Bewertung aktueller Cybersecurity Rechtslagen- und -änderungen für KRITIS-Betreiber der Energieerzeugung*

Stefan Loubichi

Abstract

The German energy industry is currently confronted with a large number of new cybersecurity regulations. On the one hand, these are to be found at the European level. On the other hand, they can be found at national level. In addition, some of the regulations are contradictory.

This paper first gives an overview of which regulations need to be known in cybersecurity. This article describes which requirements will have to be taken into account in the following regulations in future:

- *NIS Directive 2.0 (draft)*
- *IT-Security Law 2.0*
- *BSI Kritis Regulation 2.0 (draft)*
- *Telecommunication Law*
- *EU Directive on the Resilience of Critical Infrastructure (draft)*

The energy transition has certainly demanded considerable flexibility from the energy industry for the last years and will continue to do so in future. Digitalisation (in which we are not a frontrunner in Germany) will also require us to continuously change the IT/OT structures.

For this reason, it is understandable that cybersecurity is not always given the highest priority. However, in order to achieve this, the new regulations were built to help the energy industry prevent a blackout due to a cyber attack.

This paper is intended to help CISOs and CIOs, but also the corresponding I&C and IT department heads, to identify which legal requirements will have to be proven in future. It should also be mentioned at this point that penalties of up to 10 million EUR can be incurred in the event of non-implementation.

Autor

Prof. h.c. PhDr. Dipl.-Kfm./Dipl.-Vw. Stefan Loubichi
international experienced lead auditor for management systems (ISO 27001, ISO 14001, ISO 9001, ISO 45001, ISO 26000), auditor according to § BSI-Law and IT-security catalogue
Essen, Deutschland

Systematische Einordnung der relevanten Gesetze, Verordnungen und Richtlinien

Betrachten wir uns erst einmal, welche Gesetze, Verordnungen und Standards man zum gegenwärtigen Zeitpunkt im Bereich der Cybersecurity für Energieerzeuger kennen sollte:

Auf Europäischer Ebene sind die nachfolgenden Richtlinien und Verordnungen in Sachen Cybersecurity für Energieerzeuger von Relevanz:

- NIS Direktive (EU) 2016/1148 [16]
- NIS Direktive 2.0 (KOM 2020/823) [17]
- EU Cybersecurity Act 2019/881 [18]
- EU-Verordnung 2016/631 zur Festlegung eines Netzkodexes mit Netzanschlussbestimmungen für Stromerzeuger [04]
- Richtlinie 2018/172 Kodex für die elektronische Kommunikation [07]
- Europäisches Programm für den Schutz kritischer Infrastrukturen KOM (2006) 786 [11]
- COM (2020) 829 Richtlinienvorschlag über die Resilienz kritischer Einrichtungen [13]
- Richtlinie (EU) 2019/944 Elektrizitätsbinnenmarkt [14]
- Verordnung (EU) 2019/943 Elektrizitätsbinnenmarkt [15]

Vor allem die Nummern 1.-3. und 5.-7. der o.g. Liste müssen stets beachtet werden, will man sich ernsthaft mit der Thematik Cybersecurity bei Energieerzeugern auf EU-Ebene beschäftigen.

National sind in Deutschland derzeit alle folgenden sieben Gesetze und Verordnungen zwingend zu beachten bzw. zu berücksichtigen:

- IT-Sicherheitsgesetz 2.0 [19]
- Energiewirtschaftsgesetz [03]
- Telekommunikationsgesetz [06]
- BSI Kritis-Verordnung [20]
- Entwurf zur BSI Kritis-Verordnung 2.0 [21]

*) (ohne Kernkraftwerke)

- IT-Sicherheitskatalog Netze [22]
- IT-Sicherheitskatalog Erzeuger [23]
- Bundesdatenschutzgesetz [25]

Als Stand der Technik in Sachen Cybersecurity sollten derzeit in Deutschland von den Energieerzeugern folgende Publikationen beachtet werden:

- Teletrust, Stand der Technik [24]
- bdew Whitepaper 2.0 [26]
- NIST SP 800-53 Rev. 5 [27]
- BSI ICS-Security-Kompendium [28]
- BSI IT-Grundschutz-Kompendium [29]
- ISO/IEC 27001 [30]
- ISO/IEC 27002 [31]
- ISO/IEC 27019 [32]

Der Entwurf der europäischen NIS Direktive 2.0

Nachdem die erste NIS Direktive [16] in die Jahre gekommen ist, die Cyberbedrohungslage immer dramatischere Formen annimmt und die Cyberabwehr in der Europäischen Union leider nicht einheitlich umgesetzt wird, hat man sich zu einer Revision entschlossen und am 16. Dezember 2020 einen entsprechenden Legislativvorschlag vorgelegt.

Die wichtigsten Punkte für Energieerzeuger sind dabei:

1. Es wird gemäß Artikel 2 eine Ausweitung des Anwendungsbereiches angestrebt, wobei zehn wesentliche und sechs wichtige Sektoren vorgeschlagen werden. Klein- und mittelständische Unternehmen (KMUs) sollen zwar ausgeschlossen werden, aber es wird auf die Empfehlung 2003/361/EG verwiesen. Unternehmen, deren Anteile zu mindestens zu 25 % in Händen der öffentlichen Hand liegen, können aber -unabhängig von ihrer de facto Größe- nicht als KMU definiert werden und würden deshalb stets unter die Prüfpflicht fallen.

Da keine Aufteilung des Anwendungsbereiches durch das Kriterium „kritische Funktionalität für die Gesellschaft“ vorgenommen wird, würden zukünftig in Deutschland circa 2.000 Unternehmen im

Sektor Energie von der NIS Direktive 2.0 betroffen werden. Dies wird von einzelnen Branchenverbänden als nicht verhältnismäßig angesehen, während die ENISA die Auffassung vertritt, dass jeder Ausfall eines Nicht-KMU im Energiesektor weitreichende Folgen hätte.

2. Die Anbieter digitaler Infrastrukturen, wie z.B. Anbieter von Cloud-Diensten, Datenzentren, Content Delivery, Networkanbieter oder Vertrauensdienste werden durch die NIS Direktive 2.0 jetzt ebenfalls eingebunden.

3. Hard- und teilweise auch Softwarehersteller werden nach der neuen NIS Direktive 2.0 Anforderungen der Sicherheit ihrer eigenen informationstechnischen Systeme genügen müssen, gleichwohl will die EU nicht dem Wunsch der Betreiber nachkommen, Hersteller und Anbieter von IKT-Produkten, -Dienstleistungen und -Prozessen zu einem risikoorientierten und adäquaten Umgang mit Grundprinzipien der IT-Sicherheit (z.B. Security by Design) zu verpflichten. Auch lehnt es die Europäische Union eine Erweiterung der Produkthaftung gemäß Richtlinie 85/374/EWG um Aspekte der IT-Sicherheit ab.

4. Die NIS Direktive 2.0 widmet sich auch der Cybersicherheitsrisiken entlang kritischer Lieferketten. Gemäß Artikel 19 der NIS Direktive 2.0 soll eine NIS Koordinationsgruppe beauftragt werden, strukturiert und koordiniert Risikobewertungen von Lieferketten durchzuführen, um für jeden Sektor die kritischen IKT-Dienste, -Systeme -und -Produkte als auch relevante Bedrohungen und Schwachstellen zu ermitteln. Auch sollen Betreiber gemäß Art. 18 Abs. 2 d) im Rahmen des Risikomanagements verpflichtet werden, Maßnahmen für die Sicherheit von Lieferketten umzusetzen.

5. Gemäß Artikel 21 der NIS Direktive 2.0 wird die Möglichkeit geschaffen, dass Mitgliedsstaaten von der EU verpflichtet werden können, nur noch bestimmte – zuvor auf EU-Ebene- zertifizierte IKT-Produkte, -Dienstleistungen oder -Prozesse einsetzen zu dürfen. Einige Verbände sehen hier einen Verstoß gegen die im EU Cybersecurity Act ausgesprochene Freiwilligkeit von Cybersicherheitszertifizierungen.

6. Nach Artikel 29 Ziffer 4 Buchstaben h) und f) sollen Betreiber kritischer Infrastrukturen angewiesen werden können, Aspekte der Nichteinhaltung der Richtlinie veröffentlichen zu müssen. In diesem Zusammenhang soll auch bekannt gegeben werden, wer, d.h. welche i.d.R. juristische Person einen Verstoß gegen die Richtlinie begangen hat. Darüber hinaus ist es bei Verstößen gegen die Richtlinie möglich, dass die Kommission gemäß Artikel 29 Ziffer 5 Buchstabe a) die Möglichkeit hätte, in den operativen Betrieb einer wesentlichen Einrichtung einzugreifen. Nach Artikel 31, 33 wäre eine Verhängung von Geldbußen möglich, wobei diese jedoch auf ein Höchstmaß von 10 Mio. EUR begrenzt werden würden.

7. Die NIS Direktive 2.0 verpflichtet die Kritis-Betreiber darauf, erhebliche sowie potenzielle zukünftige IT-Sicherheitsvorfälle zu melden. Erfreulich ist dabei, dass in Artikel 20 Ziffer 3 eine eindeutige Definition von erheblichen Sicherheitsvorfällen vorgenommen wurde.

Natürlich wird der Referentenentwurf der NIS Direktive 2.0 in einigen Punkten verändert. Gleichwohl zeigt er aber das Bemühen, die kritischen Infrastrukturen auf europäischer Ebene einheitlicher zu schützen, da Cybersicherheit im Energiebereich nur auf europäischer Ebene sichergestellt werden kann.

IT-Sicherheitsgesetz 2.0 – kein Glanzstück eines Gesetzes

Das am 23. April 2021 vom Bundestag beschlossene IT-Sicherheitsgesetz 2.0 liefert einiges an Licht, leider aber auch viel Schatten. Da bereits mehrfach über das IT-Sicherheitsgesetz 2.0 in seinen verschiedenen Facetten und Revisionen berichtet wurde, wird das IT-Sicherheitsgesetz 2.0 hier nur am Rande erörtert.

Positiv hervorzuheben ist, dass im IT-Sicherheitsgesetz 2.0 von einem ausufernden Einsatz technischer Richtlinien abgesehen wurde, so dass ein Spielraum besteht, den Stand der Technik für Technik, das IT-Sicherheitskennzeichen und die Herstellererklärung zum Einsatz von kritischen Komponenten in einfacher Art und Weise zu konkretisieren. Bei zentralen Anforderungen des IT-Sicherheitsgesetzes 2.0 wird leider des Öfteren auf untergesetzliche Vorgaben verwiesen, was nur ein Pyrrhussieg für Gegner des IT-Sicherheitsgesetzes 2.0 ist, denn die zusätzlich gewonnene Zeit für Unternehmen wird mit einem Mangel an Rechtssicherheit erkauft.

Wenn man wesentliche Bereicherungen der Cybersecurity in dem Gesetz festmachen kann, so bestehen diese darin, dass

- gemäß § 8a Abs. 1a BSI-Gesetz ein verpflichtender Einsatz von Systemen zur Angriffserkennung bei KRITIS-Betreibern vorgeschrieben ist.
- eine Detektion von Sicherheitsrisiken für Netz- und IT-Sicherheit und von Angriffsmethoden gemäß § 7b BSI-Gesetz durch das BSI erfolgen kann
- nach § 8f BSI-G Unternehmen im besonderen öffentlichen Interesse zumindest eine Selbsterklärung zur IT-Sicherheit beim BSI abgeben müssen
- kritische Komponenten gemäß § 9b BSI-Gesetz nur eingesetzt werden dürfen, wenn der Hersteller eine entsprechende Garantieerklärung abgegeben hat.

Kommen wir nun zu den beiden Ergänzungen, die am Tage vor der Abstimmung im Bundestag durch den Innenausschuss ergänzt wurden:

- Der Begriff der Unternehmen im öffentlichen Interesse wird durch den Zusatz „wesentliche Zulieferer der nach ihrer inländischen Wertschöpfung größten Unternehmen in Deutschland“ ergänzt.
- Eine „voraussichtliche Beeinträchtigung der öffentlichen Sicherheit und Ordnung“ wird als weiterer Grund benannt, bezüglich derer das Bundesministerium des Inneren den Einsatz einer kritischen Komponente untersagen.

Dass man derartige Veränderungen einen Tag (!) vor der Verabschiedung im Bundestag durch den Innenausschuss vornimmt, ist ebenso unglücklich wie der Sachverhalt, dass die Verbände im Vorfeld einmal nur 24 Stunden Zeit hatten, um eine Stellungnahme abzugeben.

Die BSI – Kritis-Verordnung 2.0 – ein Entwurf zum …..

Betreibt eine Organisation oder ein Unternehmen eine Kritis-Anlage und überschreitet dann noch den entsprechenden Schwellenwert, so wird die Organisation bzw. das Unternehmen zu einem prüfpflichtigen Kritis-Betreiber.

Die sogenannte KRITIS-Verordnung basiert auf dem seit Juli 2015 gültigen IT Sicherheitsgesetz, welches im April 2021 als so genanntes IT-Sicherheitsgesetz 2.0 auf den Weg gebracht wurde. Der erste Teil der Kritis-Verordnung trat am 3. Mai 2016 in Kraft, der zweite Teil am 21. Juni 2017. Während bis dato die Sektoren Energie, Wasser, Ernährung, Informationstechnik und Telekommunikation, Gesundheit, Finanz- und Versicherungswesen sowie Transport und Verkehr nahezu identisch dahingehend behandelt wurden und dass eine Prüfpflicht erst ab einer betroffenen Relevanz von 500.000 betroffenen Menschen begann, hat man in der neuen Fassung, d.h. in dem derzeit zur Kommentierung vorliegenden Referentenentwurf neue Definitionen, neue Schwellenwerte sowie eine Haftungsänderung eingeführt.

Der Begriff der kritischen Dienstleistung ist uns mit folgender Definition erhalten geblieben: *„Dienstleistung zur Versorgung der Allgemeinheit in den o.g. Sektoren, deren Ausfall oder Beeinträchtigung zu erheblichen Versorgungsengpässen oder zu Gefährdungen der öffentlichen Sicherheit führen würde.“* Aber was versteht man mittlerweile unter Anlage?

Betrachten wir hierzu die Definition einer Anlage gemäß § 1 Nr. BSI-Kritis-Verordnung ändern soll. Neben

- Betriebsstätten und sonstigen ortsfesten Einrichtungen, die für die Erbringung einer kritischen Dienstleistung notwendig sind
- Maschinen, Geräten und sonstigen ortsveränderlichen Einrichtungen, die für die Erbringung einer kritischen Dienstleistung notwendig sind

wird nun ein weiteres Faktum aufgeführt, welches die Definition einer Anlage erfüllen würde:

Software und IT-Dienste, welche für die Erbringung einer kritischen Dienstleistung notwendig sind.

In der Begründung zur BSI-Kritis-Verordnung findet sich keinerlei Hinweis, welche Software oder welche IT-Dienstleistungen unter § 1 Nr. 1 c zu subsumieren sind. Leittechniksoftware dürfte unstrittig unter den Begriff der Software fallen, aber was sind für die kritischen Dienstleistungen notwendige IT-Dienste. Der Betrieb eines Rechenzentrums könnte ebenfalls eher unstrittig sein. Prinzipiell wäre es aber wichtig und hilfreich, wenn definiert würde, was man konkret unter der relevanten Software und den relevanten IT-Dienstleistungen versteht.

Aufgrund der fehlenden Spezifizierung in der Verordnung müsste man die Normen als State of the Art heranziehen. Die entsprechende Norm wäre hier die ISO/IEC 24765 [01].

Hiernach versteht man unter Softwaretechnik die Anwendung eines systematischen, disziplinierten und quantifizierbaren Ansatzes auf die Entwicklung, den Betrieb und die Wartung von Software, das heißt die Anwendung der Prinzipien des Ingenieurwesens auf Software. Software sind dabei als Programme und ggf. die dazugehörige Dokumentation und weitere Daten, die zum Betrieb eines Computers notwendig sind. Mit dieser Definition kommt man hier aber nicht weiter.

Es ist davon auszugehen, dass die Verbände genau hier ansetzen werden, um die Software als Anlagendefinition „herauszukegeln“. Dies mag vielleicht aus den Insidern bekanntem Grund gelingen, aber man dürfte in diesem Falle nicht vergessen, dass 2 Jahre nach der Verabschiedung der BSI-Kristis Verordnung diesmal auch wirklich eine Evaluation mit anschließender Anpassung erfolgen wird, so dass man aller Voraussicht nach maximal zwei Jahre gewinnt, wobei diese zusätzlichen zwei Jahren mit einer geringeren Cybersecurity erkauft werden würden.

Eine weitere -ebenfalls nicht in der Begründung kommentierte- Erweiterung erfährt der Anlagenbegriff dadurch, dass es jetzt heißt:

„Mehrere Anlagen, die durch einen betriebstechnischen Zusammenhang verbunden sind, gelten als gemeinsame Anlage, wenn Sie zur Erbringung derselben kritischen Leistung notwendig sind.“ Man mag hier aus pragmatischer Sicht zum Beispiel bei einem Pumpspeicherkraftwerk sicherlich Verständnis hinsichtlich dieser Spezifizierung aufbringen können, aber wie sieht dies bei einem Windpark oder einem anderen differenten Fall aus: Wie sieht dies bei Software als Anlage aus? Die meisten KRITI-Betreiber nutzen ERP Unternehmenssoftware wie zum Beispiel SAP S/4HANA, so dass man sich bei einer Verbindung mit dem Produktivsystem fragen muss, ob dann nicht auch noch zwangsläufig die gesamte SAP S/4 HANA ERP-Lösung mit betrachtet werden müsste. Bei strenger Betrachtungsweise wäre dies nach dem vorliegenden Referentenentwurf der Fall.

Spannend ist auch die Haftungserweiterung gemäß § 1 Nr. 2 S. 2 BSI Kritis-V:

„Betreiben zwei oder mehr Personen gemeinsam eine Anlage, so ist jeder für die Erfüllung der Pflichten als Betreiber verantwortlich.“

Laut enArgus [02], dem zentralen Informationssystem der Energieforschungsförderung der Bundesrepublik Deutschland ist ein Kraftwerksbetreiber wie folgt definiert:

„Ein Kraftwerksbetreiber ist ein Marktteilnehmer in der elektrischen Energieversorgung. Seine Aufgabe ist es, ein Kraftwerk zu steuern. Er verfügt damit über die Kraftwerksleistung und bestimmt deren Einsatz. Der Betreiber eines Kraftwerks kann sowohl der Eigentümer der Anlage, als auch der der Pächter der Anlage sein. Betreiber eines Kraftwerks sind natürliche oder juristische Personen sowie Personenvereinigungen. Wird die Anlage in einem Betrieb bzw. in einem Unternehmen eingesetzt, ist der Betriebsinhaber bzw. der Unternehmensinhaber der Anlagenbetreiber.“

Dieser Begriff wäre wahrscheinlich zielführender als der aus § 3 Nr. 18 EnWG [03]:

„Energieversorgungsunternehmen sind natürliche oder juristische Personen, die Energie an andere liefern, ein Energieversorgungsnetz betreiben oder an einem Energieversorgungsnetz als Eigentümer Verfügungsbefugnis besitzen; der Betrieb einer Kundenanlage oder einer Kundenanlage zur betrieblichen Eigenversorgung macht den Betreiber nicht zum Energieversorgungsunternehmen.“

Gleich, welche Definition angewandt werden wird, kann man davon ausgehen, dass die Haftung zukünftig eine andere sein wird.

Schauen wir uns an dieser Stelle einmal an, welche Anlagentypen und Schwellenwerte es jetzt in der Stromversorgung gibt:

1. Stromerzeugung:

Erzeugungsanlage
Bewertungskriterium: installierte Maximalkapazität (elektrisch) in MW
Schwellenwert 36 (vormals 420)

Dezentrale Energieerzeugungsanlage
Bewertungskriterium: installierte Maximalkapazität (elektrisch) im MW
Schwellenwert 36 (vormals 420)

Speicheranlage
Bewertungskriterium: installierte Nettonennleistung (elektrisch) in MW
Schwellenwert: 420 (unverändert)

Anlage oder System zur Steuerung / Bündelung elektrischer Leistung
Bewertungskriterium: installierte Nettonennleistung (elektrisch) in MW
Schwellenwert: 420 (unverändert)

Der vormals definierte Anlagetypus Erzeugungsanlage mit Wärmeauskopplung, d.h. die KWK Anlage) wurde aus der Verordnung gestrichen.

2. Stromübertragung:

Übertragungsnetz:
Bewertungskriterium: Entnommene Jahresarbeit in GWh/Jahr
Schwellenwert: 3.700 (unverändert)

Zentrale Anlage und System für den Stromhandel
Bewertungskriterium: Handelsvolumen an der Börse in TWh/Jahr:
Schwellenwert: 3700 (vormals 200)

3. Stromverteilung:

Verteilernetz
Bewertungskriterium: Entnommene Jahresarbeit in GWh/Jahr
Schwellenwert: 3.700 (unverändert)

Das Bundesministerium des Inneren verweist hinsichtlich der unterschiedlichen Schwellenwerte darauf, dass für Energieerzeugungsanlagen und dezentrale Energieerzeugungsanlagen nicht mehr der Regelschwellenwert von 500.000 versorgten Personen zu Grunde gelegt wird, sondern Absatz 5 Satz 3 der EU-Verordnung 2016/631 [04]. Dass eine Senkung des Schwellenwertes für Energieerzeugungsanlagen von 420 auf mindestens 50 MW aus EU-Vorgaben erfolgen muss, hat der Verfasser dieses Artikels bereits in einem Artikel im VGB PowerTech Journal 03/2020 [05] vorhergesagt. Bei einem Vortrag des Verfassers dieses Artikels auf dem Kraftwerkstechnischen Kolloquiums 2020 in Dresden zu exakt dieser Thematik kannte niemand die vorstehend erwähnte EU-Verordnung. Somit erfolgt hier nicht eine willkürliche Schlechterstellung der Energieerzeuger gegenüber anderen Betreiber kritischer Infrastrukturen.

Interessant wird nunmehr sicherlich sein, wie es zu bewerten sein wird, dass die früher als „heilige Kuh“ gehandelte 500.000 Bemessungsgrundlage durchbrochen wird. Hier darf aber nicht vergessen werden:

LEX SPECIALIS DEROGAT LEGI GENERALI

Gemäß diesem Rechtsgrundsatz geht eine spezielle Regelung immer der generellen Regelung vor. Eine Norm ist dann spezieller als andere, wenn erstere zusätzlich zu sämtlichen Tatbestandsmerkmalen der Letzteren mindestens noch ein weiteres Kriterium enthält. Neben der Orientierung an der Bezugsgröße von 500.000 zu versorgenden Personen, müssen Energieerzeuger eine zusätzliche Anforderung ge-

mäß Absatz 5 Satz der EU-Verordnung 2016/631 erfüllen. Somit liegt aller Voraussicht nach ein Musterfall des Rechtsgrundsatzes lex spezialis derogat legi generali vor, an dem sich auch die Gerichte orientieren müssten.

Gemäß Begründung zur BSI Kritis-Verordnung 2.0 ist im Übrigen mit 150 neuen Stromerzeugern zu rechnen, welche neu in die Kategorie Kritis-Betreiber fallen.

Die TKG – Novelle

Das Telekommunikationsgesetz (TKG) vom 21. April 2021, erfährt leider ein Nischendasein bei KRITIS-Betreibern, obgleich es durchaus eine hinreichende Relevanz hat. Mit dem TKG wird die EU-Richtlinie 2018/1972 in nationales Recht umgesetzt.

Die für Kritis-Betreiber relevanten Schwerpunkte der TKG – Novelle liegen in den nachfolgenden Bereichen:

- Verbesserung der Informationen über telekommunikationsrelevante Infrastrukturen
- Modernisierung der Frequenzverwaltung
- Modernisierung des Universaldienstes inkl. Verankerung des Rechts auf angemessene Versorgung mit Telekommunikationsdiensten
- Anpassung der Verpflichtungen im Bereich der öffentlichen Sicherheit an veränderte Bedürfnisse und technische Entwicklungen
- Integration und Anpassung an den veränderten Bedarf der Nachfrager der den Bereich Telekommunikation betreffenden Vorschriften des Gesetzes zur Sicherstellung von Postdienstleistungen und Telekommunikationsdiensten
- Neuregelung organisatorischer und verfahrensrechtlicher Fragen der Bundesnetzagentur
- Überarbeitung des Bußgeldkataloges

Nun zu den einzelnen Herausforderungen des neuen TKG:

Vorratsdatenspeicherung:

Man kann aus verschiedenen Gründen pro oder contra Vorratsdatenspeicherung sein. Seit Jahren kassieren unsere höchsten Gerichte auf nationaler und europäischer Ebene legislative Anordnungen hierzu. Durch den § 113b TKG wird wieder versucht, die Vorratsdatenspeicherung einzuführen. Es bleibt zu befürchten, dass den höchsten Gerichten irgendwann einmal der Geduldsfaden reißt und das gesamte TKG für nichtig erklärt werden könnte, so dass dann auch keine Gesetzesgrundlage für den Ausbau der Netze gegeben wäre.

Manuelles und automatisiertes Auskunftsverfahren gemäß §§ 112 f. TKG:

Während im § 113 TKG (Manuelles Auskunftsverfahren) dezidiert festgelegt ist, welche Daten unter welchen Voraussetzungen an welche Behörde zur Verfügung gestellt werden können, ist in § 112 TKG (Automatisiertes Auskunftsverfahren) nur rudimentär geregelt, welche Daten an welche Behörden zur Verfügung gestellt werden.

Nun könnte man natürlich bei entsprechendem Vertrauen in den Staat argumentieren, dass der Staat schon weiß, warum er welche Daten benötigt. Das Problem liegt aber darin, dass gemäß §§ 112 f. TKG eine Richtlinie erlassen werden muss, an dem die wesentlichen Anforderungen an die technischen Verfahren festzulegen sind. Es stellt sich deshalb die Frage, unter welchen technischen Sicherheitsstandards zum jetzigen Zeitpunkt überhaupt eine Datenübertragung stattfindet oder ob man vielleicht bis zum Inkrafttreten einer Richtlinie mit der Übertragung wartet.

Man muss hier auch an eine der unzähligen Versionen des IT-Sicherheitsgesetzes 2.0 denken, wo es hieß, dass Kritis-Betreiber an das Bundesamt für Sicherheit (BSI) eine entsprechende Assetliste übersenden sollten. Man hat dann darauf verzichtet, da man wohl der technischen Übertragung an das BSI nicht getraut hat oder Angst hatte, dass die Daten im BSI „verloren“ gehen könnten. Gerade bei der automatisierten Auskunftserteilung könnte es eine Katastrophe darstellen, wenn das Übertragungsverfahren technische Fehler aufweisen würde, durch die ausländische Cyberkriminelle oder Cyberterroristen an relevante Telekommunikationsdaten gelangen würden. Mit größtmöglicher technischer Sorgfalt bei gleichzeitiger Kürze der Zeit muss eine entsprechende Verordnung erlassen werden, die gemäß dem Stand der Technik hier maximale Sicherheit gewährleistet. Durch die verstärkte Verwendung von 5G bei Energieerzeugern erhält dieser Sachverhalt eine sehr große Relevanz.

Man muss sich in diesem Zusammenhang aber auch etwas anderes fragen:

Gemäß §§ 112 f. TKG haben die Verpflichteten alle technischen Vorkehrungen in ihrem Verantwortungsbereich auf eigene Kosten zu treffen, welche für die Erteilung der Auskünfte erforderlich sind. Dazu gehört auch die Anschaffung der zur Sicherstellung der Vertraulichkeit und des Schutzes vor unberechtigten Zugriffen erforderlichen Geräte.

Wir alle wissen, welch riesiger Preiskampf im Telekommunikationsmarkt herrscht und dass einige TKG-Verpflichteten es sich kaum aus monetärer Sicht leisten können, die sicherheitstechnisch besten Optionen anzuschaffen, so dass hierdurch ein latentes Sicherheitsrisiko entstehen könnte.

So gut gemeint das TKG in diesem Sinne vielleicht einmal gemeint gewesen sein mag, so kann es zu einem großen Sicherheitsrisiko werden oder es wird eine nicht gerade kleine Marktbereinigung erfolgen.

IMSI-Catcher:

Mobilfunknetzbetreiber müssen zukünftig gewährleisten, dass Sicherheitsbehörden IMSI-Catcher zum Orten und Abhören in künftigen Netzen wie dem gerade implementierten Netz der fünften Generation (5G) nutzen dürfen. IMSI-Catcher senden dabei mit einem stärkeren Signal als Basisstationen der offiziellen Netzbetreiber, sodass sich Smartphones dort einwählen werden und dann von den Sicherheitsbehörden einfacher überwacht werden können. Abgesehen davon, dass das Ergebnis einer Liveabstimmung auf heise-online ergab, dass 92 % der Auffassung sind, dass die Überwachungsgesetze der Bundesregierung zu weit gehen, muss aus Cybersecurity-Gesichtspunkten berücksichtigt werden, dass auf jeden Fall sichergestellt sein müsste, dass die IMSI-Catcher nicht missbräuchlich eingesetzt werden können.

Zu bedenken gibt bei dem neuen TKG, dass keine Evaluierung vorgesehen ist, ob die gewählten Maßnahmen überhaupt geeignet sind, Kriminalität im Internet zu bekämpfen.

Es stellt sich in diesem Zusammenhang die Frage, welche Sicherheitsanforderungen man in Telekommunikationsbereich derzeit als Stand der Technik ansehen kann. Hier erlaubt der Autor auf den von der Bundesnetzagentur am 29.04.2020 herausgegebenen Katalog von Sicherheitsanforderungen für das Betreiben von Telekommunikations- und Datenverarbeitungssystemen sowie für die Verarbeitung personenbezogener Daten nach § 109 TKG [08] (jedoch die alte Fassung) zu verweisen. In diesem Katalog werden folgende Gruppen von Sicherheitsanforderungen benannt:

- Organisation
- Sicherheit im Personalmanagement
- Sicherheit von Daten, Systemen und Einrichtungen
- Betriebsführung
- Störungen und Sicherheitsvorfälle
- Not- und Ausfallmanagement
- Überwachungs- und Testverfahren
- Beurteilung der Sicherheitsdaten
- Einhaltung der gesetzlichen Anforderungen

Ende-zu-Ende-Verschlüsselung:

Eine weitere Herausforderung bahnt sich gerade im Telekommunikationsbereich an:

Durch den seit Dezember 2020 geltenden Europäischen Kodex für die Telekommunikation fallen Kommunikationsdienste unter die E-Privacy Richtlinie aus dem Jahr 2002. Die Europäische Kommission will im ad hoc Verfahren eine Übergangsverordnung einführen, wonach EU-seitig die laufende E-Mail-Kommunikation automatisch auf Abbildungen von Kindesmissbrauch überprüfen kann. Prinzipiell ist der Kampf gegen Kindesmissbrauch immer zu begrü-

ßen, aber die E-Privacy-Richtlinie [09] von 2002 bietet keine Rechtsgrundlage für eine anlasslose Überwachung von Online-Kommunikation. Viele Unternehmen, welche sichere E-Mail-Dienste und Verschlüsselung für die Cloud anbieten, warnen derzeit davor, dass dies de facto das Ende der Ende-zu-Ende-Verschlüsselung bedeuten würde. Dies betrifft erst einmal die private Online-Kommunikation, aber der Aufhebung der Ende-zu-Ende-Verschlüsselung in der privaten Online-Kommunikation dürfte zwangsläufig zeitnah das Ende in der Business-Online-Kommunikation folgen, denn wie wollte man ansonsten verhindern, dass der Austausch krimineller Inhalte nicht über die Business-Online-Kommunikation erfolgt.

Auch bei Kritis-Betreibern ist die Ende-zu-Ende-Verschlüsselung in der elektronischen Kommunikation von grundlegender Bedeutung und eine prinzipielle Aufhebung der Ende-zu-Ende-Verschlüsselung würde dazu führen, dass auch für die Cybersecurity relevante Daten leichter in die Hände von Cyberkriminellen oder Cyberterroristen fallen könnten.

Auch bei der europäischen ePrivacy-Verordnung passiert derzeit viel. Eigentlich sollte die neue Revision der ePrivacy-Verordnung zeitgleich zur Datenschutzgrundverordnung (DSGVO) 2018 in Kraft getreten. Dies wurde aber immer auf EU-Ebene verhindert. Unerwartet hat man sich nun am 10.02.2021 auf den portugiesischen Entwurf zur ePrivacy-Verordnung geeinigt.

Der 2021er-Entwurf enthält vielfältige Ausnahmen von der bisher enthaltenen Einwilligungspflicht für die Nutzung von Cookies und ähnlichen Technologien, welche auf Informationen im Endgerät zugreifen oder diese darauf speichern. Ohne auf die Thematik weiter einzugehen, sei hier nur auf die Stellungnahme des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit vom 10.02.2021 wie folgt verwiesen [10]: „Wenn die ePrivacy-Verordnung so bleibt, wie der Rat der EU sie heute beschlossen hat, wäre das ein schwerer Schlag für den Datenschutz. Ich appelliere dringend an das Europäische Parlament und die EU-Kommission während der Trilog-Verhandlungen für eine Anhebung des Datenschutzniveaus einzutreten."

Vieles, was man im Bereich der Gesetzmäßigkeiten in Sachen Telekommunikation ändern will, wurde sicher auf der Grundlage bester Absichten geplant. Leider gilt aber auch heute noch der Grundsatz: „Gut gemeint ist nicht immer gut gemacht."

Der Entwurf der EU-Richtlinie über die Resilienz kritischer Einrichtungen

Die europaweite Bedeutung kritischer Infrastrukturen wird von der Europäischen Union seit Langem anerkannt. So hat die EU zum Beispiel 2006 das Europäische Programm für den Schutz kritischer Infrastrukturen (EPSKI) [11] aufgelegt und 2008 die Richtlinie über europäische kritische Infrastrukturen (EKI) [12] angenommen. Diese Richtlinie, die nur für den Energie- und den Verkehrssektor gilt, sieht ein Verfahren zur Ermittlung und Ausweisung von (EKI) vor, deren Störung oder Zerstörung erhebliche grenzüberschreitende Auswirkungen in mindestens zwei Mitgliedstaaten hätte. Außerdem werden in ihr bestimmte Schutzanforderungen für die Betreiber von EKI und die zuständigen Behörden der Mitgliedstaaten festgelegt. Bisher wurden 94 EKI ausgewiesen, von denen zwei Drittel in drei Mitgliedstaaten in Mittel- und Osteuropa liegen. Der Anwendungsbereich der EU-Maßnahmen zur Resilienz kritischer Infrastrukturen geht jedoch über diese Maßnahmen hinaus und umfasst auch sektorspezifische und sektorübergreifende Maßnahmen, unter anderem in den Bereichen Klimasicherung, Katastrophenschutz, ausländische Direktinvestitionen und Cybersicherheit.

Diese Richtlinie wird im Übrigen eine andere Rechtswirkung erfahren als EPSKI und EKI.

Anders als die Richtlinie 2008/114/EG, die auf Artikel 308 des Vertrags zur Gründung der Europäischen Gemeinschaft (entspricht dem derzeitigen Artikel 352 des Vertrags über die Arbeitsweise der Europäischen Union) beruht, stützt sich dieser Richtlinienvorschlag auf Artikel 114 AEUV, in dem die Angleichung der Rechtsvorschriften zur Verbesserung des Binnenmarktes vorgesehen ist. Dies ist aufgrund der Verlagerung des Ziels, Anwendungsbereichs und Gegenstands der Richtlinie, der zunehmenden wechselseitigen Abhängigkeiten und der notwendigen Schaffung einheitlicherer Ausgangsbedingungen für kritische Einrichtungen gerechtfertigt. Anstatt eine begrenzte Anzahl physischer Infrastrukturen zu schützen, deren Störung oder Zerstörung erhebliche grenzüberschreitende Auswirkungen hätte, besteht das Ziel darin, die Resilienz der Einrichtungen in den Mitgliedstaaten zu verbessern, die entscheidend für die Erbringung von Diensten sind, die in einer Reihe von Sektoren, die das Funktionieren vieler anderer Wirtschaftszweige der Union stützen, für die Aufrechterhaltung essenzieller gesellschaftlicher Funktionen oder wirtschaftlicher Tätigkeiten auf dem Binnenmarkt wesentlich sind. Aufgrund der zunehmenden grenzüberschreitenden wechselseitigen Abhängigkeiten zwischen den Diensten, die über kritische Infrastrukturen in diesen Sektoren erbracht werden, kann eine Störung in einem Mitgliedstaat Auswirkungen auf andere Mitgliedstaaten oder die Union insgesamt haben.

Um die Relevanz dieser Richtlinie zu erkennen, wird auf Art. 1 Abs. 1 verwiesen:

„Diese Richtlinie

a. verpflichtet die Mitgliedsstaaten …

b. legt Verpflichtungen für kritische Einrichtungen fest, die darauf abzielen, ihre Resilienz und ihre Fähigkeit zur Erbringung dieser Dienste im Binnenmarkt zu verbessern

c. regelt die Beaufsichtigung von und die Durchsetzungsmaßnahmen gegenüber kritischen Einrichtungen sowie den die spezifische Aufsicht über kritische Einrichtungen, die für Europa von besonderer Bedeutung sind."

Zwar fällt die Resilienz-Richtlinie subsidiär hinter die NIS Direktive 2.0 zurück, gleichwohl bedeutet dies aber, dass die Resilienz-Richtlinie dann zur Anwendung kommen mag, wenn die NIS Direktive 2.0 nicht greift.

Folgende Sektoren werden von der Resilienzrichtlinie betroffen sein:

01. Energie
02. Verkehr
03. Bankwesen
04. Finanzmarktinfrastrukturen
05. Gesundheit
06. Trinkwasser
07. Abwasser
08. Digitale Infrastruktur
09. Öffentliche Verwaltung
10. Weltraum

Die betroffenen Einrichtungen inkl. Schwellenwerte werden dabei ausschließlich über EU-Richtlinien und Verordnungen definiert. Für den Teilsektor Strom im Sektor Energie sind dies gemäß

- Richtlinie (EU) 2019/944 [14]
  - Art. 2 Nr. 57 (Elektrizitätsunternehmen)
  - Art. 2 Nr. 29 (Verteilernetzbetreiber)
  - Art. 2 Nr. 35 (Übertragungsnetzbetreiber)
  - Art. 2 Nr. 38 (Erzeuger)
- Verordnung (EU) 2019/943 [15]
  - Art. 2 Nr. 8 (nominierte Strommarktbetreiber)
  - Art. 2 Nr. 25 (Elektrizitätsmarktteilnehmer)

Kommen wir nun zum Inhalt der Resilienzrichtlinie:

In Artikel 3 ist festgelegt, dass die Mitgliedstaaten eine Strategie zur Stärkung der Resilienz kritischer Einrichtungen annehmen (müssen). Artikel 4 zufolge müssen die zuständigen Behörden eine Liste wesentlicher Dienste erstellen und regelmäßig eine Bewertung aller relevanten Risiken vornehmen, die sich auf die Erbringung dieser wesentlichen Dienste auswirken können, um kritische Einrichtungen zu ermitteln. Gemäß Artikel 5 ermitteln die Mitgliedstaaten kritische Einrichtungen in bestimmten Sektoren und Teilsektoren. Dabei sollten die Ergebnisse der Risikobewertung berücksichtigt und bestimmte Kriterien ange-

wandt werden. Die Mitgliedstaaten erstellen eine Liste kritischer Einrichtungen, die regelmäßig und bei Bedarf aktualisiert wird. In Artikel 6 wird der Begriff „erhebliche Störung“ im Sinne von Artikel 5 Absatz 2 definiert und es werden die Mitgliedstaaten verpflichtet, der Kommission bestimmte Arten von Informationen über die von ihnen ermittelten kritischen Einrichtungen und die Art und Weise der Ermittlung zur Verfügung zu stellen. Artikel 7 legt fest, dass die Mitgliedstaaten Einrichtungen in den Sektoren Banken, Finanzmarktinfrastruktur und digitale Infrastruktur ermitteln sollten, die ausschließlich für die Zwecke des Kapitels II als kritischen Einrichtungen gleichwertig zu behandeln sind. Nach Artikel 10 bewerten kritische Einrichtungen regelmäßig alle relevanten Risiken auf der Grundlage nationaler Risikobewertungen und anderer relevanter Informationsquellen. In Artikel 11 ist vorgeschrieben, dass kritische Einrichtungen geeignete und verhältnismäßige technische und organisatorische Maßnahmen ergreifen, um ihre Resilienz zu gewährleisten, und sicherstellen, dass diese Maßnahmen in einem Resilienzplan oder gleichwertigen Dokument(en) beschrieben werden. Gemäß Artikel 13 stellen die Mitgliedstaaten sicher, dass kritische Einrichtungen der zuständigen Behörde Sicherheitsvorfälle melden, die ihren Betrieb erheblich stören oder erheblich beeinträchtigen könnten. Die zuständigen Behörden stellen der meldenden kritischen Einrichtung ihrerseits relevante Folgeinformationen zur Verfügung.

Gemäß Artikel 14 handelt es sich bei kritischen Einrichtungen von besonderer europäischer Bedeutung um Einrichtungen, die als kritische Einrichtungen eingestuft wurden und wesentliche Dienste für bzw. in mehr als einem Drittel der Mitgliedstaaten erbringen. Nach Erhalt der Mitteilung gemäß Artikel 5 Absatz 6 teilt die Kommission der betreffenden Drucksache 119/21-14-Einrichtung mit, dass sie als kritische Einrichtung von besonderer europäischer Bedeutung gilt, welche Verpflichtungen sich daraus ergeben und ab wann diese Verpflichtungen gelten. In Artikel 15 werden die besonderen Aufsichtsvereinbarungen für kritische Einrichtungen von besonderer europäischer Bedeutung beschrieben, wozu auch gehört, dass die Aufnahmemitgliedstaaten der Kommission und der Gruppe für die Resilienz kritischer Einrichtungen Informationen über die Risikobewertung gemäß Artikel 10 und die gemäß Artikel 11 ergriffenen Maßnahmen sowie etwaige Aufsichts- oder Durchsetzungsmaßnahmen übermitteln.

Fazit

Die letzten Monate waren dadurch gekennzeichnet, dass sowohl auf europäischer Ebene als auch auf nationaler Ebene in Sachen Cybersecurity diverse weitreichende Änderungen entweder abgeschlossen wurden oder sich im Abschlussprozess befinden. Gerade auf EU-Ebene kann erkannt werden, dass oberste Priorität auf Cybersecurity gelegt wird.

Da höherwertiges EU-Recht niederwertigeres nationales Recht übertrumpft, werden sich die Betreiber kritischer Infrastrukturen zukünftig an gesteigerte Anforderungen gewöhnen müssen.

Getreu eines alten Sprichwortes „Wenn der Wind der Veränderung weht, bauen die einen Mauern und die anderen Windmühlen“ sollten wir uns überlegen, ob wir die neuen – für viele strenger als erwarteten-Cybersecurity-Vorschriften als Chance wahrnehmen, um die Sicherheit der Anlagen zu erhöhen [, was allen zugutekommt] oder im Rahmen einer Fundamentalopposition zu versuchen, die Vorschriften temporär hinauszuzögern. Es wird von niemandem mehr ernsthaft bestritten, dass der Blackout aufgrund einer Cyberattacke auch Europa treffen wird. Die Frage ist nur, wie wir uns dann darauf vorbereitet haben.

Im Jahr 2020 waren auch viele nicht auf eine Pandemie vorbereitet und hatten den Nationalen Pandemieplan aus dem Jahr 2007 vergessen. Es bleibt zu hoffen, dass es bei einem Blackout aufgrund eines Cybersecurity-Angriffes nicht heißen wird: 2020/2021 gab es viele neue und weiterreichende Regularien in Sachen Cybersecurity. Hätten wir die nur mal umgesetzt.

Referenzen

[01] ISO/IEC 24765:2017 Systems and software engineering – Vocabulary

[02] https://www.enargus.de/pub/bscw.cgi/d6217-2/*/*/Kraftwerksbetreiber.html?op=Wiki.getwiki

[03] Gesetz über die Elektrizitäts- und Gasversorgung [EnWG]

[04] Verordnung 2016/631 der Kommission vom 14.4.2016 zur Festlegung eines Netzkodex mit Netzanschlussbestimmungen für Stromerzeuger

[05] VGB PowerTech Journal 03/2020, Der Testplan gemäß § 4 II g) 2017/2196) und vorgelagerte EU-VOs aus IT-/OT-Cybersecurity-Sicht für Energieerzeuger

[06] Telekommunikationsgesetz vom 21. April 2021

[07] Richtlinie 2018/172 über den Europäischen Kodex für die elektronische Kommunikation vom 11. Dezember 2018

[08] Katalog von Sicherheitsanforderungen für das Betreiben von Telekommunikations- und Datenverarbeitungssystemen sowie für die Verarbeitung personenbezogener Daten nach § 109 TKG, Version 2.0 vom 29.04.2020

[09] Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation

[10] https://www.bfdi.bund.de/DE/Infothek/Pressemitteilungen/2021/03_Ratsposition-ePrivacy-VO.html

[11] Europäisches Programm für den Schutz kritischer Infrastrukturen, KOM (2006) 786, Amtsblatt C vom 7. Juni 2007

[12] Richtlinie 2008/114/EG über die Ermittlung und Ausweisung europäischer kritischer Infrastrukturen und die Bewertung der Notwendigkeit, ihren Schutz zu verbessern

[13] COM (2020) 829 final vom 16.12.2020, Vorschlag für eine Richtlinie über die Resilienz kritischer Einrichtungen

[14] Richtlinie (EU) 2019/944 vom 5.6.2019, Gemeinsame Vorschriften für den Elektrizitätsbinnenmarkt

[15] Verordnung (EU) 2019/943 vom 5.6.2019 über den Elektrizitätsbinnenmarkt

[16] Richtlinie (EU) 2016/1148 vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union

[17] (Vorschlag für eine) Richtlinie über Maßnahmen über ein hohes gemeinsames Cybersicherheitsniveau in der Union und zur Aufhebung der Richtlinie (EU) 2016/1148 vom 16.12.2020

[18] Verordnung (EU) 2019/881 über die ENISA und über die Zertifizierung von Cybersicherheit von Informations- und Kommunikationstechnik

[19] Gesetz über das Bundesamt für Sicherheit in der Informationstechnik vom 23. April 2021, Drucksache 19/28844

[20] Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI- Gesetz, zuletzt geändert am 21. Juni 2017

[21] Referentenentwurf zur Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI- Gesetz vom 22. April 2021

[22] IT-Sicherheitskatalog für Betreiber von Strom- und Gasnetzen gemäß § 11 Abs. 1a EnWG vom August 2015

[23] IT-Sicherheitskatalog für Betreiber von Energieanlagen gemäß § 11 Abs. 1b EnWG vom Dezember 2018

[24] TeleTrust – Bundesverband der IT-Sicherheit e.V., Handreichung zum Stand der Technik technischer und organisatorischer Maßnahmen, 2020

[25] Bundesdatenschutzgesetz, zuletzt geändert am 20.11.2019

[26] bdew, Whitepaper Anforderungen an sichere Steuerungs- und Kommunikationssysteme, Version 2.0, Stand: Mai 2018

[27] NIST SP 800-53 Rev. 5 Security and Privacy Controls for Information Systems and Organizations, 10/2020

[28] Bundesamt für Sicherheit in der Informationstechnik, ICS-Security-Kompendium, 25.11.2013

[29] Bundesamt für Sicherheit in der Informationstechnik, IT-Grundschutz-Kompendium, 01.02.2021

[30] DIN EN ISO/IEC 27001:2017 Informationstechnik – Sicherheitsverfahren – Informationssicherheitsmanagementsysteme – Anforderungen

[31] DIN EN ISO/IEC 27002:2017 Informationstechnik – Sicherheitsverfahren – Leitfaden für Informationssicherheitsmaßnahmen

[32] DIN EN ISO/IEC 27019:2020 Informationstechnik – Sicherheitsverfahren – Informationssicherheitsmaßnahmen für die Energieversorgung