Stellungnahme

IT-Sicherheitsgesetz 2.0

Zum aktuellen Referentenentwurf des zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme vom 1. Dezember 2020

Dezember 2020

Zentralverband Elektrotechnik- und Elektronikindustrie

Inhalt

Einleitung

Die Elektroindustrie ist mit ihren innovativen Produkten und Diensten essenziell für die Umsetzung und das weitere Voranschreiten der Digitalisierung und Vernetzung. Sie befindet sich in den ZVEI-Leitmärkten Industrie, Energie, Mobilität, Gesundheit und Gebäude an der Schnittstelle der digitalen Transformation unserer Gesellschaft und Wirtschaft und stellt die hierfür erforderlichen Produkte weltweit zur Verfügung. Dabei nimmt der europäische Binnenmarkt als Exportraum für Komponenten und Produkte eine besondere Stellung ein, sodass sein reibungsloses Funktionieren sichergestellt sein muss. Um dies zu gewährleisten sollte das kommende zweite Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (im Folgenden: IT-Sicherheitsgesetz 2.0 – IT-SiG 2.0) auf den europäischen Binnenmarkt ausgerichtet sein und diesen entsprechend berücksichtigen. Hierzu gehört hinsichtlich des starken Exports von Komponenten und Produkten aus Deutschland in den europäischen Binnenmarkt auch, dass die im Entwurf getroffenen Definitionen einen besseren und verständlicher umsetzbaren Bezug zur Komponentenebene herstellen. Um das gegenseitige Verständnis zu stärken wäre es dabei sinnvoll, auch die Hersteller von Komponenten über Angebote wie UP KRITIS zu beteiligen.

Die ganzheitliche Stärkung der europäischen Cybersicherheit ist der Elektroindustrie sehr wichtig. Hier sollte das IT-SiG 2.0 einen wertvollen Beitrag leisten und an bereits bestehende, erfolgreiche Ansätze anknüpfen und diese, wo nötig, ergänzen. Eine ernst gemeinte Berücksichtigung der europäischen Ebene kann, im Blick auf Produkte, dabei nur unter Berücksichtigung des New Legislative Frameworks (NLF) und hinsichtlich technischer und organisatorischer Anforderungen nur über die europäische Standardisierung und Normierung geschehen. Die Mitgliedsunternehmen des ZVEI stehen dem Vorhaben der Stärkung der Cyberresilienz unterstützend zur Seite und haben bereits in der Vergangenheit den proaktiven Umgang mit dieser Thematik forciert.

Aus genau diesem Wunsch nach zielgerichteten inkrementellen Verbesserungen entspringt nun die Sorge, dass es bei verschiedenen wichtigen Kernaspekten des Gesetzes zu einer Abkehr von bisher erfolgreichen Herangehensweisen und damit einem Verlassen des gemeinsamen Zielpfades kommt.

Zentral sind hier die fehlende europäische Einbindung, die Abkehr vom kooperativen Ansatz, die einseitige Kompetenzballung und die vielfach fehlende Berücksichtigung der stabilen, auch rechtlichen, Rahmenbedingungen, die es zum Betrieb von kritischen Infrastrukturen und zur Herstellung kritischer Komponenten bedarf, zu nennen.

Zusammenfassend sieht die Elektroindustrie folgenden Anpassungsbedarf:

- Stärkere Ausrichtung des IT-SiG 2.0 auf den europäischen Binnenmarkt; d. h. weniger nationale Initiativen und mehr Inhalte für eine NIS 2.0.
- Rückgriff auf das New Legislative Framework, wann immer es um Anforderungen für Produkte und Komponenten geht.
- Wiederbelebung des kooperativen Ansatzes; d. h. keine neue Cyber-Initiativen, dafür stärkere Zusammenarbeit von BSI und Industrie in der Normung (siehe Best Practice mit DIN Spec 27072 und EN 303645).

Für eine Anknüpfung an den europäischen Binnenmarkt und eine internationale Kompatibilität nationaler Gesetzgebung zu Cybersicherheit

Cybersicherheit endet nicht an Ländergrenzen. Die Regulierung von IT-Sicherheit muss daher mindestens europäisch gedacht werden. Hierzu bestehen mit der sog. NIS-Richtlinie für „Betreiber wesentlicher Dienste und Anbieter digitaler Dienste“ bereits Sicherheitsanforderungen und Meldepflichten auf europäischer Ebene. Zum Ende des Jahres 2020 steht ein Review der NIS-Richtlinie an. Hier bietet sich die ideale Gelegenheit, um die nationale und europäische Gesetzgebung weiter zu verzahnen, indem, folgend auf einer umfassenden Evaluierung des ersten IT-Sicherheitsgesetzes, Anforderungen für möglicherweise identifizierte Lücken direkt auf europäischer Ebene gestellt werden könnten. Die Evaluierung wäre prinzipiell notwendig, um einschätzen zu können, ob die getroffenen Maßnahmen ihr Ziel erreicht haben und um eine Übersicht über die Entwicklung, auch hinsichtlich der Bedrohungslage, seit dem ersten IT-Sicherheitsgesetz zu erhalten. Wir begrüßen es daher auch, dass im aktuellen Entwurf unter Artikel 7 eine zumindest teilweise Evaluierung in Zukunft verankert werden soll. Außerdem wäre es aus Sicht der Elektroindustrie sinnvoll, zum einen Informationen zum Rücklauf zu den Meldepflichten und damit zu deren Effektivität zu erhalten. Zum anderen wären häufigere und differenziertere Lagebilder wünschenswert, da diese eine sinnvolle Rückmeldung an Hersteller bieten und somit zur Verbesserung von Produkten beitragen können. Hinzu kommt das Informationsinteresse der Bevölkerung, welches noch weitreichender sein dürfte.

Mit dem aktuellen Entwurf des IT-SiG 2.0 scheint ein solches Vorgehen nicht verfolgt zu werden. Vielmehr sollen neue Elemente, wie neue Sektoren kritischer Infrastrukturen, neue Kategorien („Unternehmen im besonderen öffentlichen Interesse“), neue Formen der Erlaubnis zum Marktzugang und der Marktbeschränkung (§ 9b Untersagung des Einsatzes kritischer Komponenten) und ein neues nationales Siegel (§ 9c Freiwilliges IT-Sicherheitskennzeichen) auf nationaler Ebene und ohne Berücksichtigung der europäischen Anbindung eingeführt werden.

Auch das in § 7a verankerte Recht auf umfangreiche Produktprüfung unter Offenlegung technischer Details ist unter der Annahme, dass zumindest weitere der 27 Mitgliedstaaten der EU sich ein solches Recht mittels nationaler Gesetzgebung vorbethalten könnten, kritisch zu sehen. Es wäre daher sinnvoller im Rahmen einer horizontalen Produktregulierung im NLF auch die entsprechenden Organe der Marktüberwachung zu stärken. Somit würden auch divergierende Anforderungen durch unterschiedliche nationale Gesetze vermieden werden.

Das Ziel einer europäischen Harmonisierung muss besonders für Cybersicherheit gelten. Dabei liegen inzwischen nahezu alle Stränge vor, die man zum Zusammenführen auf europäischer Ebene bräuchte: Neben der bereits erwähnten Überarbeitung der NIS-Richtlinie sind hier Fortschritte in der europäischen Standardisierung und Normierung zur Cybersicherheit zu nennen sowie die Etablierung des Cybersecurity Acts als freiwilligem Zertifizierungsrahmen, der europäisch harmonisierte Zertifizierungen ermöglicht, und die zum Jahresende 2020 begonnene Arbeit an einem horizontalen Rechtsakt zu Cybersicherheit. Es bestünde nun also die einmalige Gelegenheit in einem solchen neuen Entwurf des IT-Sicherheitsgesetzes Anknüpfungspunkte für diese Entwicklungen zu schaffen, statt konkurrierende

nationale Regeln zu setzen. Cybersicherheit ist elementarer Teil des europäischen Digitalen Binnenmarkts. Die Harmonisierung betrifft dabei sowohl Produkt- und Prozessanforderungen als auch das Kredo der Vertrauenswürdigkeit und der Security-Anbieter.

Beispiel 1:

Ein Beispiel für die fehlende europäische Sicht ist das in § 9c beschriebene „Freiwillige IT-Sicherheitskennzeichen“: Zum einen bewertet die Elektroindustrie Vorhaben für die Einführung von Zertifizierungs- und Labelsystemen ohnehin kritisch, da die Aussagekraft eines Kennzeichens angesichts der dynamischen Natur der Cybersicherheit immer schwierig sein wird, auch wenn die mit dem Entwurf vom 01.12.2020 eingeführte Möglichkeit der Festlegung einer Zeitdauer hier eine Verbesserung darstellt. Zum anderen sollte, sofern es zur Einführung eines solchen Kennzeichens kommt, dieses europäisch harmonisiert erfolgen. Die Intention für den Verbraucher Transparenz zu schaffen ist lobenswert, allerdings steht eine nationale Errichtung möglicherweise in Konflikt mit einem sinnvollen europäischen Ansatz. Entscheidend sind dabei die zugrundeliegenden Kriterien – diese müssen mit der Wirtschaft entwickelt werden und sollten dynamisch sein, eine Differenzierung erlauben und möglichst auf etablierten internationalen Standards beruhen. Eine einseitige Fokussierung auf rein nationale Vorgaben, wie den Technischen Richtlinien des BSI, die im Entwurf vom 01.12.2020 deutlich als zentrale Referenz benannt werden, ist vor allem auch für die international agierende deutsche Industrie kontraproduktiv.

Beispiel 2:

Auch die Einführung der neuen Kategorie von Unternehmen im besonderen öffentlichen Interesse auf Ebene des Einzelstaates nach § 2 Abs. 14 des Referentenentwurfs sollte überdacht werden. Vor allem hinsichtlich § 2 Abs. 14 (2) (volkswirtschaftliche Bedeutung anhand erbrachter Wertschöpfung) dürfte an der Effektivität der im weiteren Gesetzestext aufgeführten Maßnahmen gezweifelt werden. Gerade Unternehmen, mit einer besonders herausgestellten wirtschaftlichen Bedeutung und einem besonderen Beitrag zur Wertschöpfung, besitzen bereits ein sehr großes Eigeninteresse ihre Infrastruktur zu sichern und benötigen keine Regulierung um dies zu tun, besonders nicht durch Vorgaben die parallelen Strukturen zu bereits existierenden Maßnahmen aufbauen könnten. Außerdem würde selbst bei einer Ausweitung auf EU-Ebene, bei Unternehmen mit internationaler Supply Chain, für Angreifer immer die Möglichkeit bleiben, gezielt außereuropäische Schlüssel-Zulieferer, welche nicht über diese Regelung erfasst sind, ins Visier zu nehmen.

Beispiel 3:

Durch den im Entwurf vom 01.12.2020 nochmals gestärkten Verbraucherschutzaspekt wird das etablierte Verfahren des Inverkehrbringens im New Legislative Framework (NLF) indirekt berührt. Würde eine Regelung, wie sie im Entwurf des IT-Sicherheitsgesetzes angelegt ist, z. B. durch eine überarbeitete oder zweite Auflage der NIS-Richtlinie auf die europäische Ebene überführt werden, so wären 27 nationale Cybersicherheitsbehörden befugt, vernetzte Verbraucherprodukte zu testen, hierzu zu warnen und Anforderungsrichtlinien zu schreiben. Dies kann weder von der Politik noch der Industrie gewünscht sein. Wir sind davon überzeugt, dass Cybersecurity, wie Privacy in der GDPR oder Safety und Produktsicherheit, europäisch geregelt werden kann, wir sprechen uns daher deutlich für eine horizontale Produktregulierung im NLF aus. Das uneingeschränkte Funktionieren des europäischen Binnenmarktes muss gewährleistet sein.

Empfehlung:

Im Hinblick auf den, während der deutsche Ratspräsidentschaft bewiesenen, Fokus auf Cybersicherheit sollte hier noch ein Umdenken stattfinden: Eine Anknüpfung an den europäischen Binnenmarkt und eine internationale Kompatibilität nationaler Gesetzgebung zu Cybersicherheit sind von hoher Relevanz. Daher sollten die im IT-SiG 2.0 beschriebenen Aspekte in das Review der NIS-Richtlinie eingebracht werden bzw. in entsprechenden Gesetzesvorhaben, wie einer horizontalen Produktrichtlinie im NLF, auf europäischer Ebene geregelt werden.

Für einen kooperativer Ansatz zur verantwortungsgerechten Beteiligung aller Akteure

Cybersecurity ist Teamwork. Alle Beteiligten haben ihr Scherflein beizutragen, jeder in der Wertkette, bis zum Endkunden, trägt Verantwortungen, denen er sich stellen muss. Aus diesem Verständnis schätzt und sucht die Elektroindustrie von je her die Zusammenarbeit mit dem Gesetzgeber, um ihrer Verantwortung, auch gegenüber der Gesellschaft gerecht zu werden. Daher vermissen wir, als Stimme der Elektroindustrie, den mit dem ersten IT-Sicherheitsgesetz verankerten kooperativen Ansatz zwischen Politik und Wirtschaft. Vielmehr scheint an seine Stelle eine vorrangig kleinteilig kontrollierende und strafende Herangehensweise getreten zu sein. Die Rolle des Bundesamtes für Sicherheit in der Informationstechnik (BSI) als Aufsichtsbehörde mit unzähligen Eingriffsmaßnahmen wird sehr betont. Insbesondere im Hinblick auf Regeln bezüglich der Produkthersteller, lässt sich dieser Eindruck kaum vermeiden.

Wir würden einen kooperativen Ansatz – wie er z. B. von den Datenschutzbehörden praktiziert wird – sehr begrüßen. Solch eine Kooperation kann auf verschiedenen Ebenen erfolgen und hilfreich sein:

- Einbindung von Komponentenherstellern in UP-KRITIS: Im Idealfall arbeiten das BSI und die Industrie aber regelmäßig zusammen bzw. sich gegenseitig zu, vor allem in der Normung, um technische und organisatorische Anforderungen auszugestalten, wie es z. B. bei der DIN SPEC 27072 bereits erfolgreich geschehen ist.

- Domänenspezifische, Bedrohungskataloge, wie sie z. B. für ICS-Komponenten existieren, sollten für weitere Bereiche, idealerweise auf europäischer Ebene, ausgebaut bzw. erstellt werden. Derartige Kataloge geben Orientierung für die Security-Kommunikation zwischen Marktakteuren (z. B. Zulieferer und OEM). Zudem bieten sie eine wertvolle Grundlage für die Produkt-/Systementwicklung sowie die Bedrohungs- und Risikoanalyse.

- Zusammenarbeit von europäischen Cybersicherheitsbehörden: Wir befürworten eine Zusammenarbeit der Regulierer der europäischen Staaten auf Augenhöhe. Unabgestimmtes Vorgehen könnte weitere Probleme nach sich ziehen: Es ist nicht ersichtlich, welche Vorstellung zur Überführung des IT-Sicherheitskennzeichen auf die europäische Ebene existiert. Ein Fokus auf die nationale Ebene beinhaltet bei übergreifenden, europäischen Themen wie Cybersicherheit immer die Gefahr widersprechender Regulierung, welche zu einseitigen Wettbewerbsnachteilen führen könnte. Kombiniert mit der Ausweitung auf Produkte ist hier zu befürchten, dass gegen das Prinzip des europäischen „level playing field“ verstoßen wird.

Ein bestrafender Ansatz verkennt auch die intrinsische Motivation von Herstellern und Betreibern: Die Elektroindustrie hat ein ureigenes Interesse daran, dass sie ihre Anlagen und Standorte sicher betreiben kann und das in sie gesetzte Vertrauen aller ihrer Kunden, sowohl B2B als auch B2C, erfüllt, indem sie sichere Produkte, darunter auch Komponenten für den sicheren Betrieb von kritischer Infrastruktur, anbietet.

Cybersicherheitsvorfälle sind existenzbedrohend, sie bedrohen vorrangig die Existenz des betroffenen Unternehmens. Durch die Dynamik in der Cybersicherheit gibt es immer Verbesserungspotential, um die Cyber-Resilienz zu erhöhen. Der maßgebliche Weg in der Breite über kritische Infrastrukturen hinaus muss daher sein, diejenigen Betreiber und Hersteller, die deutlichen Nachholbedarf haben, davon zu überzeugen, dass es vor allem in ihrem eigenen Interesse ist, diesen Rückstand aufzuholen. Das BSI sollte hier daher vielmehr unterstützender und kooperierender Helfer sein, der Unternehmen durch Aufklärung, Warnungen und Hilfestellungen im Ernstfall auch davor bewahrt sich durch ggf. fehlende Informationen selbst zu schaden. Dies sollte mittels Aufklärung und Unterstützung und nicht durch eine zu befürchtende Bestrafung geschehen, diese ist bereits durch die Gefährdungslage gegeben.

Empfehlung:

Wir sprechen uns deutlich dafür aus, dass die Politik, die ausführenden Behörden und die Industrie, als Partner im Sinne der gesamten Gesellschaft kooperieren. Es sollten keine künstliche Widerstände erzeugt werden und auch die Verengung etablierter und innovativer Verfahren, das Risiko von Cybersicherheitsvorfällen zu mitigieren, auf die Sichtweise eines einzelnen Akteurs, sollte vermieden werden.

Es ist außerdem sinnvoll, Angebote zum Austausch und der Beteiligung, wie UP KRITIS auch auf Hersteller von Komponenten und Unternehmen im besonderen öffentlichen Interesse auszuweiten.

Für eine Aufgabenteilung, um gemeinsam mehr Cybersicherheit zu erreichen

Auch die umfangreiche Kompetenzausweitung des BSI wirft Fragen auf. Regulierungen zu Cybersicherheit sollten prinzipiell dem (Schutz-)Ziel dienen, einen höheren Grad an Cybersicherheit bzw. eine größere Resilienz zu entwickeln. Es erscheint zumindest rechtssystematisch problematisch, wenn eine bedeutende Rechtsthematik national nahezu exklusiv über eine Behörde geregelt werden soll, insbesondere dann, wenn die Regelungen Produkte, Wirtschaftsakteure und Betreiber betreffen.

Aber auch ohne diesen Lösungsweg in Frage zu stellen, stimmt die aktuelle Ausweitung der Kompetenzen und Befugnisse des BSI kritisch. Die voranschreitende Kompetenzausweitung des BSI führt zu einem Ungleichgewicht, wie es in unserer auf Gewaltenteilung basierenden Demokratie eigentlich nicht vorgesehen ist. Das BSI würde bei Umsetzung des aktuellen Referentenentwurfs Regelsetzer, anerkennende Stelle, Auditor, Kontrolleur und Bestrafungsinstanz in einer Behörde sein. Das BSI und hinsichtlich kritischer Komponenten auch das BMI würde die Regeln festlegen, überprüfen und mittels Bußgelder entsprechend abstrafen. Bei einer solchen umfangreichen Konzentration von Kompetenzen müssen daher auch praktikable Verfahren und Stellen für Widerspruch und Schlichtung vorhanden sein.

Dabei sprechen wir uns deutlich nicht gegen ein starkes BSI aus. So ist die inhaltliche Ausgestaltung und Verankerung der Rolle des BSI als nationaler Behörde für die Cybersicherheitszertifizierung entsprechend des EU Cybersecurity Acts, (EU) 2019/881, in § 9a, als klärend zu begrüßen.

Vielmehr äußern wir die Befürchtung, dass das BSI mit Aufgaben und Anforderungen überfrachtet werden könnte und es somit seine wichtigen Aufgaben weniger klar verfolgen kann.

Beispiel:

Als symptomatisch für dieses Problem kann „§ 3 Abs. 1 Satz 2, Nr. 20“ des Referentenentwurfs gesehen werden: In diesem Absatz wird gefordert, dass das BSI einen Stand der Technik entwickelt und veröffentlicht, („Entwicklung und Veröffentlichung eines Stands der Technik bei sicherheitstechnischen Anforderungen an IT-Produkte“).

Ein solcher einseitiger Definitionsanspruch verkennt das Wesen des Standes der Technik: Man kann keine technische Regel schreiben und als herausgebender Regelsetzer verbindlich festlegen, dass dies der Stand der Technik sei. Denn ein Stand der Technik entsteht über das Handeln der Beteiligten und ist keine deklaratorische Eigenschaft, sondern ein sich ergebender Zustand. Er ist laufenden Änderungen unterworfen, die der Regelsetzer nicht beeinflussen kann. Demzufolge wird er in Gesetzen normalerweise nur „vermutet“, nicht gesetzt. Der Herausgeber kann sich nur bemühen, mit größtmöglicher Wahrscheinlichkeit den Stand der Technik zu beschreiben. Dieser kann sich während und nach der Beschreibung und Veröffentlichung bereits wieder geändert haben. Ob etwas Stand der Technik ist, kann immer nur aktuell und im Nachhinein im Einzelfall, ggf. durch ein Gericht, festgestellt werden. Dementsprechend sind die oft gemeinsam auftauchenden Begriffe für „allgemein anerkannte Regeln der Technik“, „Stand der Technik“ und „Stand von Wissenschaft und Technik“, die sich im Fortschrittsgrad unterscheiden, im Wesentlichen durch Urteile des Bundesgerichtshofs definiert worden.

Empfehlung:

Statt den Stand der Technik verbindlich festlegen zu wollen, sollte das Bundesamt lediglich Hilfestellungen oder Hinweise bei der Ermittlung des Standes bzw. bei der Ermittlung von Mindestanforderungen an den Stand der Technik bieten. Generell trägt das BSI durch die Veröffentlichung seiner Dokumente zum Stand der Technik bei, es legt ihn jedoch nicht fest! Wir würden es im Sinne einer voranschreitenden Harmonisierung von Anforderungen daher begrüßen, wenn das BSI vermehrt seine Expertise in der internationalen Standardisierung einbringen würde und die technischen Richtlinien nach und nach entfallen würden. Eine kooperative Zusammenarbeit in der internationalen Standardisierung erlaubt ein Zusammenkommen verschiedener kompetenter Akteure und entsprechend demokratische Teilhabe, aktiviert somit Gruppenintelligenz, und stärkt die Umsetzung und Akzeptanz von anspruchsvollen Cybersecurity-Anforderungen. Währenddessen unilaterale (technische) Deutungsansprüche, selbst bei herausragender Kompetenz, in nahezu allen Fällen ein Akzeptanzproblem haben.

Für klare Regeln und eine zielgerichtete Gesetzgebung

Die im Referentenentwurf beschriebene Ausweitung des Geltungsbereiches zusammen mit der vielfach nachgestellten Ausarbeitung in Form von Rechtsverordnungen nach § 10, sorgt für eine größere Betroffenheit der Industrie bei gleichzeitig verstärkter Verunsicherung.
Der aktuelle Referentenentwurf des IT-Sicherheitsgesetzes 2.0 berührt wesentlich stärker als das erste Gesetz die Produkt- und Komponentenebene.

Daraus ergeben sich zwei zentrale Effekte: Zum einen bedarf es besonders in diesem Kontext der bereits angesprochenen Einordnung in den europäischen Rahmen. Denn hinsichtlich Produkten muss immer der europäische Binnenmarkt bedacht werden, in welchen diese in Verkehr gebracht werden. Jegliche Vorgaben, Kennzeichen, Listung, Bewilligungen etc. müssen daher auf ihre Wirkung für den Europäischen Binnenmarkt und Europa allgemein hin untersucht werden. Dieser Aspekt fehlt im aktuellen Entwurf vollständig. Eine Prüfung des Vorhabens sollte daher hinsichtlich Sinnhaftigkeit, Bedeutung, Auswirkung und die Übertragbarkeit auf die europäische Ebene auf jeden Fall erfolgen, um potenzielle wirtschaftliche Schäden vermeiden zu können.
Zum anderen erhöht sich über die Zulieferer der Kreis, der indirekt betroffenen Unternehmen deutlich gegenüber dem ersten IT-Sicherheitsgesetz. Dabei werden nun auch Unternehmen mittelbar betroffen, die bisher wenig Kontakt mit kritischen Infrastrukturen und den geltenden spezifischen Anforderungen hatten und die außerdem häufig auch andere Bereiche, mit z. T. gleichen Produkten, beliefern. Damit dieser Aspekt nicht zu mehr Unsicherheit führt, müssen die Kriterien für Produkte und Anforderungen umso klarer sein.
Dadurch, dass der Geltungsbereich allerdings zweigliedrig erweitert wurde, indem sowohl die direkt betroffenen Unternehmen mit der Hinzunahme weiterer KRITIS-Sektoren und den „Unternehmen im öffentlichen Interesse“ erweitert wurden als auch der Produktfokus, und damit die mittelbare Betroffenheit von Zulieferern, vergrößert wurde, wurde hier beidseitig weitere Unsicherheit injiziert.

Empfehlung:

Wir empfehlen daher, dass zumindest einer dieser beiden Bereiche bereits im Gesetz ausreichend definiert wird. Eine doppelte nachträglich zeitversetzte Definition durch Rechtsverordnungen versetzt die möglicherweise betroffenen Unternehmen in eine nicht zu akzeptierende Rechtsunsicherheit.

Untersagung des Einsatzes kritischer Komponenten

Dieser Aspekt tritt im Spezialfall der „kritischen Komponenten nicht vertrauenswürdiger Hersteller“ noch einmal verstärkt hervor. Hier ergeben sich einige grundsätzliche Probleme:

Wie wird Vertrauenswürdigkeit rechtssicher definiert, wie kann diese überprüft werden?

Die mit dem aktuellen Entwurf vom 01.12.2020 zunächst erfolgte Eingrenzung „kritischer Komponenten“ auf Komponenten, für die mit dem Katalog von Sicherheitsanforderungen nach § 109 Absatz 6 des Telekommunikationsgesetzes, bereits ein Bezugspunkt existiert, ist zwar eine deutliche Verbesserung. Allerdings können über weitere gesetzliche Festlegungen zusätzliche kritische Komponenten in

den Geltungsbereich des Gesetzes genommen werden, sodass die Industrie alle Anforderungen unter dem Gesichtspunkt liest, dass diese auch für beliebige andere Komponenten in kritischen Infrastrukturen Gültigkeit erlangen könnten. Hier sollte die allgemeine Definition hinsichtlich kritischer Komponenten noch weiter spezifiziert werden.

Auch die klare Aussage, dass das Bundesministerium des Innern, für Bau und Heimat aus sicherheitspolitischen Gründen sowohl die Zertifikatserteilung (§ 9) als auch den Einsatz kritischer Komponenten (§ 9b) untersagen kann ist zu begrüßen, da diese klar den tatsächlichen Beweggrund, sicherheitspolitische Abwägungen, und den verantwortlich Entscheidenden benennt.

Die Aberkennung der Vertrauenswürdigkeit bleibt allerdings weiterhin sehr problematisch für die KRITIS Betreiber, da sie eine Komponente nur einsetzen dürfen, wenn der Hersteller ihnen eine Erklärung über seine Vertrauenswürdigkeit abgegeben hat. Verschärft wird diese Problematik dadurch, dass im Entwurf vom 01.12.2020 eindeutig genannt wird, dass der Betrieb untersagt werden kann, wenn ein Hersteller vom Bundesministerium des Innern, für Bau und Heimat als nicht (mehr) vertrauenswürdig eingestuft wird. KRITIS-Betreiber müssten somit nach Aberkennung der Vertrauenswürdigkeit die Komponenten und ggf. die Anlage, in der diese verbaut sind, stilllegen. Dies dürfte schwerlich umzusetzen sein und würde auch wiederum Konsequenzen hinsichtlich der Aufrechterhaltung kritischer Infrastrukturen haben. Zudem würden sich in einem solchen Fall umfangreiche Haftungsimplikationen stellen. Ähnliches gilt auch für zusammengesetzte Produkte, was sind die Konsequenzen, wenn der Hersteller eines Bauteils plötzlich nicht mehr vertrauenswürdig ist, muss es dann zu einem Rückruf kommen? Wer trägt hierfür die Kosten? Hier müssen Lösungen gefunden werden, die auch beim Eintreten dieses Falles, den sicheren Betrieb kritischer Infrastrukturen ermöglichen. Daher müssen hierzu ebenfalls klare Aussagen getroffen werden.

Auch die Frage nach allgemein überprüfbaren transparenten Parametern um Vertrauenswürdigkeit im Vorfeld „testen“ zu können und vertrauenswürdigen Prozesse ist noch zu lösen.

Die Garantieerklärung stellt ein großes Problem dar und dürfte sich als Nachteil für KRITIS-Betreiber und entsprechende Komponentenhersteller erweisen. Die Erklärung soll sich auf die gesamte Lieferkette des Herstellers beziehen. Hier dürften Hersteller zum einen Schwierigkeiten haben, Garantieerklärungen von internationalen Zuliefern zu bekommen bzw. die Verantwortung für diese zu übernehmen. Die „Garantieerklärung“ darf außerdem auch nicht die gesetzliche Gewährleistungsverpflichtung des Herstellers überspannen bzw. keinesfalls eine faktische Garantie im Sinne des BGB bedeuten.

Es stellt sich prinzipiell die Frage, warum solche Verpflichtungen und Garantien nicht, wie bisher übliche Praxis, in bilateralen Verträgen festgehalten werden? Warum wird hier die Regelung von der Vertragsebene auf ein Gesetz verlagert? Als wie schwerer Eingriff in die Vertragsfreiheit ist dies zu sehen?

Auch hinsichtlich der Bedingungen, die dazu führen, dass ein Hersteller als nicht vertrauenswürdig eingestuft wird, überwiegen die Fragen:

Die Verhältnismäßigkeit betreffend, wäre es schwer nachzuvollziehen, wenn nicht die Anzahl der konform eingesetzten Produkte und die bisherige Erfahrung mit einem Hersteller in die Bewertung seiner Vertrauenswürdigkeit einfließen würden. Hat sich

ein Hersteller bisher trotz des Einsatzes vieler unterschiedlicher Komponenten als sehr verlässlich und vertrauenswürdig erwiesen, so sollte es keinen Automatismus geben, dass ein alleiniger Vorfall die Vertrauenswürdigkeit für das gesamte Produktportfolio entzieht. In jedem Fall stellt die drohende Aberkennung der Vertrauenswürdigkeit ein großes Risiko für die Hersteller dar, da zu erwarten ist, dass der KRITIS-Betreiber versuchen wird, entsprechende Kosten auf die Hersteller umlegen. Die Garantieerklärung wird daher letztendlich dazu führen, dass KRITIS-Komponentenhersteller sich bei der Auswahl ihrer Zulieferer stark einschränken werden. Dies widerspricht damit dem europäischen Ansatz, wie er mit der „EU toolbox on 5G Cybersecurity“ verfolgt wird, die auf eine Multi-Vendor-Strategie und die Stärkung von Interoperabilität setzt und einen europäischen Rahmen für die Nutzung der Potentiale der Technologie schaffen soll.

Auch hier wäre ein kooperativer Umgang wünschenswert. Zumal der Industrie aktuell, mit dem Fehlen einer Beschreibung der rechtlichen Verfahren und Widerspruchsmöglichkeiten seitens des Herstellers, der Rahmen zur korrekten Einschätzung fehlt. Außerdem stellen sich auch in diesem Kontext Fragen zur Einhaltung der Gewaltenteilung, für den Fall das BSI bzw. BMI alleinig über die Vertrauenswürdigkeit entscheiden und somit die Regeln setzen, deren Einhaltung überprüfen und am Ende beurteilen würden.

Hinsichtlich der Bedingungen unter § 9b Abs. (5), die Hersteller einer kritischen Komponente nicht vertrauenswürdig machen, gibt es außerdem folgende weitere Probleme, welche die derzeitige Einschätzung erschweren.
Vor allem Punkt 5., der regelt, dass ein Hersteller einer kritischen Komponente nicht vertrauenswürdig ist, wenn „die kritische Komponente über technische Eigenschaften verfügt, die geeignet sind, missbräuchlich auf die Sicherheit, Integrität, Verfügbarkeit oder Funktionsfähigkeit der Kritischen Infrastruktur einwirken zu können“, wirft viele Fragen auf. So könnten hierunter auch Industriekomponenten fallen, die dank ihrer Funktionalität (z. B. Fernwartung, Remote Service, Condition-Monitoring etc.) geeignet sind auch missbräuchlich verwendet zu werden. Aber gerade solche Komponenten und die Dienstleistungen, die diese ermöglichen, stellen den Mehrwert von Industrie 4.0 dar. Sie de facto zu verbannen, würde die weitere Entwicklung in diesem Bereich und somit auch die internationale Führungsrolle der europäischen Komponentenhersteller gefährden.

Auch hinsichtlich des Einsatzes von Komponenten internationaler Hersteller stellen sich Fragen: Welche Vermutungen soll der jeweilige KRITIS-Betreiber anstellen? Sind in der Vergangenheit erfolgte Einflussnahmen von staatlicher Seite ein Ausschlusskriterium? Über welchen zeitlichen Rahmen wird hier gesprochen, wie kann die Einschätzung erfolgen, welche belastbaren Grundlagen können überhaupt herangezogen werden?

Die skizzierte einmalige Zulassung mittels einer Garantieerklärung stellt Betreiber und Hersteller vor neue Probleme bei gleichzeitig fraglichem Nutzen: Ein Katalog „zugelassener Komponenten“ erhöht auch für die Besitzer und Betreiber kritischer Infrastruktur die Kosten und bremst Innovationen. Unter Umständen könnte der erhöhte Aufwand bzw. die befürchtete Unmöglichkeit der Erfüllung der Garantieerklärungsanforderungen dazu führen, dass einige Hersteller von betroffenen Produkten diese speziellen kritischen Komponenten aus dem Sortiment nehmen bzw. den Einsatz in kritischen Infrastrukturen ausschließen. Zumal das einmalige Zulassen von Komponenten wenig echten Schutz bietet, da sich Cybersecurity Bedrohungen in sehr hoher Geschwindigkeit ändern und daher der Lebenszyklus in Fokus stehen sollte.

Empfehlung:

§9b ist in der jetzigen Form aus Sicht der Elektroindustrie und auch im Sinne Deutschlands bzw. einer europäischen Einbettung unbedingt zu vermeiden. In seiner jetzigen Form würde er, vor allem im Blick auf Komponenten über § 109 Absatz 6 TKG hinaus, zu einer deutlich erhöhten Rechtsunsicherheit führen und Investitionen hemmen. Die Im Referentenentwurf skizzierte Regelung ist nicht praktikabel umsetzbar und impliziert den Besitzern und Betreibern von Kritischer Infrastruktur lediglich eine „falsche Sicherheit".

Es ist prinzipiell sinnvoll, dass Komponentenlieferanten die Lieferketten besser kontrollieren. Der Fokus sollte aber darauf liegen, wie Produkte im Einsatz in kritischer Infrastruktur widerstandsfähiger gemacht werden und wie mit dem Restrisiko umzugehen ist.

Zur Erreichung des Ziels des Gesetzes, einen zuverlässigen Schutz und eine erhöhte Widerstandsfähigkeit von kritischer Infrastruktur zu bieten, wäre eine regelmäßige ganzheitliche Bedrohungsanalyse mit entsprechender Maßnahmenumsetzung viel effektiver als eine rein technikbezogene Zertifizierung auf Komponentenebene. So könnte auch berücksichtigt werden, dass beinahe alle „unsicheren" Komponenten mittels zusätzlicher organisatorischer und technischer Maßnahmen (z. B.: Industrial Firewall) in Anlagen nachgerüstet werden können, um die Ziele in Bezug auf Sicherheit, Integrität, Verfügbarkeit und Funktionsfähigkeit zu erreichen.

In jedem Fall muss bereits im Gesetz der grundlegende Rahmen definiert sein, der es zum einem dem Hersteller entsprechender Komponenten erlaubt, seine Produkte anzubieten und seine Vertrauenswürdigkeit zu erhalten und zum anderen dem Betreiber der kritischen Infrastruktur die Möglichkeit gibt, diese Komponenten rechtssicher einzusetzen. Wahrscheinlich wäre auch eine wissenschaftliche Aufarbeitung der zur Vertrauenswürdigkeitsmessung verfügbaren Parameter sinnvoll, idealerweise in Zusammenarbeit mit der Industrie.

Fazit

Im Kern haben Politik, ausführende Behörden, die Industrie und auch die Verbraucher das gleiche Interesse: Sie alle möchten Produkte mit einem hohen Grad der Cybersicherheit, die möglichst sicher eingesetzt und betrieben werden können und somit einen angemessenen Schutz gegenüber den missbräuchlichen Angriffen Cyberkrimineller bieten. Gleichzeitig haben alle ein großes Interesse an einem funktionierenden europäischen Binnenmarkt und einer international konkurrenzfähigen europäischen Wirtschaft. Um diese beiden Kernbedingungen europäischer Prosperität erfüllen zu können bedarf es der gemeinsamen arbeitsteiligen Kooperation aller Beteiligten in ihren jeweiligen Verantwortungsrollen. Denn selbst eine kompetente und umfangreich ausgestattete Behörde wie das BSI wird eine solche Herausforderung nicht allein stemmen können, zumal viele Herausforderungen die Ebene des

Nationalstaats übersteigen. Daher ist eine europäische Arbeitsteilung auch im Sinne des BSI, um sich auf seine Kernaufgaben konzentrieren zu können.

Wir sollten uns in der Umsetzung gemeinsamen europäischen Lösungen und einem europäischen Modell zuwenden, welches auf erfolgreichen von Verantwortung getragenen Rahmenwerken aufbaut, wie es der NLF hinsichtlich von Regelungen für Produkte bietet.

Stellungnahme zum aktuellen Referentenentwurf des zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz 2.0) vom 1. Dezember 2020

Herausgeber:
ZVEI - Zentralverband Elektrotechnik- und Elektronikindustrie e. V.
Innovationspolitik

Lyoner Str. 9
60528 Frankfurt am Main

Verantwortlich:
Marcel Hug
Telefon: +49 69 6302-432
E-Mail: Marcel.Hug@zvei.org

www.zvei.org

Dezember 2020