ZVEI:
Die Elektroindustrie

Whitepaper

Horizontale Produktregulierung für Cybersicherheit

Die Stärken des New Legislative Framework für den Digital Single Market nutzen

November 2018

Zentralverband Elektrotechnik- und Elektronikindustrie

ZVEI:
Die Elektroindustrie

Horizontale Produktregulierung für Cybersicherheit

Herausgeber:
ZVEI - Zentralverband Elektrotechnik- und Elektronikindustrie e. V.
Fachverband Sicherheit
Lyoner Straße 9
60528 Frankfurt am Main

Verantwortlich: Lukas Linke
Telefon: +49 69 6302-432
E-Mail: linke@zvei.org

Redaktion: Arbeitskreis Cybersicherheit.

www.zvei.org
November 2018

Inhalt

1 Es besteht Harmonisierungsbedarf

Die Herausforderung: Die Digitalisierung und vernetzbare Endprodukte prägen immer stärker das Umfeld von Menschen, Unternehmen und Staaten. Einerseits entsteht dadurch tatsächlicher Nutzen. Andererseits steigt die Verantwortung jedes Endprodukts und damit jedes Herstellers, da sich die Endprodukte im Zuge der Vernetzung in größere Systeme integrieren lassen (z. B. Kommunikations- und Energienetz). Spätestens mit dem Internet der Dinge (englisch IoT) wird de facto alles mit allem vernetzt werden können. Folglich können kompromittierte Produkte Einfluss auf das gesamte System nehmen und die Summe vieler kompromittierter vernetzter Produkte kann das Umfeld von Menschen, Unternehmen und nicht zuletzt Staaten prägen. Werden grundlegende Maßnahmen der Cybersicherheit (hier englisch Security) nicht umgesetzt, kann dies zur Beeinträchtigung von Umwelt, Gesundheit und Leben beziehungsweise der öffentlichen Sicherheit führen.

Die Folge: Angesichts dieser Herausforderungen und jüngsten Ereignisse (siehe Mirai, WannaCry, Router-Vorfall etc.) ist verständlich, dass Cybersicherheit aus Gründen des Verbraucherschutzes durch die Politik adressiert wird. So hat die Bundesregierung die Erstellung eines zweiten IT-Sicherheitsgesetzes beschlossen, das Unternehmen und Produkte außerhalb der bisher definierten kritischen Infrastrukturen (KRITIS) erfassen soll. Darüber hinaus sieht der Koalitionsvertrag die Einführung eines Gütesiegels für IT-Sicherheit für vernetzbare Konsumgüter vor. Erste Pilotprojekte für technische Richtlinien des Bundesamts für Sicherheit in der Informationstechnik (BSI) für Breitbandrouter und den Smart-Home-Bereich wurden gestartet. Es wird deutlich, dass Produkte zusätzlich zum bisherigen KRITIS-Betreiber-Ansatz im Fokus der Politik stehen. Auf EU-Ebene steht die Einführung eines europäischen Rahmenwerks für Cybersicherheit-Zertifizierungen kurz bevor (siehe EU Cybersecurity Act). Zusätzlich gibt es ernst zu nehmende Überlegungen, Regeln für Cybersicherheit in bestehende Produktrichtlinien[1] wie der Funkanlagen- oder Maschinenrichtlinie einzubringen (Übersicht siehe Kapitel 4).

Die Antwort der Elektroindustrie: Aus Sicht der Elektroindustrie dürfen die Initiativen auf keinen Fall zu einer nationalen oder inkonsistenten Regulierung der Cybersicherheit führen. Es besteht die klare Notwendigkeit, dass eine Produktregulierung für Cybersicherheit EU-weit einheitlich, kompatibel zu globalen Standards und WTO-konform erfolgt. Dies in enger Abstimmung mit der Industrie umzusetzen, ist Aufgabe der europäischen Politik. Die nachträgliche Einbringung der Cybersicherheit in bestehende Produktregulierungen schwächt die Wettbewerbsfähigkeit europäischer Unternehmen.

Es darf nicht zu uneinheitlichen, inkompatiblen Vorschriften für einzelne Produktsektoren kommen.

Die Elektroindustrie bevorzugt daher eine europäische horizontale Produktregulierung für Cybersicherheit für vernetzbare Endprodukte, wenn dadurch die Einbringung von Security-Vorgaben in bestehende sektorale Produktregulierungen verhindert und eine risikobasierte Basis-Cybersicherheit auf Grundlage des NLF etabliert wird.

Im Gegensatz dazu sollte es Ziel eines gemeinsamen Vorgehens der europäischen Politik und Industrie sein, ein domänen- und industrieübergreifendes Security-Schutzziel für vernetzbare Endprodukte verbindlich zu etablieren.

[1] Den Autoren ist bekannt, dass es inzwischen eine Vielzahl von produktrechtlichen EU-Verordnungen gibt. Insofern ist der rechtlich zutreffende Begriff „produktrechtliche Harmonisierungsvorschriften". Da das Whitepaper sich an eine breite Öffentlichkeit und zum Teil rechtliche Laien wendet, verwendet der Text jedoch weiterhin den Begriff „Produktrichtlinien", um die Leserlichkeit und Verständlichkeit zu stärken.

Mit diesem Vorschlag sind klare Erwartungen der Elektroindustrie verbunden, um die Cybersicherheit in der EU tatsächlich zu stärken und die Industrietauglichkeit zu gewährleisten:

1. Keine nachträgliche Einbringung von Security-Vorgaben in bestehende europäische Produktregulierungen (siehe Kapitel 4)

2. Keine nationalen Produktvorgaben oder Prüfvorschriften für Cybersicherheit außerhalb des behördlichen oder Hochsicherheitsbereichs (z. B. Militär und Behörden); ein einheitliches europäisches Vorgehen ist für den ZVEI maßgeblich

3. Verwendung des etablierten „New Legislative Framework" (NLF) als Grundlage für die Ausgestaltung der Regulierung (siehe Kapitel 2)

4. Ein Level-Playing-Field für Hersteller und Importeure

5. Industrietaugliche Übergangsregelungen und Bestandsschutz

6. Wahrung der Flexibilität und Innovationskraft der Herstellerunternehmen

Gemeinsame Verantwortung: Die Stärkung der Cybersicherheit erfordert die Beteiligung aller Stakeholder: Hersteller, Nutzer und insbesondere im industriellen Umfeld die Betreiber und Integratoren. Eine isolierte Maßnahme ist nicht ausreichend, um einen angemessenen Schutz zu erreichen. Vielmehr müssen mehrere, untereinander abgestimmte und koordinierte Maßnahmen umgesetzt werden. Die Endprodukte müssen eine angemessene Widerstandsfähigkeit haben. Die Nutzer spielen jedoch eine entscheidende Rolle, indem sie die Endprodukte sicherheitsbewusst verwenden sowie im Industrieumfeld geeignet in ihre Lösung integrieren, konfigurieren und während der Lebenszeit der Lösung das eingestellte Schutzniveau aufrechterhalten.

Produktebene als ein Baustein der Cybersicherheit, weitere Schritte sind notwendig: Aus der beschriebenen Herausforderung folgt, dass das Internet der Dinge sicher zu machen und hierfür eine Cybersicherheit der Endprodukte in der Breite erforderlich ist. Die „Dinge" im IoT sind vor allem vernetzbare Endprodukte (Hinweise zur Definition siehe Anhang 1). Eine horizontale Produktregulierung könnte die Cybersicherheit insgesamt anheben und die europäische Kompetenz in diesem Bereich widerspiegeln. Dennoch ist eindeutig, dass weitere Aspekte der Cybersicherheit zu betrachten sind: Services, Plattformen sowie die Betreiber- und Nutzerpflichten. Daneben sind auch wichtige Haftungs- und Gewährleistungsfragen zu klären. Hierfür müssen außerhalb einer Produktregulierung Lösungen gefunden werden. Entsprechend geht das Whitepaper nicht auf diese Aspekte ein.

Das Whitepaper und der Anhang 1 formulieren die Vorstellungen der Elektroindustrie, wie eine Produktregulierung für Cybersicherheit aussehen könnte. Dies dient der Unterstützung der notwendigen Debatte; will aber dem anstehenden politischen Prozess nicht vorgreifen. Die Inhalte stehen offen zur Diskussion. Zudem spiegelt das Papier das Selbstverständnis der ZVEI-Mitgliedsunternehmen wider, dass Cybersicherheit ein selbstverständlicher Bestandteil der Produktqualität und entsprechend kontinuierlich weiterzuentwickeln ist.

2 Das New Legislative Framework als Grundlage

Die Regulierung von Endprodukten wird nur dann ein Erfolg, wenn verschiedene Prinzipien berücksichtigt werden:

Ausrichtung der Regulierung Prinzip der „Better Regulation“	Auswahl der Anforderungen „SMERC-Prinzip“
• Grundlegende gesetzliche Anforderung; Konkretisierung in Normen • Abgestuft und risikobasiert • Wahrung der Flexibilität des Herstellers zur Umsetzung der Vorgaben • Einbeziehung internationaler Standards • WTO-Akzeptanz und international kompatibel • Level-Playing-Field für alle • Technologie- und Lösungsneutral	• Specific – Anforderungen müssen anwendungsspezifisch betrachtet werden. • Measurability – Anforderungen müssen eindeutig bestimmbar bzw. nachprüfbar sein. • Enforceability – Anforderungen müssen durch die Marktüberwachung durchsetzbar sein. • Relevance – Anforderungen müssen relevant für die Security und Anwender sein. • Competition friendly – Es darf keine nennenswerten nachteiligen Auswirkungen auf die Wettbewerbsfähigkeit der Industrie geben.

Der ZVEI ist überzeugt, dass das New Legislative Framework (NLF) bestens dafür geeignet ist, diese Prinzipien regulatorisch abzubilden. Seit der Etablierung in den 1980er-Jahren unter dem Schlagwort „New Approach“ und der Überarbeitung im Jahr 2008 konnten sehr viele Erfahrungswerte sowohl für sektorale (z. B. Maschinenrichtlinie) als auch für horizontale Regulierungen (z. B. Richtlinie zur elektromagnetischen Verträglichkeit) gesammelt werden. Aus Sicht der Elektroindustrie gibt es keine besser geeigneten Modelle, um eine regulatorische Basis für vernetzbare Endprodukte für den EU-Binnenmarkt zu schaffen.

Die Elektroindustrie fordert die Einhaltung der Prinzipien „SMERC“ und „Better Regulation“ bei der Ausgestaltung der Cybersicherheit, um eine innovationsfreundliche und industrietaugliche Umsetzung zu gewährleisten.

Cybersicherheit ist ein querschnittliches Phänomen. Künftig wird es keinen Gesellschaftsbereich oder Industriesektor geben, der nicht auf irgendeine Weise davon betroffen sein wird. Jedoch gelten in den verschiedenen Bereichen zum Teil spezifische Rahmenbedingungen hinsichtlich der Cybersicherheit. Daher stellt sich die Frage, ob Cybersicherheit überhaupt horizontal adressierbar ist oder nicht viel eher jeweils sektorspezifisch geregelt werden sollte.

3 Machbarkeit: horizontaler Ansatz für Cybersicherheit

Aus rechtlicher Perspektive ist dies jedoch keine neue Herausforderung. So regelt zum Beispiel die EMV-Richtlinie die elektromagnetische Verträglichkeit querschnittlich als Phänomenrichtlinie – völlig unabhängig davon, wo das Phänomen EMV stattfindet. Sie kann als sogenannte „Auffang-Richtlinie" Endprodukte in unterschiedlichsten Einsatzorten erfassen und abdecken.

Als weiteres Vorbild kann die ATEX-Richtlinie für den Bereich des Explosionsschutzes dienen. Diese Richtlinie sieht insbesondere vor, dass der Hersteller selbst die bestimmungsgemäße Verwendung und damit die Gefährdungsklassen des Produkts festlegt. Hieraus ergeben sich dann die von der Richtlinie jeweils vorgegebenen Produktanforderungen und das anzuwendende Konformitätsnachweisverfahren. Die Sicherstellung des Explosionsschutzes basiert allerdings nicht nur auf der herstellerorientierten Inverkehrbringens-Regulierung für Produkte, sondern wird ergänzt durch Vorschriften an den Betrieb von ATEX-Produkten (Richtlinie 1999/92/EG), die Anforderungen an den Betreiber stellen, beispielsweise die Einteilung von gefährdeten Bereichen, organisatorische Maßnahmen und Auswahlkriterien für geeignete Geräte. Diese Aspekte sind in gleicher Weise für Cybersicherheit relevant.

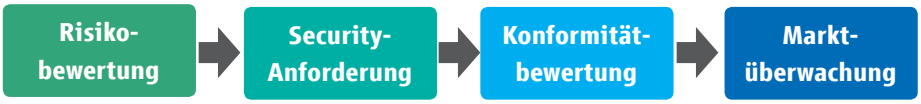
Diese Vorbilder machen deutlich, dass eine Richtlinie oder Verordnung ausreichen kann, um ein horizontales Phänomen zu erfassen, eine allgemeingültige Anforderung aufzustellen und diese auf Ebene der Normen sektorspezifisch zu konkretisieren. Inwiefern ist dieser Ansatz übertragbar? Die Schutzziele der Cybersicherheit (Verfügbarkeit, Integrität und Vertraulichkeit) lassen sich horizontal auf alle Anwendungsbereiche anwenden, wenn auch in unterschiedlicher Gewichtung, abhängig von der jeweiligen Risiko- und Bedrohungsanalyse. Ihre Gewährleistung ist allerorts wichtig für die Sicherung und Stabilität des Internets der Dinge. Künftig müssen vernetzbare Endprodukte so beschaffen sein, dass sie risikobasiert nach dem Stand der Technik (definiert in internationalen Normen) und dem vorgesehenen bestimmungsgemäßen Gebrauch die erwartete Cybersicherheit sicherstellen.[2]

Die Chance des horizontalen Ansatzes besteht auch darin, über ein verbindliches Mandat an die Normung oder anderer geeigneter Plattformen einheitliche Anforderungen an die Cybersicherheit für möglichst viele vernetzbare Endprodukte zu erstellen. Als Konsequenz schafft man die Grundlage dafür, von der geforderten Cybersicherheit abweichende Endprodukte vom EU-Binnenmarkt fernzuhalten. Durch die Etablierung eines übergreifenden, verbindlichen Schutzziels entsteht ein gemeinsames Fundament, auf dem sich wiederum über Normen einheitlichere Umsetzungsmaßnahmen in der Breite bilden und die verschiedenen Sektoren mit höheren Security-Anforderungen spezifisch aufbauen können.

Die Elektroindustrie ist der Ansicht, dass Cybersicherheit horizontal zu adressieren ist, auch wenn Cybersicherheit keine physikalische Messgröße besitzt. Entscheidende Leitprinzipien sind der risikobasierte Ansatz und der Stand der Technik.

Als Best Practice dienen zum Beispiel die EMV- oder ATEX-Richtlinie.

Darüber hinaus bildet der NLF-Ansatz regulatorisch einen wesentlichen Teil der gesamten Security-Kette für den gesamten EU-Binnenmarkt ab. Man greift jedoch zu kurz, wenn nur technische Anforderungen bei Endprodukten diskutiert werden. Allein die stringente Herleitung der Security-Anforderung, ihre Prüfung und nicht zuletzt Sanktionierung führt zu einer tatsächlichen Stärkung der Cybersicherheit.



[2] Den Autoren ist bewusst, dass es im Rahmen des Produktsicherheitsgesetzes die Tendenz gibt, den vorhersehbaren Fehlgebrauch ebenfalls bei den wesentlichen Anforderungen zu berücksichtigen. Dies ist wiederum bei der EMV, die hier als maßgebliches Vorbild dienen soll, nicht der Fall. Daher ist in einem späteren Schritt zu diskutieren, ob und inwiefern eine entsprechende Bezugnahme auf den vorhersehbaren Gebrauch zielführend ist.

4 Eine horizontale Cybersicherheitsregulierung ergänzt aktuelle europäische Regulierung und Initiativen

NIS-Richtlinie

Der NLF-Produktansatz führt die Logik der bisherigen Regulierung für Cybersicherheit konsequent fort. Bisher wurden die Betreiber von kritischen Infrastrukturen und Diensten über die NIS-Richtlinie adressiert. Sichere Infrastrukturen und Dienste benötigen wiederum sichere Produkte (hier im Sinne der Security), auf denen sie aufbauen können. Gleiches gilt für den Verbraucherschutz und die Datenschutzgrundverordnung, für die eine Basis-Cybersicherheit in vernetzbaren Endprodukten ebenfalls eine Voraussetzung ist. Insofern müssen bei der Stärkung der Cybersicherheit Infrastrukturen, Netze, Unternehmen und Endprodukte zusammen betrachtet werden. Der NLF-Ansatz ergänzt in diesem Sinne die NIS-Richtlinie.

Cybersecurity Act

Des Weiteren kann der horizontale Ansatz für Cybersicherheit den neuen EU-Cybersecurity Act unterstützen. Der Act stellt einen wertvollen ersten Schritt für die Harmonisierung von bestehenden nationalen Zertifizierungsschemata dar. Auf freiwilliger Basis können Unternehmen für die B2C- und B2B-Märkte (d. h. außerhalb der kritischen Infrastrukturen) über eine europäisch-einheitliche Konformitätsbewertung ein gesondertes Security-Versprechen gegenüber ihren Kunden abgeben. Zudem adressiert der Cybersecurity Act auch Prozesse und Dienste; zwei Bereiche, die dem Produkt-Fokus unbedingt hinzuzufügen sind. Der horizontale NLF-Ansatz geht den nächsten Schritt weiter und legt das Fundament für eine verbindlich-einheitliche Cybersicherheit für Endprodukte auf dem europäischen Binnenmarkt. Beide Ansätze zusammen können zu einem Markenkern Europas werden. Sie setzen internationale Maßstäbe und drücken das Selbstverständnis aus, im besonderen Maße Vertrauen durch Cybersicherheit zu schaffen. Das gelingt jedoch nur, wenn eine horizontale Produktregulierung keine Verpflichtung zu einer doppelten oder mehrfachen Prüfung und Konformitätsbewertung (ggf. Zertifizierung) gleicher Sachverhalte und Anforderungen enthält.

Common Criteria

Bei den Common Criteria (CC) mit dem Abkommen zur gegenseitigen Anerkennung von Prüfungen (siehe SOG-IS MRA) stehen Sicherheitsprodukte (im Sinne der Security) und der Hochsicherheitsbereich im Fokus. Entsprechend existieren sehr spezifische Anforderungen an die Produkte und Prüfungen. Sie lassen sich relativ schwer für den normalen B2B- und B2C-Massenmarkt skalieren. Vor diesem Hintergrund kann der NLF-Ansatz, ohne Auswirkungen auf die CC-Welt bzw. parallel dazu, ohne Probleme umgesetzt werden.

Bestehende EU-Produktregulierungen

Wie im ersten Kapitel kurz skizziert, bestehen für einige existierende Produktrichtlinien Überlegungen, Cybersicherheit nachträglich zu integrieren. Folgende Regulierungen stehen im Fokus: Funkanlagenrichtlinie (RED), Maschinenrichtlinie (MD), Niederspannungsrichtlinie (LVD), Medizinproduktenverordnung (MDR).

Vier Gründe sprechen aus Sicht der Elektroindustrie gegen eine Integration der Cybersicherheit in bestehende Produktrichtlinien.

1. Es wird kaum möglich sein, die verschiedenen Anforderungen kompatibel zueinanderzuhalten. Allein der jeweils stattfindende legislative Prozess im Parlament und Rat macht aufgrund unterschiedlicher Perspektiven und Ansprechpartner ein konsistentes Regelungssystem unwahrscheinlich.

2. Der Versuch, eine konsistente Regelung zu erreichen, nimmt sehr viel Zeit in Anspruch. Daher betrachtet der ZVEI das Argument, dass Erweiterungen bestehender Richtlinien schneller umzusetzen sind, mit großer Skepsis.

3. Es wird keine übergreifende verbindliche Vorgabe für Cybersicherheit geschaffen. Selbst wenn Security-Anforderungen in alle vier Regulierungen integriert würden, blieben mehr Bereiche offen, als wenn vernetzbare Endprodukte horizontal erfasst würden.

4. Ein weiterer Aspekt ist zu bedenken: Die Aufspaltung der Security-Anforderung auf verschiedene Regelwerke verhindert eine prägnante Wahrnehmung und Bewusstseinssteigerung des Themas in der Öffentlichkeit. Auch wenn es sich dabei um einen „soft factor" handelt, kann im Gegensatz dazu eine grundlegende horizontale Regulierung die Aufmerksamkeit für Cybersicherheit und nicht zuletzt die Wahrnehmung der europäischen Kompetenz in diesem Bereich im In- und Ausland stärken.

Der horizontale NLF-Ansatz ist auch mit den Sektoren kompatibel, für die bereits produktspezifische Security-Vorgaben bestehen. In diesen Fällen sollte folgende Bewertung vorgenommen werden:

1. Enthält die bestehende Produktregulierung Vorgaben für die Cybersicherheit? Wenn ja, gelten im Sinne der Lex-Specialis-Regelung die konkreteren Vorgaben. Entsprechend können sektorspezifische Regelungen außerhalb des NLF-Ansatzes (mit der CE-Kennzeichnung), wie zum Beispiel bei der Einzel- oder Typzulassungen im Automobil- und Eisenbahnbereich, erhalten bleiben, wenn sie das gleiche oder ein höheres Security-Schutzziel erreichen.

2. Bestehen keine Security-Vorgaben, dann sollten zumindest die horizontalen Anforderungen, initiiert durch den hier beschriebenen NLF-Ansatz, gelten. Im Rahmen der Lex-Specialis-Regelung können bei konkretem Bedarf höhere oder zusätzliche Security-Anforderungen gegebenenfalls auch nachträglich in den Sektoren festgelegt werden.

Hinweis: Im Sinne der gemeinsamen Verantwortung aller Akteure für Cybersicherheit muss jedes holistische Security-Konzept gemäß dem Produktlebenszyklus Vorgaben für Entwicklung, Fertigung, Installation, Integration, Betrieb/Nutzung und Abkündigung vorsehen. Die Betreiber- und Nutzungspflichten sollten sinnvollerweise aber nicht in einer Produktregelung festgeschrieben werden, sondern sind an anderer Stelle festzulegen (siehe z. B. Verhältnis zwischen Maschinenrichtlinie (= Produkt-/Systemvorgaben) und Arbeitsstättenverordnung (= Betreiberpflichten)).

Anhang 1: Mögliche Inhalte einer NLF-Regulierung

(Orientierung an Beschluss 768/2008/EU)

Der nachfolgende Anhang soll als Unterstützung skizzieren, wie eine NLF-artige Produktregulierung für Cybersicherheit aussehen könnte. Der Aufbau entstammt dem Rahmenwerk des Beschlusses 768/2008 und der EMV-Richtlinie. Die Inhalte des Anhangs sollen eine konkrete Grundlage für die weitere Sondierung bieten. Sie dienen der Unterstützung der notwendigen Debatte; können und wollen aber dem anstehenden politischen Prozess nicht vorgreifen. Die ZVEI-Mitgliedsunternehmen stellen die hier aufgeführten Punkte bewusst offen zur Diskussion.

Mögliche Inhalte einer EU-Verordnung – am Vorbild EMV-Richtlinie

A.1 Gegenstand

Gegenstand der Verordnung ist die Cybersicherheit von vernetzbaren Endprodukten. Sie fordert ein risikobasiertes und ein gemäß dem Stand der Technik angemessenes Niveau für Cybersicherheit.

A.2 Geltungsbereich

Diese Verordnung gilt für vernetzbare Endprodukte gemäß der Begriffsbestimmung im Abschnitt „Begriffsbestimmung".

Diese Verordnung gilt im Sinne des Lex-Specialis-Prinzips nicht für Endprodukte, die im Hinblick auf die Cybersicherheit in anderen Richtlinien oder Verordnungen spezifisch geregelt sind. Das bedeutet, dass spezifischere Vorgaben Vorrang haben. Wenn jedoch ein Delta zwischen den spezifischeren Vorgaben und der horizontalen NLF-Regulierung besteht, muss dieses Delta durch Anwendung der NLF-Regulierung geschlossen werden.

A.3 Wesentliche Anforderungen für Cybersicherheit

Vernetzbare Endprodukte müssen risikobasiert nach dem Stand der Technik so entworfen und gefertigt sein, dass sie zum Zeitpunkt des Inverkehrbringens bei bestimmungsgemäßer oder vernünftigerweise vorhersehbarer Verwendung

a. andere vernetzbare Endprodukte im Hinblick auf deren Cybersicherheit nicht wesentlich gefährden oder beeinträchtigen;
b. hinreichend gegen zu erwartende Cybersicherheitsbedrohungen standhalten, ohne dass ihre Verwendung wesentlich eingeschränkt ist.

Hinweis: Die Möglichkeit, einen höheren Grad der Cybersicherheit zu erreichen, oder die Verfügbarkeit anderer Endprodukte, die ein geringeres Risiko darstellen, ist kein ausreichender Grund, ein Endprodukt als unsicher (im Sinne der Security) anzusehen.

Hinweis: Alle konkreten technischen und prozessualen Anforderungen werden über Normen und Standards spezifiziert. Ziel ist es, eine horizontale Security-Norm zu schaffen, die durch sektorale Security-Normen ergänzt oder ersetzt werden kann (siehe Lex-Specialis-Ansatz). Es ist ein wichtiges Prinzip des NLF, dass in der Regulierung keine technischen Vorgaben festgeschrieben werden. Es wird lediglich das Schutzziel verbindlich vorgeschrieben.

A.4 Begriffsbestimmung

A.4.1 Spezifisch:

Vernetzbare Endprodukte:
a. Produkte, die dafür vorgesehen sind, direkt oder indirekt über das Internet zu kommunizieren sowie
b. Produkte, bei denen unabhängig vom bestimmungsgemäßen Gebrauch eine direkte oder indirekte Kommunikation über das Internet vernünftigerweise vorherzusehen ist.

Vernetzbare Endprodukte umfassen auch die zugehörige eingebettete Firmware und Software, die für die Hauptfunktion des Endprodukts essenziell ist,
c. entsprechend auf einem Endprodukt nach 1a oder 1b vorinstalliert ist oder
d. die nachträglich für ein Endprodukt nach 1a und 1b, zum Beispiel als Funktionserweiterung oder Update, vom Hardware-Hersteller oder einem Software-Hersteller kommerziell und eigenständig in Verkehr gebracht wird und dafür bestimmt ist, auf dem Endgerät installiert zu werden.

Hinweis: In einem späteren Schritt müssen wie bei nahezu jeder Regulierung notwendige Ausnahmeregelungen diskutiert werden. Dies soll jedoch nicht in diesem Whitepaper geschehen.

Hinweis: Der Begriff „Endprodukt" umfasst auch den Bereich der „Lösungen", das heißt, die Verschachtelung von Endprodukten zu einer komplexen Lösung.

Hinweis: In den nachfolgenden Abschnitten wird der Begriff „Produkt" stets im Sinne eines „Endprodukts" verwendet.

Cybersicherheit im Sinne dieser Verordnung:
Cybersicherheit umfasst alle Maßnahmen und Fähigkeiten eines Produkts (Hardware und Software) zur Gewährleistung der für den bestimmungsgemäßen Gebrauch erforderlichen Vertraulichkeit, Verfügbarkeit und Integrität.

A.4.2. Aus der 765/2008 übernommen:

Bereitstellung auf dem Markt: jede Abgabe eines Endprodukts zum Vertrieb, Verbrauch oder zur Verwendung auf dem Gemeinschaftsmarkt im Rahmen einer Geschäftstätigkeit;

Inverkehrbringen: die erstmalige Bereitstellung eines Produkts auf dem Gemeinschaftsmarkt;

Hersteller: jede natürliche oder juristische Person, die ein Produkt herstellt bzw. entwickeln oder herstellen lässt und dieses Produkt unter ihrem eigenen Namen oder ihrer eigenen Marke vermarktet;

Händler: jede natürliche oder juristische Person in der Lieferkette, die ein Produkt auf dem Markt bereitstellt, mit Ausnahme des Herstellers oder des Einführers;

Harmonisierte Norm: eine harmonisierte Norm gemäß der Definition in Artikel 2 Absatz 1 Buchstabe c der Verordnung (EU) 1025/2012;

Akkreditierung: hat die Bedeutung gemäß der Verordnung (EG) 765/2008;

Nationale Akkreditierungsbehörde: hat die Bedeutung gemäß der Verordnung (EG) 765/2008;

Konformitätsbewertung: das Verfahren zur Bewertung, ob spezifische Anforderungen an ein Produkt, ein Verfahren, eine Dienstleistung, ein System, eine Person oder eine Stelle erfüllt worden sind;

Endnutzer: jede natürliche oder juristische Person mit Wohnsitz oder Niederlassung in der Union, dem ein Produkt entweder als Verbraucher, außerhalb von Handel, Gewerbe, Handwerk oder Beruf oder als gewerblicher Endverbraucher im Rahmen seiner gewerblichen Tätigkeit zur Verfügung gestellt wurde.

Hinweis: Die Verordnung (EG) 765/2008 sieht noch weitere Marktteilnehmer vor, wie zum Beispiel den Einführer, Bevollmächtigten und Händler. Um den Umfang und die Komplexität des Anhangs zu beschränken, wurden diese Rollen in diesem ersten Schritt nicht mitaufgenommen. In einer vollständigen Betrachtung sind sie selbstverständlich mitaufzuführen, um auch den Realitäten im e-Commerce gerecht zu werden.

A.5 Pflichten der Marktakteure

A.5.1 Hersteller

1. Die Hersteller gewährleisten, wenn sie ihre Produkte in Verkehr bringen, dass diese gemäß den wesentlichen Anforderungen (siehe A.3.) entworfen, hergestellt und bewertet wurden.

2. Die Hersteller erstellen die erforderlichen technischen Unterlagen und führen das anzuwendende Konformitätsbewertungsverfahren durch oder lassen es durchführen.

3. Wurde mit diesem Verfahren nachgewiesen, dass das Produkt den geltenden Anforderungen entspricht, stellen die Hersteller eine EU-Konformitätserklärung aus und bringen die Konformitätskennzeichnung an.

4. Die Pflichten hinsichtlich der Konformitätsbewertungsverfahren, -erklärung und -kennzeichnung entfallen, wenn bei der Herstellung des Produkts
   - Produkte verbaut werden, die die Cybersicherheitsanforderungen dieser Verordnung vollständig erfüllen;
   - diese Produkte bestimmungsgemäß eingebaut werden und
   - dadurch die Cybersicherheit des Gesamtprodukts sichergestellt ist.

   Dies erfordert eine Bewertung des zusammenfügenden Herstellers, ob durch das Zusammenfügen nicht vielleicht doch weitere Maßnahmen nötig sind.

5. Die Hersteller bewahren die technischen Unterlagen und die EU-Konformitätserklärung [üblicherweise zehn Jahre] ab dem Inverkehrbringen des Produkts auf.

6. Die Hersteller gewährleisten durch geeignete Verfahren, dass Konformität bei Serienfertigung sichergestellt ist und dass Änderungen am Entwurf des Produkts oder an seinen Merkmalen sowie Änderungen der harmonisierten Normen oder der technischen Spezifikationen, auf die bei Erklärung der Konformität eines Produkts verwiesen wird, angemessen berücksichtigt werden.

7. Die Hersteller führen erforderlichenfalls ein Verzeichnis der Beschwerden, der nichtkonformen Produkte und der Produktrückrufe und halten die Händler über diese Überwachung auf dem Laufenden.

8. Die Hersteller gewährleisten, dass ihre Produkte eine Typen-, Chargen- oder Seriennummer oder ein anderes Kennzeichen zu ihrer Identifikation tragen, oder, falls dies aufgrund der Größe oder Art des Produkts nicht möglich ist, dass die erforderlichen Informationen auf der Verpackung oder in den dem Produkt beigefügten Unterlagen gegeben werden. Dies gilt auch für Software, die nach A.4.1 ein vernetzbares Endprodukt ist.

9. Die Hersteller geben ihre Kontaktadresse, ihren eingetragenen Handelsnamen oder ihre eingetragene Handelsmarke entweder auf dem Produkt selbst oder, wenn dies nicht möglich ist, auf der Verpackung oder in den dem Produkt beigefügten Unterlagen an. Bei Software, die nach A.4.1 ein vernetzbares Endprodukt ist, kann dies auch innerhalb der Software erfolgen.

10. Die Hersteller gewährleisten, dass dem Produkt die Gebrauchsanleitung und die Informationen zur Cybersicherheit bzw. zum sicheren Gebrauch sowie zur Produktklasse (siehe A.6) beigefügt werden und gegebenenfalls gemäß der Entscheidung des betreffenden Mitgliedstaats in einer Sprache zur Verfügung gestellt werden, die von den Verbrauchern und sonstigen Endnutzern leicht verstanden werden kann.

11. Die Hersteller veröffentlichen eindeutig und transparent den jeweiligen Zeitraum oder Zeitpunkt, innerhalb dessen oder bis zu dem sie Unterstützungs- und Korrekturmaßnahmen für ihr Produkt zur Verfügung stellen. Bis zu diesem Datum ergreifen Hersteller, die der Auffassung sind oder Grund zu der Annahme haben, dass ein von ihnen in Verkehr gebrachtes Produkt angesichts des aktuellen Stands der Technik nicht mehr hinreichend die Cybersicherheit sicherstellt, unverzüglich die erforderlichen Korrekturmaßnahmen. Mögliche Korrekturmaßnahmen sind zum Beispiel Updates, Kompensationsmaßnahmen oder Informationen und Hinweise für Betreiber und Endnutzer.

    Hinweis: Die Korrektur- oder Kompensationsmaßnahmen können auch Vorgaben für eine Veränderung oder Beschränkung der Verwendungsweise des Produkts umfassen. Diese Anpassungen müssen dem Endkunden gegenüber mitgeteilt und technisch ermöglicht werden.

12. Außerdem unterrichten die Hersteller unverzüglich die zentral zuständige europäische Behörde, wenn mit dem Produkt Gefahren (im Sinne der Cybersicherheit) für die Allgemeinheit sowie für das Leben und Gesundheit von Menschen verbunden sind.

    Hinweis: Derzeit existiert keine zentrale Behörde für diesen Vorgang. In einem späteren Schritt sollte geklärt werden, durch welches Verfahren sichergestellt wird, dass Unternehmen europaweit nur an eine Stelle melden müssen.

13. Die Hersteller händigen der zuständigen nationalen Behörde auf deren begründetes Verlangen hin alle Informationen und Unterlagen für den Nachweis der Konformität des Produkts in einer Sprache aus, die von dieser zuständigen nationalen Behörde leicht verstanden werden kann. Sie kooperieren mit dieser Behörde auf deren Verlangen bei allen Maßnahmen zur Abwendung von Gefahren für die Cybersicherheit, die mit Produkten verbunden sind, die sie in Verkehr gebracht haben.

A.5.2 Integratoren

Die rechtliche Rolle der Integratoren hängt im Einzelfall vom Einfluss ihrer Integrationsarbeit auf die Cybersicherheit des von ihnen zusammengebauten Endprodukts ab:

- Wenn Integratoren lediglich gemäß dieser Rechtsvorschrift vollständig bewertete Produkte verwenden, reduzieren sich die Pflichten und Verfahren (siehe Nummer 4 in A.5.1). Dies kann dazu führen, dass dem Integrator im NLF lediglich die Rolle eines Händlers zukommt.
- Wenn die Integrationsarbeit aber Einfluss auf die Cybersicherheit des Endprodukts hat, kommt dem Integrator jedoch die Rolle eines Herstellers zu. Er hat die Cybersicherheit des von ihm zusammengebauten Endprodukts insgesamt zu bewerten und zu erklären. Bei bestimmungsgemäßer Verwendung bereits bewerteter Komponenten kann der Integrator aber auch in diesem Fall die Konformitätsbewertungsergebnisse dieser Komponenten übernehmen (siehe Punkt 3 des Modul A in A.7.1).

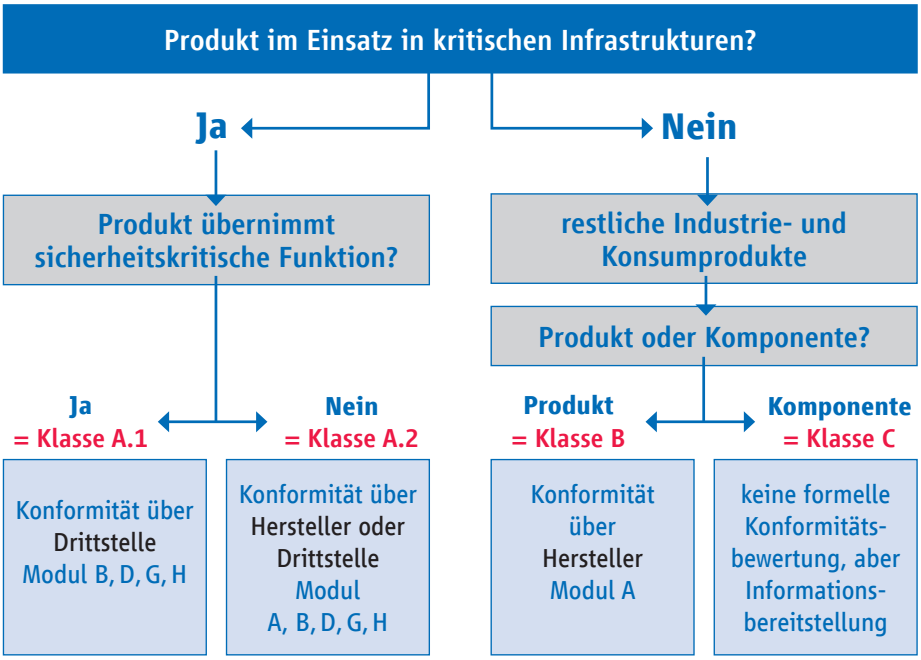
Hinweis: Im Bereich der Konsumgüter und Privatpersonen kann die hier genannte Rolle mit ihren Pflichten anders (rechtlich) belegt sein und/oder verstanden werden. Die sich daraus ergebenden Unterschiede zu den hier genannten Pflichten sind in einem nachfolgenden Schritt zu evaluieren und kenntlich zu machen.

Hinweis: Wie im Hauptteil des Whitepapers bereits erwähnt, sind im Sinne der gemeinsamen Verantwortungen die Betreiberpflichten ein wesentlicher Bestandteil der Security-Kette. Betreiberpflichten werden nicht in einer Produktregulierung geregelt. Diese werden zum Beispiel in der Arbeitsstättenverordnung etc. behandelt. Klar ist, dass die Betreiberpflichten gegebenenfalls in anderen Regulierungen zu ergänzen sind. Hierzu gehören beispielsweise die Installation von Updates auf sowie das stetige Patchen von Produkten im Rahmen der betreiberspezifischen Risikobewertung und -reduzierung.

A.6 Stufung und Produktklassen

Hinweis: Die Anforderungen für die Security-Funktionen und den Security-Prozess werden in Normen und nicht durch das Konformitätsbewertungsmodul festgelegt. Alle unterschiedlichen Module A bis H können sich theoretisch auf die gleiche Norm beziehen. Das heißt, auch das Modul A kann sehr anspruchsvolle Anforderungen stellen.

Übersicht:



Hinweis: Den Autoren ist bewusst, dass es mehrere Ansätze und Gewohnheiten gibt, einen Entscheidungsbaum aufzubauen. Der hier gewählte Ansatz soll zunächst eine möglichst leichte und schnelle Einordnung ermöglichen. Die vorgestellte Modul-Auswahl leitet sich aus dem eingeschätzten Risikoumfeld ab, muss selbstverständlich aber im weiteren Verlauf vertieft werden.

Erläuterung:

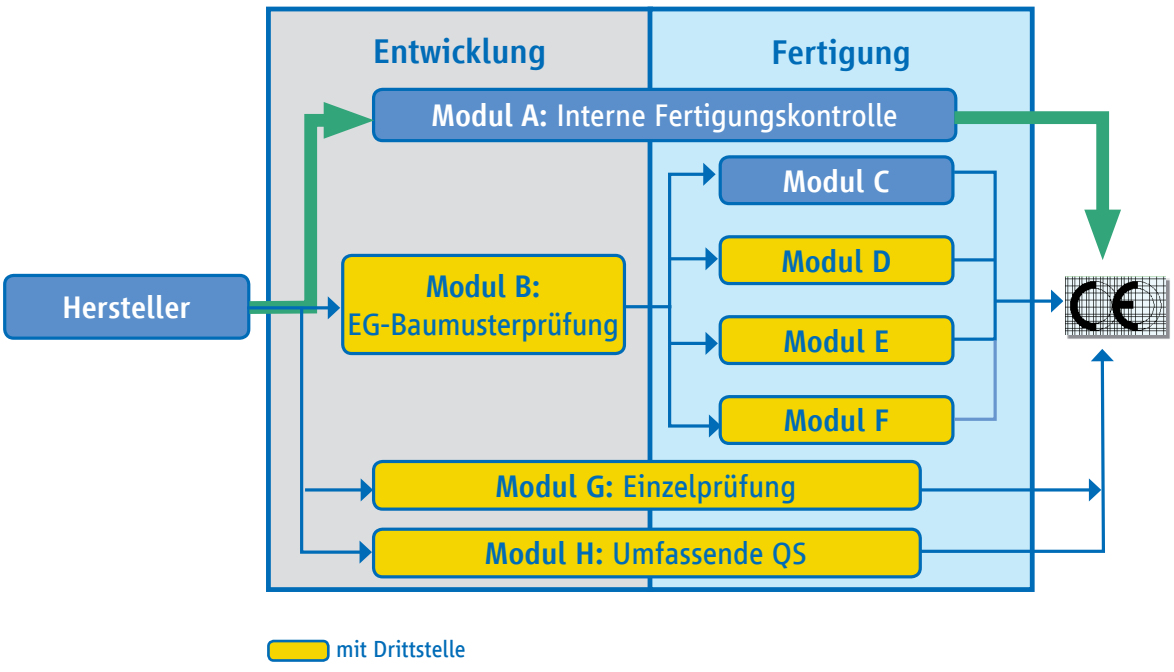
Produkt-klasse	Erläuterung	Modulfestlegung
A.1	Vernetzbare Produkte, die für den Einsatz in kritischen Infrastrukturen bestimmt sind und deren Ausfall, Störung oder Manipulation die Vertraulichkeit, Verfügbarkeit oder Integrität der Infrastruktur gefährden würde	Einbindung einer Drittstelle über wahlweise Modul B + D Modul G Modul H
A.2	Vernetzbare Produkte, die für den Einsatz in kritischen Infrastrukturen bestimmt sind und deren Ausfall, Störung oder Manipulation die Vertraulichkeit, Verfügbarkeit oder Integrität der Infrastruktur nicht gefährden würde	Einbindung einer Drittstelle über wahlweise Modul A Modul B + D Modul G Modul H
B	Alle anderen vernetzbaren Produkte	Modul A mit Herstellerselbsterklärung
C	Vernetzbare Produkte, die im Sinne einer Komponente dazu bestimmt sind, durch einen Hersteller in andere Produkte oder Anlagen eingebaut zu werden und daher nur begrenzte Security-Funktionalitäten beinhalten	Kein Konformitätsbewertungsverfahren, aber Informationsbereitstellung hinsichtlich der vorhandenen Cybersicherheitsmaßnahmen an den Verwender. „Was kann die Komponente und was kann sie nicht?“

A.7 Übersicht Konformitätsbewertungsverfahren

Es ist anzunehmen, dass Modul A für viele vernetzbare Produkte im niedrigen Risikoumfeld anwendbar ist. Daher wird es hier gesondert beschrieben, um einen ersten Eindruck zu ermöglichen.

Übersicht: Konformitätsbewertungsverfahren nach NLF

(Anhang 2 zu Beschluss 768/2008/EU)



Übersicht der Anforderung Modul A (nach 768/2008) – Interne Fertigungskontrolle[3]:

1. Bei der internen Fertigungskontrolle handelt es sich um das Konformitätsbewertungsverfahren, mit dem der Hersteller die in den Nummern 4, 5 und 6 genannten Verpflichtungen erfüllt sowie gewährleistet und auf eigene Verantwortung erklärt, dass die betreffenden Produkte den für sie geltenden Anforderungen der Rechtsvorschrift genügen.

2. Bewertung der Cybersicherheit: Der Hersteller hat die Cybersicherheit seines Produkts zu bewerten, um festzustellen, ob es die wesentlichen Anforderungen nach Anhang A.3 erfüllt. Bei der Bewertung der Cybersicherheit sind alle üblichen Bedingungen zu berücksichtigen, die beim bestimmungsgemäßen sowie beim vernünftigerweise vorherzusehenden Gebrauch abzusehen sind.

3. Verwendung und Bewertung von Komponenten: Werden für ein Produkt Komponenten bestimmungsgemäß verwendet/zusammengefügt, so kann der Hersteller deren Konformitätsbewertungsergebnisse im Hinblick auf die Cybersicherheit übernehmen.

4. Technische Unterlagen: Der Hersteller erstellt die technischen Unterlagen. Anhand dieser Unterlagen muss es möglich sein, die Übereinstimmung des Produkts mit den betreffenden Anforderungen zu bewerten; sie müssen eine nach Maßgabe dieser Rechtsvorschrift ausgeführte geeignete Risikoanalyse und -bewertung enthalten.[4] In den technischen Unterlagen sind die geltenden Anforderungen aufzuführen und der Entwurf, die Herstellung und der Betrieb des Produkts zu erfassen, soweit sie für die Bewertung von Belang sind.

   Die technischen Unterlagen enthalten gegebenenfalls zumindest folgende Elemente:
   - eine allgemeine Beschreibung des Produkts mit seiner festgelegten Produktklasse nach A.6,
   - Beschreibungen und Erläuterungen, die zum Verständnis dieser Unterlagen sowie der für die Cybersicherheit relevanten Funktionsweisen des Produkts erforderlich sind,
   - eine Aufstellung, welche harmonisierten Normen und/oder anderen einschlägigen technischen Spezifikationen, deren Fundstellen im Amtsblatt der Europäischen Union veröffentlicht wurden, vollständig oder in Teilen angewandt worden sind, und eine Beschreibung, mit welchen Lösungen den wesentlichen Anforderungen des Gesetzgebungsinstruments insoweit genügt wurde, als diese harmonisierten Normen nicht angewandt wurden. Im Fall von teilweise angewendeten harmonisierten Normen werden die Teile, die angewendet wurden, in den technischen Unterlagen angegeben,
   - die Ergebnisse der Konstruktionsberechnungen, Prüfungen usw. und
   - Prüfberichte.

5. Herstellung von Waren: Der Hersteller trifft alle erforderlichen Maßnahmen, damit der Fertigungsprozess und seine Überwachung die Übereinstimmung der Produkte mit den in Nummer 4 genannten technischen Unterlagen und mit den für sie geltenden Anforderungen der Rechtsvorschriften gewährleistet.

6. Konformitätskennzeichnung und Konformitätserklärung:
   a. Der Hersteller bringt an jedem einzelnen Produkt, das den geltenden Anforderungen der Rechtsvorschrift genügt, die nach der Rechtsvorschrift vorgeschriebene Konformitätskennzeichnung an.

[3] Hinweis: Die Anforderungspunkte 2 und 3 des Moduls A gelten auch für die anderen Module.

[4] Als Grundlage für die Risikoanalyse können internationale Spezifikationen dienen.

b. Der Hersteller stellt für ein Produktmodell eine schriftliche Konformitätserklärung aus und hält sie zusammen mit den technischen Unterlagen zehn Jahre lang nach dem Inverkehrbringen des Produkts für die nationalen Behörden bereit. Aus der Konformitätserklärung muss hervorgehen, für welches Produkt sie ausgestellt wurde. Ein Exemplar der Konformitätserklärung wird den zuständigen Behörden auf Verlangen zur Verfügung gestellt.

7. Bevollmächtigter: Die in Nummer 6 genannten Verpflichtungen des Herstellers können von seinem Bevollmächtigten in seinem Auftrag und unter seiner Verantwortung erfüllt werden, falls sie im Auftrag festgelegt sind.

A.8 Weitere Hinweise für die Ausgestaltung der Verordnung

A.8.1 Bedeutung der Marktüberwachung

Die Marktüberwachung ist übergreifend geregelt, zum Beispiel in der Verordnung (EG) 765/2008. Eine effektive und funktionierende Marktüberwachung ist wichtig für das Gelingen der Verordnung.

A.8.2 Rolle internationaler Security-Normen

Vermutungswirkung: Bei vernetzbaren Produkten, die mit harmonisierten Normen oder Teilen davon übereinstimmen, deren Fundstellen im Amtsblatt der Europäischen Union veröffentlicht worden sind, wird eine Konformität mit den Anforderungen von A.3 vermutet, die von den betreffenden Normen oder Teilen abgedeckt sind. Internationale Normen fließen aufgrund der Frankfurter- und Wiener-Abkommen vorrangig in die europäische Normung ein.

A.8.3 Übergangsfristen

Die Übergangsfristen sind industrietauglich, das heißt in Berücksichtigung des jeweiligen Produktlebenslaufs (oder der jeweiligen Produktklasse) zu gestalten. Sinnvoll erscheint eine Staffelung der Zeiträume. Wie üblich sollte die Übergangsfrist beginnen, wenn die Veröffentlichung im Amtsblatt für Produkte, die dann in Verkehr gebracht werden (= Abgabe vom Hersteller in den Markt bzw. bei Importprodukten der Grenzübertritt in den Unionsmarkt), erfolgt ist.

A.8.4 Übergangs- und Ausnahmeregelungen

Die aus diesem Vorschlag resultierenden Anforderungen gelten nur für neu in Verkehr gebrachte Endprodukte nach Ablauf der Übergangsfristen. Der bereits in Verkehr gebrachte und installierte Bestand wird davon nicht berührt; entsprechend ergeben sich keine Pflichten für die Hersteller.

Des Weiteren ist der Abverkauf von langlebigen Produktgenerationen und Lagerbeständen durch anwendungsbezogene Ausnahmen oder Übergangsfristen (siehe A.8.3) zu gewährleisten, auch wenn die Produkte die Anforderungen dieses Vorschlags oder des aktuellen Stands der Technik zum Zeitpunkt ihres Inverkehrbringens nicht bzw. nicht vollständig erfüllen.

Zur Aufrechterhaltung der Betriebsfähigkeit von kritischen Infrastrukturen und von langlebigen Investitionsgütern muss zudem gewährleistet sein, dass baugleiche Produkte für deren Instandhaltung und Erweiterung weiterhin dem Betreiber zur Verfügung gestellt werden können. Dies umfasst auch Produkte, die dem Stand der Technik für Cybersicherheit nicht mehr entsprechend, aber bei denen durch kompensierende Maßnahmen das Schutzziel weiterhin erreicht wird (zum Beispiel im Rahmen von „Defense in Depth"-Konzepten), sodass die Produkte weiterhin in sicheren Anwendungen eingesetzt werden können.

Über den ZVEI

Der ZVEI - Zentralverband Elektrotechnik- und Elektronikindustrie e. V. vertritt die gemeinsamen Interessen der Elektroindustrie und der zugehörigen Dienstleistungsunternehmen in Deutschland. Rund 1.600 Unternehmen haben sich für die Mitgliedschaft im ZVEI entschieden. Die Branche beschäftigt in Deutschland über 872.000 Arbeitnehmer und weitere 706.000 weltweit.

Der ZVEI repräsentiert eine Branche mit 192 Milliarden Euro Umsatz im Jahr 2017. Etwa 40 Prozent davon entfallen auf neuartige Produkte und Systeme. Jede dritte Neuerung im Verarbeitenden Gewerbe insgesamt erfährt ihren originären Anstoß aus der Elektroindustrie.

ZVEI - Zentralverband Elektrotechnik-
und Elektronikindustrie e.V.
Lyoner Straße 9
60528 Frankfurt am Main

Telefon: +49 69 6302-0
Fax: +49 69 6302-317
E-Mail: zvei@zvei.org
www.zvei.org