. Bei der letzten Änderung des Paragraphen am 30. Juni 2017, wurde der Umfang der meldepflichtigen Störungen erweitert.

Zuvor mussten lediglich „erhebliche Störungen“ unter bestimmten Bedingungen gemeldet werden. Nun fallen „Störungen“ grundsätzlich unter die Meldepflicht, sofern es zu einer Versorgungsbeeinträchtigung oder –unterbrechung gekommen ist.

Im xmera : lawbook können Sie den Gesetzestext vor der Änderung mit dem Gesetzestext nach der Änderung direkt vergleichen.

Was bedeutet die Meldepflicht für Energieversorgungsnetzbetreiber?

Kontaktstelle

Neben den KRITIS-Energieversorgungsnetzbetreibern sind nun auch alle Nicht-KRITIS-Energieversorgungsnetzbetreiber zur Meldung von IT-Sicherheitsvorfällen verpflichtet.

Somit gibt es keine Ausnahmen mehr. Für alle rund 1600 Energieversorgungsnetze müssen die Betreiber bestimmte IT-Sicherheitsvorfälle melden.

Die Meldungen erfolgen über eine Kontaktstelle, die beim BSI registriert worden sein muss. Mit einer Kontaktstelle ist in erster Linie ein Funktionspostfach gemeint, das an 24 Stunden über 7 Tagen in der Woche erreichbar sein muss.[1]

Ein Funktionspostfach ist zwar schnell eingerichtet. Doch was bedeutet 24/7 Erreichbarkeit? Das BSI sendet über dieses Postfach beispielsweise Warnungen und Lagebilder. Benötigt das BSI dafür eine Lesebestätigung? Nein, das ist nicht der Fall.

[1] Vgl. Bundesamt für Sicherheit in der Informationstechnik (2017).

> ! Nach telefonischer Aussage des BSI wird keine Lesebestätigung erwartet.
>
> Die weitere Verwendung der Informationen liegt im Ermessen des Empfängers, sofern dabei die TLP-Einstufung berücksichtigt wird.

Energieversorger verwenden das Postfach zur Versendung der Meldungen nach § 11 Abs. 1c EnWG. Für diesen Informationswechsel muss ein operativer Kontakt als Hauptansprechpartner und ein Ansprechpartner für organisatorische Themen angegeben werden.

Eine explizite Umsetzungsfrist für die Registrierung der Kontaktstelle gibt es nicht. Die Registrierung muss jedoch so bald wie möglich geschehen, da die Meldepflicht seit dem 30. Juni 2017 gilt.

Meldestufen

Ist ein IT-Sicherheitsvorfall erkannt worden, muss er unverzüglich gemeldet werden. Akute Folgen des Vorfalls dürfen jedoch vor Absetzen der Meldung eingedämmt werden. Die Meldung kann grundsätzlich in Stufen erfolgen:

1. Erstmeldung – Meldung darf unvollständig sein.
2. Folgemeldung – fehlende Informationen werden nachgereicht.
3. Abschlussmeldung – erfolgt nach Umsetzung aller Maßnahmen.

Sind noch nicht alle Informationen zum Zeitpunkt der Erstmeldung bekannt, kann eine Folgemeldung mit ergänzenden Angaben getätigt werden. Sind alle Maßnahmen zur Bearbeitung des Sicherheitsvorfalles abgeschlossen, erfolgt die Abschlussmeldung.

Die Meldepflicht ist erfüllt, wenn es von Seiten des BSI keine Nachfragen zu dem Vorfall gibt.

Melde- und Informationsportal

Die Meldung wird im Melde- und Informationsportal, also online, vorgenommen. Dabei müssen Angaben zur Störung, zu möglichen grenzübergreifenden Auswirkungen, zur vermuteten oder tatsächlichen Ursache sowie zur betroffenen IT gemacht werden.

Der Informationsbereich hält verschieden sensible Dokumente zur Cyber-Sicherheitslage bereit. Darunter fallen Cyber-Sicherheitswarnungen, Jahreslageberichte, Monatslageberichte, Themenlagebilder, ein Cyber-Sicherheits-Dashboard und eine Kurzinfo zu Schwachstellen in IT-Produkten.

Meldeaufwand

Schätzungen der Bundesregierung zufolge wird davon ausgegangen, dass ein KRITIS-Betreiber maximal sieben Meldungen von IT-Sicherheitsvorfällen pro Jahr vornehmen muss.

Der Mehraufwand, der bei Bearbeitung des Sicherheitsvorfalles über das bisher übliche Maß hinaus entsteht, wird auf 11 Zeitstunden geschätzt.[2]

Bei einem Stundensatz von 80 EUR entstehen Mehraufwendungen in Höhe von 880 EUR pro Meldung. Bei den geschätzten sieben meldepflichtigen Sicherheitsvorfällen sind das 6.160 EUR pro Jahr.

Für Energieversorger erscheint die Durchschnittszahl von sieben Meldungen pro Jahr sehr hoch angesetzt. Unter den Energieversorgern dominiert eine regionale Struktur. Mit der Größe des Energieversorgers nehmen die Komplexität der Sekundärtechnik und damit auch die Anfälligkeit gegenüber Angriffen zu.

Daher sind bei kleinen regionalen Energieversorgern weniger Meldungen zu erwarten. Zudem kommt, dass insbesondere bei Energieversorgern ohne Leitsystem oder ohne Steuerfunktion, wie es häufig im Gasverteilnetz zu beobachten ist, ein meldepflichtiger Vorfall kaum zu konstruieren ist.

Welche IT-Sicherheitsvorfälle müssen gemeldet werden?

Gesetzestext

Der neue Absatz 1c des § 11 EnWG lautet seit dem 30. Juni 2017 wie folgt:

> *Betreiber von Energieversorgungsnetzen und von solchen Energieanlagen, die durch Inkrafttreten der Rechtsverordnung gemäß § 10 Absatz 1 des BSI-Gesetzes als Kritische Infrastruktur bestimmt wurden, haben*
>
> > *1. Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse, die zu einem Ausfall oder einer erheblichen Beeinträchtigung der Funktionsfähigkeit des Energieversorgungsnetzes oder der betreffenden Energieanlage geführt haben,*
> >
> > *2. erhebliche Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse, die zu einem Ausfall oder einer erheblichen Beeinträchtigung der Funktionsfähigkeit des Energieversorgungsnetzes oder der betreffenden Energieanlage führen können,*
>
> *über die Kontaktstelle unverzüglich an das Bundesamt für Sicherheit in der Informationstechnik zu melden.*

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

> *Die Meldung muss Angaben zu der Störung, zu möglichen grenzübergreifenden Auswirkungen sowie zu den technischen Rahmenbedingungen, insbesondere der vermuteten oder tatsächlichen Ursache und der betroffenen Informationstechnik, enthalten. Die Nennung des Betreibers ist nur dann erforderlich, wenn die Störung tatsächlich zu einem Ausfall oder einer Beeinträchtigung der Funktionsfähigkeit der Kritischen Infrastruktur geführt hat. Das Bundesamt für Sicherheit in der Informationstechnik hat die Meldungen unverzüglich an die Bundesnetzagentur weiterzuleiten. […]*

Besonders hervorzuheben ist, dass der IT-Sicherheitskatalog gemäß § 11 Abs. 1a EnWG lediglich die Schutzziele Verfügbarkeit, Integrität und Vertraulichkeit vor gibt. Die DIN ISO/IEC 27000 stellt es dem Anwender frei, zusätzlich die Schutzziele Authentizität, Verbindlichkeit, Zuverlässigkeit und Nichtabstreitbarkeit zu berücksichtigen.

> **!** Der § 11 Abs. 1c EnWG impliziert, dass für Energieversorger i.S.d. EnWG die Authentizität zu den im ISMS implementierten Schutzzielen gehört.

Weitere Schlüsselwörter und Begriffe sind „Störungen“, „erhebliche Störungen“, „erhebliche Beeinträchtigung“ und „Ausfall“. Sie werden nachfolgend definiert.

Definitionen der Schlüsselwörter und –begriffe

Störung

Der Gesetzgeber definiert den Begriff Störung in einem Entwurf des IT-Sicherheitsgesetzes wie folgt:[3] [4]

> *Eine Störung im Sinne des BSI-Gesetzes liegt […] vor, wenn die eingesetzte Technik die ihr zugedachte Funktion nicht mehr richtig oder nicht mehr vollständig erfüllen kann oder versucht wurde, entsprechend auf sie einzuwirken.*

Gemeint sind somit technische Funktionseinschränkungen bis hin zu Funktionsausfällen der IKT. Besonders hervorzuheben ist, dass allein der Versuch eine technische Funktionseinschränkung oder einen Funktionsausfall herbeizuführen, schon eine Störung ist.

[3] Die Bundesregierung der Bundesrepublik Deutschland (2015).
[4] Die Meldepflicht für Energieversorgungsnetzbetreiber und KRITIS-Energieanlagebetreiber wird zwar durch das Energiewirtschaftsgesetz und nicht durch das BSI-Gesetz geregelt. Doch die Rechtstexte stimmen in Sachen Meldepflicht fast ausnahmslos Wort für Wort überein. Sich an den Definitionen des IT-SiG zu orientieren ist daher sinnvoll.

Störung der Schutzziele

In § 11 Abs. 1c EnWG wird von einer „Störung der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit" der „informationstechnischen Systeme, Komponenten oder Prozesse" ausgegangen.

Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit sind Schutzziele der Informationssicherheit. Diese Ziele werden im Rahmen des ISMS für Risikoelemente vom Typ „Systeme, Komponenten oder Prozesse der Informations- und Kommunikationstechnik (IKT)"[5] formuliert.

Die Definition für Störung im Sinne des BSI-Gesetzes muss daher an dieser Stelle enger gefasst werden. Bei einer Störung der Schutzziele von Risikoelementen im obigen Sinne wurde mindestens eines der Schutzziele angegriffen, weil

i) eine Sperrung oder Unbrauchbarkeit von IT-Systemen, -Komponenten oder -Prozessen erfolgt ist oder versucht wurde (Verletzung der Verfügbarkeit),
ii) eine Manipulation von IT-Systemen, -Komponenten oder -Prozessen erfolgt ist oder versucht wurde (Verletzung der Integrität),
iii) eine Fälschung von IT-Systemen, -Komponenten oder -Prozessen erfolgt ist oder versucht wurde (Verletzung der Authentizität),
iv) ein unberechtigter (Lese-)Zugriff auf IT-Systeme, -Komponenten oder -Prozesse erfolgt ist oder versucht wurde (Verletzung der Vertraulichkeit).

Auch hier gilt wieder, das Schutzziel muss nicht tatsächlich verletzt worden sein. Ein Versuch ist ausreichend, um von einer Störung der Schutzziele zu sprechen. Somit zählen auch erfolgreich abgewehrte Angriffe auf die von Energieversorgern eingesetzte IT-Technik als Störung der Schutzziele.

Die Eingrenzung auf „Störung der Schutzziele" impliziert, dass Störungen, die die Schutzziele nicht angreifen, nicht gemeldet werden müssen, da durch sie auch kein Ausfall oder erhebliche Beeinträchtigung der Versorgung zu erwarten ist.

[5] Vgl. Bundesamt für Sicherheit in der Informationstechnik (2015).

Meldepflichtige Störungen der Schutzziele der IT-Systeme, -Komponenten und –Prozesse sind beispielsweise Verletzungen der Schutzziele durch:[6]

- Sicherheitslücken,
- Schadprogrammen,
- außergewöhnliche und unerwartete technische Defekte,

sofern sie sich auf die Versorgungssicherheit auswirken.

Erhebliche Störung der Schutzziele

In der Neuregelung des § 11 Abs. 1c EnWG unterscheidet der Gesetzgeber zwischen „Störungen der Schutzziele" und „erheblichen Störungen der Schutzziele". Eine erhebliche Störung liegt gemäß dem Entwurf des IT-SiG vor,

> *[...] wenn durch sie die Funktionsfähigkeit der erbrachten kritischen Dienstleistung bedroht ist. Nicht meldepflichtig sind Störungen, die zu keiner Beeinträchtigung der Funktionsfähigkeit der Kritischen Infrastrukturen führen können. Erheblich sind insbesondere solche IT-Störungen, die nicht bereits automatisiert oder mit wenig Aufwand mithilfe der nach § 8a als Stand der Technik beschriebenen Maßnahmen abgewehrt werden können.*[7]

Bei einer erheblichen Störung ist somit nicht nur die Funktionsfähigkeit der eingesetzten Technik in Gefahr, sondern als Folge daraus die Funktionsfähigkeit der damit zusammenhängenden kritischen Dienstleistung bedroht.

Beispiele für erhebliche Störungen der Schutzziele

Zu den erheblichen Störungen können nach dem Gesetzesentwurf nachfolgende Fälle gezählt werden:[8]

- neuartige oder außergewöhnliche IT-Vorfälle,
- gezielte Angriffe,
- neue Modi Operandi,
- unerwartete Vorkommnisse,
- Vorfälle, die zur Bewältigung einen erhöhten Ressourceneinsatz benötigen.

Die Beispiele des BSI sind etwas konkreter. Darauf gehen wir noch im Zusammenhang mit der Meldesystematik ein.

[6] Vgl. Die Bundesregierung der Bundesrepublik Deutschland (2015).
[7] Die Bundesregierung der Bundesrepublik Deutschland (2015).
[8] Vgl. Die Bundesregierung der Bundesrepublik Deutschland (2015).

Beispiele für nicht erhebliche Störungen der Schutzziele

Nicht erheblich sind dagegen IT-Störungen, die tagtäglich vorkommen und ohne große Probleme abgewehrt werden können:[9]

- Spam,
- übliche Schadsoftware, die der Virenscanner abfängt,
- Hardwareausfälle im üblichen Rahmen.

Auch hier gibt es seitens des BSI konkretere Beispiele, die wir im Rahmen der Meldesystematik darstellen werden.

Erheblichkeitskriterium

Warum der Gesetzgeber „nachgebessert" hat und nun zwischen „Störungen" und „erheblichen Störungen" unterscheidet ist nicht leicht nachvollziehbar. Ein Blick in den Entwurf des NIS-Richtlinien-Umsetzungsgesetzes und in die NIS-Richtlinie selbst gibt Klarheit.

Der Fokus der Änderungen war zwar Erheblichkeit. Jedoch nicht in Verbindung mit der Störung, sondern in Verbindung mit der Beeinträchtigung der Funktionsfähigkeit des Energieversorgungsnetzes oder der betreffenden Energieanlage. Mit der Betonung des Erheblichkeitskriteriums sollen Artikel 14 Absatz 3 und 4 der NIS-Richtlinie umgesetzt werden.[10]

Führt eine Störung unabhängig von ihrer Ausprägung, zu einer erheblichen Beeinträchtigung oder einem Ausfall, ist sie unverzüglich zu melden.

> **!** Das Erheblichkeitskriterium bezieht sich auf den Grad der Beeinträchtigung der Funktionsfähigkeit des Energieversorgungsnetzes oder der betreffenden Energieanlage.

[9] Vgl. Die Bundesregierung der Bundesrepublik Deutschland (2015).
[10] Vgl. Die Bundesregierung der Bundesrepublik Deutschland (2017).

Erhebliche Beeinträchtigung für KRITIS-Betreiber

Das BSI nimmt auf das Erheblichkeitskriterium in seiner Interpretation des Begriffes „Beeinträchtigung“ keinen Bezug. Jedoch formuliert es einen Grenzwert, bei dessen Unterschreiten die Funktionsfähigkeit beeinträchtigt genug ist, um den Vorfall als meldepflichtig einzustufen. Der Begriff „Beeinträchtigung“ bezieht sich somit auf die Quantität der erbrachten kritischen Dienstleistung.[11]

Der Grenzwert liegt bei mindestens 50% der in der BSI-KritisV angegebenen Schwelle.[12] Die Anlage eines KRITIS-Energieanlagenbetreibers leistet nach KritisV mindestens 420 MW. Der Grenzwert liegt somit bei 210 MW. Demnach ist die Anlage beim Unterschreiten von 210 MW in ihrer Funktionsfähigkeit (erheblich) beeinträchtigt. Die Grenzwerte der Strom- und Gasnetze von KRITIS-Energieversorgungsnetzbetreibern liegen bei 1850 und 2595 GWh/Jahr.

Erhebliche Beeinträchtigung für Nicht-KRITIS-Energieversorgungsnetzbetreiber

Völlig unklar ist allerdings was der Ausdruck „erhebliche Beeinträchtigung“ für Nicht-KRITIS-Energieversorgungsnetzbetreiber bedeutet.

Das BSI erklärt lediglich was „unter einer Beeinträchtigung der Funktionsfähigkeit der betriebenen Kritischen Infrastruktur zu verstehen ist“.[13]

Würden sich Nicht-KRITIS-Energieversorgungsnetzbetreiber nach denselben Grenzwerten wie KRITIS-Energieversorgungsnetzbetreiber richten, dann würden vermutlich nur wenige der Nicht-KRITIS-Energieversorgungsnetzbetreiber die Grenzwerte erreichen.

Somit müssten die betroffenen Nicht-KRITIS-Energieversorgungsnetzbetreiber weder über IT-Sicherheitsvorfälle mit eingetretenem Versorgungsengpass noch über solche mit bedrohter Versorgungssicherheit Meldung erstatten. Vermutlich ist das nicht im Sinne des Gesetzgebers.

[11] Vgl. Bundesamt für Sicherheit in der Informationstechnik (2016a).
[12] Vgl. Bundesamt für Sicherheit in der Informationstechnik (2016a).
[13] Bundesamt für Sicherheit in der Informationstechnik (2016a).

Es ist unklar nach welchen Grenzwerten Nicht-KRITIS-Energieversorgungsnetzbetreiber über eine erhebliche Beeinträchtigung ihrer Strom- und Gasnetze entscheiden.

Dem BSI liegt eine schriftliche Anfrage der xmera zum Thema vor. Über die Stellungnahme werden wir berichten, sobald sie uns vorliegt.

Ausfall

Ein Ausfall liegt im Sinne des BSI bereits vor „wenn sich die Qualität der von der Anlage erbrachten kritischen Dienstleistung durch eine IT-Störung derart verschlechtert, dass sie den Anforderungen der kritischen Dienstleistung an die Qualität nicht mehr genügt."[14]

Hier haben wir es mit einem qualitativen Kriterium zu tun. Daher spielt es nun keine Rolle, ob der IT-Sicherheitsvorfall von einem KRITIS-Energieversorgungsnetzbetreiber oder einem Nicht-KRITIS-Energieversorgungsnetzbetreiber beurteilt werden muss.

Trotzdem ist es nicht einfach im Bereich der Strom- und Gasnetze von einem Qualitätsverlust zu sprechen, wenn Quantität auszuschließen ist. Denn die einschlägigen Qualitätskennzahlen der DINEN 50160 für Strom und G260 für Gas sind ungeeignet, um Qualitätseinbußen im Zusammenhang mit IT-Störungen zu messen.

Bei einem Cyber-Angriff kommt es mit großer Wahrscheinlichkeit entweder zu einem Totalausfall oder einem Teilausfall. Letzteres stellt jedoch im Sinne des BSI eine Beeinträchtigung dar.

Meldesystematik

Das BSI hat aufgrund häufiger Nachfragen Kriterien aufgestellt, anhand derer entschieden werden kann, ob eine IT-Störung gewöhnlich oder außergewöhnlich ist.

Warum von Seiten des BSI nicht die im Gesetzestext und –entwurf verwendeten Begriffe „erhebliche Störung" und „nicht erhebliche Störung" verwendet werden, wird nicht erklärt. Die Grafiken zur Meldesystematik des BSI sind online einsehbar.

[14] Bundesamt für Sicherheit in der Informationstechnik (2016a).

Die nachfolgende Grafik orientiert sich näher an den Begriffen des Gesetzestextes.

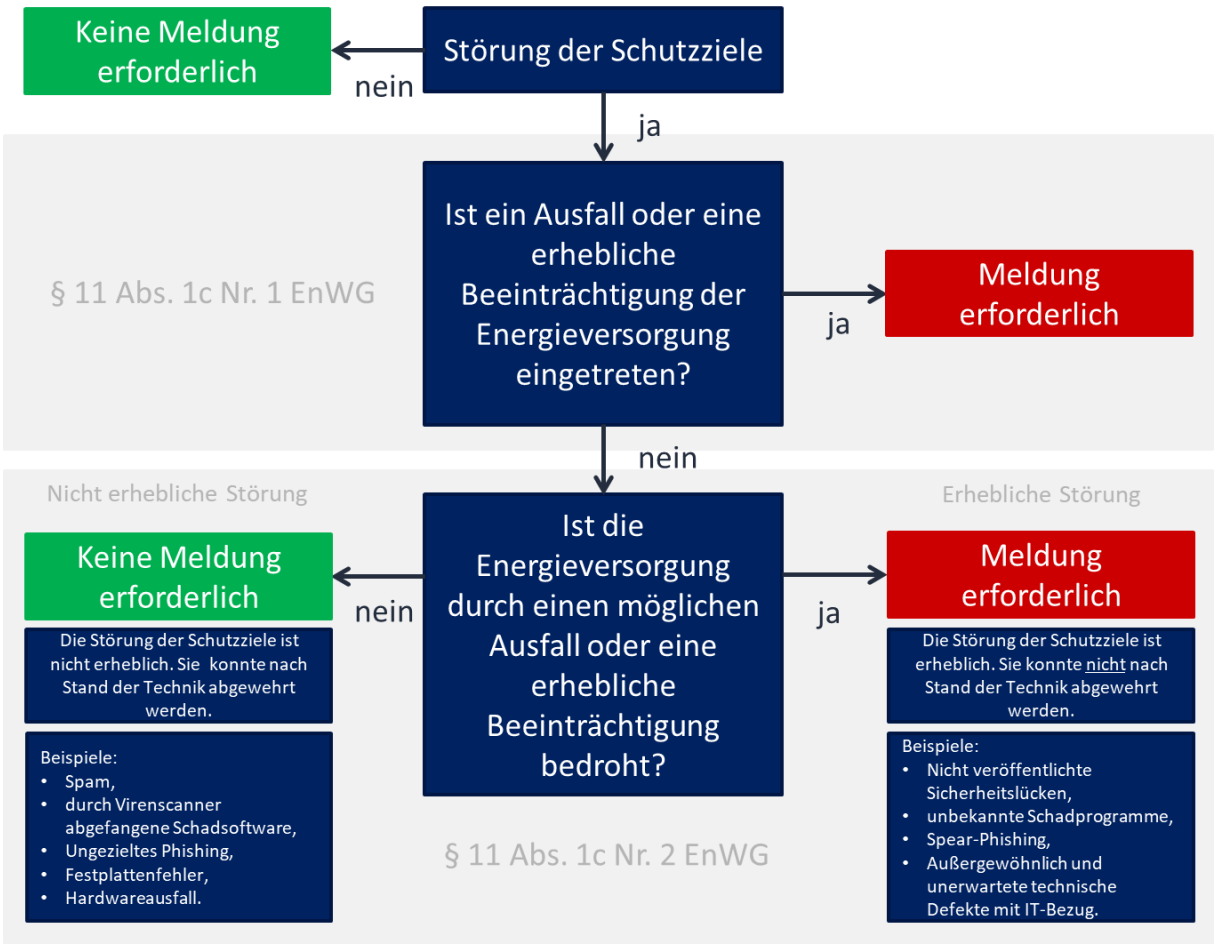

ABBILDUNG 1: MELDESYSTEMATIK § 11 ABSATZ 1C ENWG

Die Beispiele für nicht erhebliche Störungen und erhebliche Störungen entsprechen denen des BSI für gewöhnliche IT-Störungen und außergewöhnliche IT-Störungen.[15]

Welche Art von Angriffen ist zu befürchten?

Bislang sind in Deutschland noch keine IT-Störungen mit Auswirkung auf die Versorgungssicherheit von Strom oder Gas bekannt geworden.

In der Ukraine dagegen sah es im Dezember 2015 anders aus. Für mindestens 225.000 Einwohner der Ukraine lag für mehrere Stunden die Stromversorgung lahm.

Grund dafür war ein Cyber-Angriff, bei dem Schadsoftware über den Anhang einer Email in das Rechnernetz des Betreibers gelangte. Auf diese Weise konnten die Schaltanlagen der Umspannwerke mittels eingeschleuster Fernwartungssoftware manipuliert werden.

[15] Vgl. Bundesamt für Sicherheit in der Informationstechnik (2017).

Weitere gezielte Maßnahmen der Angreifer führten dazu, dass sich die Wiederherstellung der Stromversorgung schließlich deutlich verzögerte.[16]

Einer Studie der TTS Trusted Technologies and Solutions GmbH aus Juni 2017 zur Folge wird Schadsoftware als stärkste Bedrohung empfunden. Gefragt wurde nach der Risikoeinschätzung für Bedrohungen der IT-Sicherheit. Unter den Befragten schätzten 72% Schadsoftware, 55% Schwachstellen in Standardprodukten und 55% Ransomware mit hohem oder sehr hohem Risiko für eine Cyber-Bedrohung ein.[17]

Wie ist das IT-Sicherheitsniveau der Energieversorger einzuschätzen?

Sicherheitsbewusstsein

Das Risikobewusstsein im Energiesektor war bei den meisten Unternehmen auch schon vor der Umsetzungspflicht für ein ISMS stark ausgeprägt. Dabei lag der Fokus jedoch mehr auf kommerzielle Risiken und Risiken im Zusammenhang mit dem Personen- und Umweltschutz. Die Versorgungssicherheit wurde daher weniger als Teil des Risiko- und IT-Management betrachtet.[18]

IKT im KRITIS-Sektor Energie war bisher vorrangig auf die Erfüllung des Schutzziels „Verfügbarkeit“ ausgerichtet. Die Schutzziele Integrität und Vertraulichkeit wurden eher nachrangig behandelt.[19]

Mittlerweile ist das Bewusstsein für drohende Ausfälle in der Stromversorgung durch Cyber-Angriffe sehr stark ausgeprägt. Dies zeigt eine Stadtwerkestudie aus 2017, in der 73 % der Befragten die Gefahr als hoch oder sehr hoch einstuften. Lediglich 8 % schätzen die Gefahr als gering oder sehr gering ein.[20]

Ein ausgeprägtes Bewusstsein allein reicht jedoch nicht. Daher geht die Mehrheit der Energieversorger für 2017 von einem erhöhten Investitionsvolumen in IT-Sicherheit aus.

Gemeinsam mit der Branche Transport und Logistik ist die Bereitschaft der Energieversorger in IT-Sicherheit zu investieren verglichen mit anderen Branchen in Deutschland am größten.[21]

IT-Sicherheitsmaßnahmen-Index

Der aktuelle Umsetzungsgrad von IT-Sicherheitsmaßnahmen bei Energieversorgern wurde mit dem sogenannten IT- Sicherheitsmaßnahmen-Index gemessen. Der IT-Sicherheitsmaßnahmen-Index beschreibt das Maß, in dem sich eine Organisation durch selbst implementierte Sicherheitsmaßnahmen vor IT-Sicherheitsrisiken schützt. Bei

[16] Vgl. Bundesamt für Sicherheit in der Informationstechnik (2016b).
[17] Vgl. TTS (2017).
[18] Vgl. Bundesamt für Sicherheit in der Informationstechnik (2015).
[19] Vgl. Bundesamt für Sicherheit in der Informationstechnik (2015).
[20] Vgl. Edelmann, H. (2017).
[21] Vgl. Bundesdruckerei GmbH (2017).

einem Indexwert von 100 würden alle zugrunde liegenden Sicherheitsmaßnahmen angewendet werden.[22]

Energieversorger haben demnach einen überdurchschnittlichen IT-Sicherheitsmaßnahmen-Index von 63,4. In diesem Vergleich sind jedoch Banken und Versicherungen mit einem Index von 79,5 besser vor Cyber-Angriffen geschützt. Der durchschnittliche Indexwert über diverse Branchen beträgt 56,4.[23]

Zusammenfassung

Die Ausweitung der Meldepflicht auf alle Energieversorgungsnetzbetreiber ist bereits seit Inkrafttreten am 30. Juni 2017 in der Branche bekannt.

Praktische Erfahrungen mit dem Meldeprozess konnten bisher höchstens KRITIS-Energieversorger machen, da sie bereits seit gut einem Jahr zur Meldung von bestimmten IT-Sicherheitsvorfällen verpflichtet sind.

Falls es überhaupt schon Routine in diesem Prozess gibt, haben auch KRITIS-Energieversorger Korrekturen an ihm vorzunehmen. Denn der Gesetzgeber hat nicht nur den Kreis der Adressaten ausgeweitet, sondern auch die Art der meldepflichtigen Störungen.

Nicht-KRITIS-Energieversorgungsnetzbetreiber müssen sich dagegen mit der neuen Situation erst noch vertraut machen und einen Meldeprozess im Unternehmen implementieren, der dem § 11 Absatz 1c EnWG gerecht wird.

Zu den größten Herausforderungen gehören dabei die Berücksichtigung des vierten Schutzziels Authentizität und die Auslegung des Begriffs Beeinträchtigung wie er im Gesetz gebraucht wird. Hier ist unklar nach welchen Grenzwerten Nicht-KRITIS-Energieversorgungsnetzbetreiber über eine erhebliche Beeinträchtigung ihrer Strom- und Gasnetze entscheiden sollen.

Über die Stellungnahme des BSI werden wir, sobald sie uns vorliegt, berichten.

Das Thema Meldepflicht macht deutlich mit welchen Unklarheiten eine konkrete gesetzliche Vorgabe behaftet sein kann. Kommt es daher zukünftig tatsächlich zu Streitigkeiten, wird es Aufgabe der Gerichte sein, für Klarheit zu sorgen.

[22] Vgl. Bundesdruckerei GmbH (2017).
[23] Vgl. Bundesdruckerei GmbH (2017).

Literaturverzeichnis

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 (2017): Entwurf eines Gesetzes Umsetzung der Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz-und Informationssystemen in der Union, Deutscher Bundestag, 18. Wahlperiode, Drucksache 18/11242, Köln.

Bundesamt für Sicherheit in der Informationstechnik (2015): KRITIS-Sektorstudie Energie, Bonn.

Bundesamt für Sicherheit in der Informationstechnik (2016a): Häufig gestellte Fragen für Betreiber Kritischer Infrastrukturen zur Meldepflicht nach IT-Sicherheitsgesetz, Bonn.

Bundesamt für Sicherheit in der Informationstechnik (2016b): Die Lage der IT-Sicherheit in Deutschland 2016, Bonn, S. 40.

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

Bundesdruckerei GmbH (2017): Digitalisierung und IT-Sicherheit in deutschen Unternehmen, Eine repräsentative Untersuchung, erstellt von der Bundesdruckerei GmbH in Zusammenarbeit mit KANTAR EMNID, Ausgabe 2017, Berlin, S. 21.

Edelmann, H. (2017): Stadtwerkestudie 2017, Der Verteilnetzbetreiber der Zukunft – Enabler der Energiewende, Juni 2017, Dortmund.

TTS (2017): 2 Jahre nach dem IT-Sicherheitsgesetz: Wirksamkeit, Durchdringung und Akzeptanz von Informationssicherheit, Berlin und Essen.

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
Oktober 2017

Bildnachweis
Abbildungen: Eigene Darstellungen der xmera.

Titelbild: https://stockata.de

Diese digitale Broschüre ist Teil des Services für Energieversorger der xmera. Die Broschüre wird kostenlos abgegeben und ist nicht zum Verkauf bestimmt.

x m e r a : werte schützen