Dominik Appelt, Matthias Enzmann, Annika Selzer

# Cybersicherheit im Energiesektor

## Herausforderungen bei der praktischen Umsetzung des geplanten § 5c Energiewirtschaftsgesetzes

Der Energiesektor ist ein attraktives Ziel von Cyberkriminellen und erfolgreiche Angriffe können u. a. den Zugang zu wichtigen Kommunikationskanälen stark einschränken. Vor diesem Hintergrund ist es essenziell, den Energiesektor bestmöglich vor Cyberangriffen zu schützen. Die Vorschriften der NIS-2-Richtlinie sowie ihrer geplanten nationalen Umsetzung unterstützen dieses Ziel regulatorisch. Doch vor welche Herausforderungen stellt NIS-2 und ihre geplante nationale Umsetzung Deutschlands Energieversorger?

### 1 NIS-2-Richtlinie als Ausgangspunkt einer höheren Cybersicherheit[1]

Zur Aufrechterhaltung ihrer Netze betreiben Energieversorger große Netzwerke, die ihnen helfen, ihre Energieinfrastruktur zu kontrollieren und zu verwalten. Dazu gehört heutzutage ein hohes Maß an Informations- und Kommunikationstechnologie, die einerseits Flexibilität und Effizienz fördert, andererseits aber auch die Energieinfrastruktur für Cyberangriffe öffnet.

#### 1.1 Energieversorger als Cyberangriffsziel

Als eines der bevorzugten Ziele von Cyberkriminellen und staatlichen Akteuren war die europäische Strominfrastruktur in den letzten Jahren zunehmend von Cyberangriffen betroffen.[2] Auch wenn großflächige Ausfälle bisher vermieden werden konnten, ist die Tatsache, dass einige dieser Angriffe erfolgreich waren, höchst beunruhigend: Der Energiesektor ist eine der wichtigsten Kritischen Infrastrukturen in jeder modernen Gesellschaft. Unterbrechungen der Strom-, Gas- und Treibstoffversorgung können die Wirtschaft zum Erliegen bringen und enormen Schaden anrichten.[3] Ohne Strom wäre u. a. die Möglichkeit, die weltpolitischen Nachrichten zu verfolgen und mit Verwandten und Freunden zu kommunizieren, stark eingeschränkt. Außerdem würde die Wasserversorgung „versiegen" und Supermärkte müssten vorübergehend schließen, weil Kühltruhen und Kassensysteme ausfallen würden. Schätzungen besagen daher, dass Stromausfälle, die (nur) wenige Tage andauern, zu bürgerkriegsähnlichen Zuständen führen könnten, wenn sie in europäischen Ländern auftreten würden.[4]

1 Die diesem Beitrag zugrundeliegenden Forschungsarbeiten wurden vom Bundesministerium für Bildung und Forschung (BMBF) und vom Hessischen Ministerium für Wissenschaft und Kunst (HMWK) im Rahmen ihrer gemeinsamen Förderung für das Nationale Forschungszentrum für angewandte Cybersicherheit ATHENE unterstützt. Der Beitrag gibt die persönliche Meinung der Autoren wieder.

**Dominik Appelt**

ist Rechtswissenschaftler am Fraunhofer-Institut für Sichere Informationstechnologie (SIT) und am Nationalen Forschungszentrum für angewandte Cybersicherheit ATHENE.

E-Mail: dominik.appelt@sit.fraunhofer.de

**Dr. Matthias Enzmann**

ist Informatiker und Wissenschaftler am Fraunhofer SIT sowie Principal Investigator in ATHENE.
E-Mail: matthias.enzmann@sit.fraunhofer.de

**Dr. Annika Selzer**

ist Abteilungsleiterin am Fraunhofer SIT und Forschungsbereichskoordinatorin in ATHENE.

E-Mail: annika.selzer@sit.fraunhofer.de

2 https://background.tagesspiegel.de/it-und-cybersicherheit/briefing/cyberangriffe-auf-22-energieunternehmen; https://www.handelsblatt.com/politik/deutschland/vertrauliche-analyse-sechs-deutsche-firmen-betroffen-cyberattacken-auf-europaeische-energie-unternehmen-haeufen-sich/28727946.html.

3 Erwgr. 1 der Richtlinie (EU) 2022/2557.

4 https://www.tagesschau.de/wirtschaft/energie/blackout-deutschland-vorbereitung-stromausfall-101.html.

## 1.2 Cybersicherheit -regulatorisch-

Die Verbesserung der Cybersicherheit des Energiesektors ist daher eine der wichtigsten und dringendsten Aufgaben der Cybersicherheitsforschung. Eine zentrale Rolle in der Verbesserung der Cybersicherheit (auch im Energiesektor) nimmt die NIS-2-Richtlinie (kurz: NIS-2) bzw. deren geplante nationale Umsetzung ein. Insbesondere über den durch die geplante nationale Umsetzung der NIS-2-Richlinie ergänzenden § 5c Abs. 1 und 2 Energiewirtschaftsgesetz (EnWG) würden (bestimmte) Betreiber von Energieversorgungsnetzen und/oder Energieanlangen zur umfangreichen Umsetzung technischer und organisatorischer Schutzmaßnahmen verpflichtet. Der geplante § 5c Abs. 3 EnWG enthält dabei Mindestanforderungen an einen entsprechenden IT-Sicherheitskatalog, der wiederum von der Bundesnetzagentur im Benehmen mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) bestimmt wird.

## 1.3 Cybersicherheit -technisch-

Neben der regulatorischen Verankerung der Cybersicherheit können technische Möglichkeiten genutzt werden, die Umsetzung der rechtlichen Vorgaben zu unterstützen und sogar teilautomatisiert zu überprüfen.

Ein Ansatz hierfür ist die Identifizierung von Kennzahlen, die zur Messung des Erfüllungsgrades rechtlicher Anforderungen – wie denen des § 5c Abs. 3 EnWG – genutzt werden können. Rechtliche Anforderungen müssen hierfür jedoch zunächst in konkret umsetzbare und überprüfbare Maßnahmen „übersetzt" werden (sogenannter Top-Down-Ansatz). Parallel werden technische Datenquellen identifiziert und auf deren Aussagekraft hinsichtlich der Umsetzung dieser Maßnahmen untersucht (sogenannter Bottom-Up-Ansatz). Basierend auf beiden Ansätzen werden sodann Metriken – also Kennzahlen zur Überprüfung (rechtlicher) Vorgaben – spezifiziert, die mittels der identifizierten technischen Daten eine teilautomatisierte oder sogar vollständig automatisierte Aussage über den Umsetzungsgrad der erfassten Maßnahmen abgeben können.[5]

Um die Relevanz der NIS-2-Richtlinie und deren geplante nationale Umsetzung – insbesondere in Bezug auf den neuen § 5c EnWG – zu untersuchen sowie Möglichkeiten zur Überprüfung der Umsetzung dieser Anforderungen im Energiesektor zu identifizieren, und ggf. hierfür Anforderungen ableiten zu können, die sich speziell für Akteure im Energiesektor ergeben, wurden Expertenworkshops durchgeführt, deren Ergebnisse nachfolgend dargestellt werden sollen.

## 2 Rolle der Cybersicherheit im Energiesektor

Bevor die Ergebnisse der Expertenworkshops dargestellt werden, fasst die nachfolgende *Tabelle 1* die Rahmenbedingungen der Workshops zusammen.

**Tab. 1 | Übersicht über die Expertenworkshops**

| | |
|---|---|
| **Ziel der Workshops** | Eruieren der Relevanz der NIS-2-Richtlinie, deren geplanten nationalen Umsetzung sowie Möglichkeiten zur Überprüfung der Umsetzung dieser Anforderungen im Energiesektor; Identifizieren von Anforderungen des Energiesektors an mögliche Umsetzungsüberprüfungsansätze |
| **Workshop-Methode** | Expertenworkshops anhand eines Gesprächsleitfadens |
| **Validierung des Gesprächsleitfadens** | Am 20. Dezember 2024 mit drei Personen |
| **Workshop-Anzahl und -Teilnehmende** | Drei Workshops; an jedem Workshop nahmen drei Cybersicherheitsexperten aus dem Energiesektor Deutschlands teil (innerhalb eines Workshops arbeiteten diese für die gleichen Organisation) |
| **Workshop-Datum und -Dauer** | Durchführung der Workshops im Zeitraum vom 22. bis 27. Januar 2025 mit jeweils ca. einer Stunde Dauer |
| **Dokumentation** | Zusammenfassende Transkription, i.d.R. während der Workshops begonnen und unmittelbar nach den Workshops finalisiert |

## 2.1 Cybersicherheit und Cybersicherheitsrecht im Arbeitsalltag

Im Rahmen der drei Expertenworkshops wurde einleitend die Frage gestellt, welche Rolle Cybersicherheit in der täglichen Arbeit der Workshopteilnehmenden spielt. Die Antworten der Workshops zeigen deutlich die zentrale Bedeutung von Cybersicherheit im beruflichen Alltag der Befragten: Im **ersten Workshop** heben die Befragten zunächst die große Rolle der Cybersicherheit für den Energiesektor im Allgemeinen hervor. Die Befragten vertiefen sodann die signifikante Zunahme der Bedrohungen seit Beginn des Ukrainekriegs. Sie beschreiben, dass ihr Unternehmen als Energieversorger seit Beginn des Krieges täglich Angriffen ausgesetzt ist, wobei sie mindestens einen Angriff pro Sekunde verzeichnen. Diese erhöhte Bedrohungslage wird laut der Befragten besonders durch die zunehmende IT-basierte Verwaltung der Energienetze verschärft, die neue Angriffsflächen geschaffen hat. Die Befragten des **zweiten Workshops** beschreiben Cybersicherheit als ihre Hauptaufgabe, die hundert Prozent ihrer Arbeitszeit einnimmt. Zu ihren Kernaufgaben gehören die Entwicklung grundlegender Rahmenbedingungen für Informationssicherheit, die Bewertung von Risiken sowie die Entwicklung und Umsetzung entsprechender Gegenmaßnahmen. Wichtig ist den Befragten dabei auch der kontinuierliche Austausch mit anderen Fachbereichen. Zusätzlich arbeiten sie an der Entwicklung und Weiterentwicklung von Sicherheitssystematiken, der Risikoabschätzung und dem Vergleich von Ist- und Soll-Zuständen im Bereich der Cybersicherheit. Auch im **dritten Workshop** beschreiben die Befragten Cybersicherheit als Kernkompetenz und umfassenden Tätigkeitsfokus. Die Befragten geben an, sich täglich mit verschiedenen Aspekten der Cybersicherheit zu beschäftigen, wobei sie technische, organisatorische und strategische Maßnahmen umsetzen.

Als nächstes wurde die Frage gestellt, welche Rolle rechtliche Vorgaben zur Cybersicherheit in der täglichen Arbeit der Workshopteilnehmenden spielen. Auch hier zeigen die Antworten aus allen drei Workshops übereinstimmend den hohen Einfluss rechtlicher Vorgaben auf den Bereich der Cybersicherheitsumsetzung: Die Befragten des **ersten Workshops** betonen die große

5 Näheres zum Top-Down und Bottom-Up-Ansatz in Diel/Kohn/Schleper/Selzer, Datenschutzmetriken im Beschäftigungsverhältnis, DuD 2021, S. 821 ff.

Rolle verschiedener rechtlicher und regulatorischer Anforderungen, die sie in ihrer täglichen Arbeit berücksichtigen müssen. Im **zweiten Workshop** beschreiben die Befragten die Erfüllung gesetzlicher Anforderungen als nicht verhandelbares Kernziel, wobei sie die Hauptherausforderung in der effizienten Umsetzung sehen. Die Befragten betonen die durchgängige Berücksichtigung rechtlicher Vorgaben und verweisen speziell auf die Relevanz des Artikels 32 DSGVO. Die Befragten des **dritten Workshops** charakterisieren rechtliche Vorgaben als zentrale Leitprinzipien ihrer Arbeit und unterscheiden zwischen internen Richtlinien und externen rechtlichen Anforderungen. Sie betonen die Komplexität durch bereichsspezifische Vorgaben (u. a. Finanzen, Personal, IT) und die Notwendigkeit, alle regulatorischen Maßnahmen in der IT- und OT[6]-Infrastruktur umzusetzen.

Im Anschluss wurden den Workshopteilnehmenden Fragen zu ihrem Kenntnisstand zur NIS-Richtlinie, NIS-2-Richtlinie und deren nationaler Umsetzung (bzw. dem nationalen Umsetzungsentwurf) gestellt. Die Antworten aus allen drei Workshops zeigen, dass beide NIS-Richtlinien und deren nationale Umsetzung (bzw. der Umsetzungsentwurf) von hoher praktischer Relevanz sind und sich die Befragten bereits intensiv mit den bestehenden sowie kommenden Anforderungen auseinandersetzen. Laut der Befragten wird besonders NIS-2 zu verstärkten Vorbereitungs- und Anpassungsaktivitäten führen.

## 2.2 Relevanz und Herausforderungen des § 5c Energiewirtschaftsgesetz

Als nächstes wurden die Workshopteilnehmenden konkret danach gefragt, ob sie mit dem Entwurf des § 5c Abs. 3 EnWG vertraut sind, der die nationale Umsetzung des Artikels 21 Abs. 2 NIS-2 darstellen und Risikomanagementmaßnahmen im Bereich der Cybersicherheit adressieren soll. Allen Teilnehmenden wurde zur Orientierung an dieser Stelle eine verkürzte Darstellung der Vorgaben aus § 5c Abs. 3 EnWG eingeblendet. Auch wenn keiner der Teilnehmenden Workshop-übergreifend unmittelbare Kenntnis von § 5c Abs. 3 EnWG hat, geben alle nach kurzer Durchsicht der eingeblendeten Inhalte an, damit bereits aus NIS-2 vertraut zu sein. Näher äußern die Befragten aus dem **ersten Workshop**, dass sich die Inhalte weitgehend mit den Anforderungen des ISO-Standards 27001 decken und sie sich auf Grund der vorhandenen ISO-27001-Zertifizierung ihres Unternehmens gut gewappnet sehen, wenngleich noch Unsicherheiten hinsichtlich der genauen, praktischen Umsetzung bestehen. Für Letzteres erwarten die Teilnehmenden spezifischere Vorgaben und Orientierungshilfen des BSI. Im **zweiten Workshop** üben die Befragten deutliche Kritik sowohl an NIS-2 als auch am deutschen Gesetzgeber. Konkret nennen die Befragten „Wortneuschöpfungen" wie Cyberhygiene, worunter sich niemand etwas vorstellen könne.[7] Zudem bemängeln die Befragten, dass der deutsche Gesetzgeber den gesetzten Zeitrahmen für die Umsetzung nicht einhält,[8] Dinge verkompliziert und immer noch „etwas draufpacken" würde, wodurch aber kein international einheitlicher Standard erreicht werden kann. Die Befragten bemängelten auch, dass die Formulierungen im EnWG zu generisch sind und es aktuell keine Orientierung oder Unterstützung von den Behörden gibt, sodass man auf eigene Interpretationen hinsichtlich der konkreten Umsetzung angewiesen ist und die Konkretisierung der Behörden erst kommen, wenn Dinge bereits umgesetzt sind. Die Befragten fordern, dass Rechtsakte und dazugehörige Orientierungshilfen zeitgleich veröffentlicht werden, damit „alle von Beginn an in die richtige Richtung laufen" und Anforderungen so formuliert werden, dass man direkt weiß, wie diese umzusetzen sind, sodass Klarheit herrscht zwischen betroffenen Unternehmen und jenen, welche die Einhaltung der Gesetze später kontrollieren. Im **dritten Workshop** werden (neben der Bestätigung der grundsätzlichen Vertrautheit mit NIS-2) keine weiteren Ausführungen gemacht.

Nach der einführenden Frage zum § 5c Abs. 3 EnWG wurden die Workshopteilnehmenden gefragt, wie relevant dieser für ihre tägliche Arbeit ist. In allen Workshops konnte mindestens eine gewisse Relevanz bestätigt werden: Die Befragten des **ersten Workshops** bezeichnen den Absatz als relevant, weil er für sie verpflichtend ist; seine Umsetzung ist jedoch unproblematisch. Im **zweiten Workshop** weisen die Befragten darauf hin, dass der Absatz für ihre eigene Gesellschaft nicht relevant ist, wohl aber für andere Tochtergesellschaften innerhalb des Konzerns. Die Befragten des **dritten Workshops** merken an, dass ein Großteil der in § 5c Abs. 3 EnWG geforderten Maßnahmen bereits umgesetzt ist, sodass der Absatz zwar relevant für sie ist, sie die praktischen Auswirkungen auf die tägliche Arbeit aber als eher gering einschätzen.

Im Anschluss wurden die Workshopteilnehmenden gefragt, ob sie die Anforderungen des vorgeschlagenen § 5c Abs. 3 EnWG bereits ganz oder teilweise in ihrer täglichen Arbeit umsetzen (und ggf. warum und in welchem Umfang). Die Antworten zeigen, dass die grundlegenden Anforderungen des § 5c Abs. 3 EnWG bereits weitgehend abgedeckt sind, insbesondere durch vorhandene ISO-27001-Zertifizierungen: Im **ersten Workshop** geben die Befragten an, die Anforderungen des § 5c Abs. 3 bereits vollständig umzusetzen, soweit sie diese in ihrer „groben Definition" verstehen. Sie betonen dabei ihre proaktive Herangehensweise als Energieversorger, Anforderungen bereits vor Inkrafttreten umzusetzen, wobei die Umsetzung bereits weitgehend im Rahmen der ISO-27001-Zertifizierung erfolgt, die wiederum sowohl vom BSI als auch von Kunden gefordert wird. Im **zweiten Workshop** verweisen die Befragten auf eine Tochtergesellschaft, die für die Umsetzung der Anforderungen zuständig ist. Einzelne Aspekte wie Nr. 11 (Systeme zur Angriffserkennung) und Cyberhygiene werden bereits adressiert, wobei auch hier die ISO 27001 als etablierter Standard dient. Es wurde jedoch angemerkt, dass bei einigen Begriffen wie „Cyberhygiene" noch Klärungsbedarf hinsichtlich der genauen Definition besteht (s. Kritik oben). Im **dritten Workshop** führen die Befragten aus, dass sie im Unternehmen bereits Prozesse und technische Systeme etabliert haben, welche den § 5c Abs. 3 Nr. 1-12 EnWG abdecken können. Auf einzelne Punkte gehen die Befragten näher ein. So gibt es bei der Bewältigung von Sicherheitsvorfällen (Nr. 2) noch ein paar administra-

6 OT (Operational Technology) meint industrielle Steuerungssysteme zur Überwachung oder Einstellung physischer Geräte, die oft nicht vernetzt sind.

7 In der Tat wird der Begriff Cyberhygiene weder in NIS-2 noch im EnWG definiert, jedoch zumindest in den Erwägungsgründen 49 und 89 der NIS-2 beispielhaft erläutert.

8 Laut der Kanzlei Orrick, Herrington & Sutcliffe LLP ist Deutschland eines von 17 EU-Ländern, das bislang nur Entwürfe für nationale Umsetzungen veröffentlicht hat, sieben weitere Länder haben NIS-2 umgesetzt und bei vier Ländern ist der Stand unklar, https://www.orrick.com/en/Insights/2024/10/NIS2-Where-do-European-Countries-Stand-on-Implementing-Cybersecurity-Strategies.

tive Herausforderungen hinsichtlich der Meldepflichten in verschiedenen EU-Ländern, bspw. was die Sprache sowie die Art und Weise der Meldung beträfe. Das Thema Krisenmanagement (Nr. 3) soll ausgebaut werden, da es aktuell eher für OT-Bereiche einschlägig ist. Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen im Bereich der IT-Sicherheit (Nr. 6) sind vorhanden, unklar ist jedoch noch, wie aussagekräftig und effizient sich diese Bewertungen in der Praxis erweisen werden. Hinsichtlich der eingesetzten IT-Maßnahmen für Daten-Backup/-Wiederherstellung (Nr. 3), Schwachstellen-Management (Nr. 5), Verschlüsselung (Nr. 8), Zugriffskontrolle (Nr. 9), Authentifizierung (Nr. 10) und Angriffserkennung (Nr. 11) zeigen sich die Teilnehmenden zuversichtlich, dass die bereits etablierten Prozesse und technischen Systeme auch den neuen regulatorischen Vorgaben entsprechen.

Danach wurden die Workshopteilnehmenden gebeten, darauf einzugehen, ob es in ihrer Organisation einen Prozess zur Überprüfung der Einhaltung rechtlicher Cybersicherheitsanforderungen gibt.[9] Die Antworten der drei Expertenworkshops zeigten deutlich unterschiedliche Reifegrade bei der systematischen Überprüfung von Cybersicherheitsanforderungen: Im **ersten Workshop** legen die Befragten dar, dass sie bereits einen umfassenden Prüfprozess etabliert haben. Eine zentrale Compliance- und Rechtsabteilung führt (je nach Schutzbedarf) wöchentliche bis sogar tägliche Analysen rechtlicher und normativer Anforderungen durch. Die ISO-27001-Zertifizierung wird durch externe Prüfer alle drei Jahre durchgeführt, mit jährlichen Zwischenprüfungen unter Mitwirkung der internen Revision. Zur Unterstützung werden Checklisten und eine Prozessmanagement-Software eingesetzt. Die Prozesse enthalten bereits Aspekte des § 5c Abs. 3 EnWG und sollen diesbezüglich noch erweitert werden, wobei der Nachweis im Rahmen von ISO-Prüfungen und durch Wirtschaftsprüfer erfolgen soll. Im **zweiten Workshop** geben die Befragten an, dass in ihrer Organisation kein dedizierter Prozess zur Überprüfung rechtlicher Cybersicherheitsanforderungen existiert, auch wenn allgemeine Compliance-Prüfungen durch interne Revision und externe Audits jährlich stattfinden. In den Tochtergesellschaften werden Informations-Management-Reifegrad-Systeme betrieben, und einige verfügen über ISO-zertifizierte Informationssicherheitsmanagementsysteme. Eine Einführung spezifischer Prüfprozesse zu § 5c Abs. 3 EnWG ist aktuell nicht geplant, da der Fokus zunächst auf der grundlegenden Umsetzung der neuen Anforderungen liegt. Im **dritten Workshop** geben die Befragten an, dass ihre Organisation über einen gelebten, wenn auch nicht vollständig formal dokumentierten Prüfprozess verfügt. Der Governance-Bereich steuert die Einhaltung rechtlicher Anforderungen mittels definierter Key-Performance-Indikatoren, die kontinuierlich überwacht und quartalsweise umfassend berichtet werden. Die Überprüfung erfolgt durch eine Kombination aus automatisierten Tools und manuellen Kontrollen. Der Prozess deckt bereits wesentliche Aspekte des § 5c Abs. 3 EnWG ab (konkret decken sich viele der Key-Performance-Indikatoren mit den einzelnen Aufzählungen des § 5c Abs. 3 Nr. 1-12 EnWG) und soll entsprechend den neuen regulatorischen Vorgaben weiter angepasst werden.

Sodann wurden die Workshopteilnehmenden gefragt, ob sie in ihrer Organisation im Rahmen der Umsetzung des vorgeschlagenen § 5c Abs. 3 EnWG Herausforderungen sehen, welche das ggf. sind und ob sich diese ggf. auf den gesamten § 5c Abs. 3 oder nur auf einzelne Ziffern des Absatzes beziehen. In den Expertenworkshops zeigte sich diesbezüglich ein differenziertes Bild der Herausforderungen, wobei sich die Hauptprobleme weniger auf die inhaltlichen Anforderungen als vielmehr auf praktische Umsetzungsfragen, Ressourcenknappheit und administrative Hürden beziehen: Im **ersten Workshop** sehen die Befragten Cybersicherheit generell als ständige Herausforderung, bewerten aber die neuen Anforderungen als nicht besonders problematisch, da sie als Standardanforderungen einzustufen sind, die weitgehend aus der ISO 27001 bekannt sind. Als spezifische Schwierigkeit werden die nationale Verwendung eigener, von NIS-2 abweichender Begrifflichkeiten und unbestimmter Rechtsbegriffe benannt (z. B. im Rahmen der Betroffenheitsanalyse eines Unternehmens). Im **zweiten Workshop** stufen die Befragten den Ressourcenmangel und die schwierige Gewinnung qualifizierter Mitarbeiter als zentrale Herausforderung ein. Besonders hervorgehoben werden auch die Komplexität des Lieferkettenmanagements und die spezifischen Herausforderungen im OT-Bereich. Dabei werden insbesondere die langen Lebenszyklen von OT-Systemen und die starke Herstellerabhängigkeit bei Systemanpassungen als problematisch identifiziert. Im Rahmen des **dritten Workshops** sehen die Befragten die größten Herausforderungen im administrativen Bereich, insbesondere bei internationalen Konzernstrukturen. Konkret werden die [derzeit noch] unklare nationale Umsetzung [Deutschland], Fragen der Berichterstattung bei internationalen Konzernen (in welcher Sprache und an welche Behörde soll berichtet werden?) und der erhebliche Verwaltungsaufwand bei der Betreuung zahlreicher Gesellschaften genannt. Die inhaltlichen Anforderungen werden als weniger problematisch eingestuft, da viele Maßnahmen bereits etabliert sind.

## 2.3 Anforderungen an eine automatisierte Verifikation der Umsetzung des § 5c

Am Anfang dieses Beitrags wurde bereits ausgeführt, dass regulatorische Anforderungen schlussendlich in praktische Maßnahmen überführt werden müssen, die nicht zuletzt Auswirkungen auf bestehende technische Systeme und Software haben, und deren Wirksamkeit nachgewiesen bzw. überprüft werden muss. Im Hinblick darauf wurde den Workshopteilnehmenden zum Ende der Workshops die Frage gestellt, ob sie sich – sofern der vorgeschlagene § 5c EnWG in Kraft treten würde – vorstellen könnten, eine fiktive Software zu nutzen, welche die Umsetzung des § 5c Abs. 3 EnWG automatisiert im Wirkbetrieb überwacht und cybersicherheitsrelevante Ereignisse aufzeigt, die die rechtskonforme Erfüllung der Vorschrift ganz oder teilweise gefährden könnte. Alle drei Expertenworkshops stuften die Idee einer automatisierten Umsetzungsverifikation für § 5c Abs. 3 EnWG als sehr nützliche, aber schwer realisierbare „eierlegende Wollmilchsau" ein.

Die Befragten des **ersten Workshops** zeigen grundsätzliches Interesse an einer solchen fiktiven Software, äußern aber Skepsis aufgrund früherer Erfahrungen mit ähnlichen Lösungsverspre-

9 Bei einer positiven Antwort wurden die Befragten gebeten, nähere Ausführungen zum Prüfturnus, der Art der Überprüfungen und dabei verwendeten Hilfsmittel zu machen und darauf einzugehen, ob der Prozess bereits Aspekte des vorgeschlagenen § 5c Abs. 3 EnWG enthält oder dies geplant ist. Bei einer negativen Antwort wurden die Befragten gebeten, ihre Antwort zu begründen und darauf einzugehen, ob dies für die Zukunft geplant ist.

chen. Als Vorteile der fiktiven Software werden die hohe Automatisierung und die Generierung energiesektorspezifischer Kennzahlen genannt. Bedenken bestehen hinsichtlich des Datenexports aus Bestandssystemen und möglicher negativer Seiteneffekte, die hiermit im Zusammenhang stehen können. Als Anforderungen an eine solche fiktive Software nennen die Befragten u. a., dass eine Datenübermittlung an Dritte unterbunden werden muss, eine gute Interpretierbarkeit der Messergebnisse, eine spezifische Ausrichtung auf den Energiesektor, verlässliche Ergebnisse mit wenig Fehlalarmen und wenig verpassten Alarmen sowie eine einfache Integration der Software. Im Rahmen des **zweiten Workshops** führen die Befragten aus, dass zunächst die grundlegenden Anforderungen des § 5c Abs. 3 EnWG umgesetzt werden müssen, bevor eine Überwachung mittels einer solchen fiktiven Software sinnvoll ist. Als wesentlichen Vorteil einer solchen Software nennen sie die potenzielle Arbeitserleichterung für den CISO durch automatisierte Überwachung. Bedenken bestehen insbesondere bezüglich der Datenbeschaffung und des zusätzlichen Ressourceneinsatzes für die Systempflege. Als Anforderungen an eine solche Software nennen die Befragten u. a. die Gewährleistung der Datenschutzkonformität, eine möglichst automatisierte Datensammlung (eventuell KI-gestützt), die Sicherheit der Software selbst sowie ihre Entwicklung innerhalb der EU. Die Befragten des **dritten Workshops** bewerten die fiktive Software als theoretisch sinnvoll, aber in der Praxis besonders für komplexe Konzernstrukturen schwer umsetzbar. Sie betonen, dass eine solche Software bereits dann einen großen Mehrwert hätte, wenn sie nur eine der in Nr. 1-12 des § 5c Abs. 3 EnWG normierten Anforderungen automatisiert überprüfbar machen könnte. Als Vorteile einer solchen Software nennen die Befragten die mögliche Vereinheitlichung von Prozessen, Automatisierung von Berichten und verbesserte interne Abstimmung. Hauptbedenken äußern sie hinsichtlich der Komplexität der Integration in verschiedene IT-Architekturen. Als Anforderungen an eine solche fiktive Software nennen die Befragten u. a. moderate Kosten, universelle Kompatibilität mit bestehenden Systemen und die Fähigkeit zu automatisiertem Reporting für die Leitungsebene.

## 3 Fazit

Die Expertenworkshops zeigen zunächst ein relativ einheitliches Bild bezüglich des Verständnisses von NIS-2 und ihrer geplanten nationalen Umsetzung: Cybersicherheit wird durchgängig als zentrale Herausforderung wahrgenommen, die durch neue regulatorische Anforderungen wie NIS-2 und dem geplanten § 5c EnWG zusätzliche Bedeutung gewinnen wird. Die grundlegenden inhaltlichen Anforderungen des geplanten § 5c EnWG werden von den Organisationen bereits weitgehend erfüllt, hauptsächlich durch bestehende IT-Sicherheitsmaßnahmen und -Prozesse sowie Zertifizierungen. Die eigentlichen Herausforderungen des geplanten § 5c EnWG liegen laut den Befragten jedoch weniger in der technischen Umsetzung als vielmehr in der Knappheit qualifizierten Personals, dem erhöhten administrativen Aufwand, spezifischen Herausforderungen im OT-Bereich, der Integration von Lieferketten und Zulieferern sowie der mit dem nationalen Umsetzungsstand von NIS-2 zusammenhängenden Unsicherheiten. Dementsprechend wird die nationale Umsetzung von NIS-2 weniger als inhaltliche, sondern vielmehr als administrative Herausforderung wahrgenommen. Softwareseitig versprechen sich die Befragten wenig Hilfe in dieser Hinsicht aufgrund der erwarteten Komplexität für die Einführung und Kopplung mit existierenden Systemen. Unterstützung wäre jedoch willkommen, da mit Hilfe von Software, möglicherweise auch nur für Teilaspekte des § 5c Abs. 3 EnWG, bspw. der Umsetzungsgrad des § 5c Abs. 3 EnWG anhand energiesektorspezifischer Kennzahlen verifiziert, Abläufe vereinheitlicht sowie Überwachungsprozesse und das Berichtswesen (teil-)automatisiert werden könnten. Die Befragten jedenfalls würden darin große Vorteile sehen.