POSITION | CYBERSICHERHEIT | EU-GESETZGEBUNG

Europaweite Cyberregulierung

Einführung horizontaler Cybersicherheitsanforderungen auf Basis des New Legislative Framework und Brücke zum EU Cybersecurity Act

1. Februar 2021

Executive Summary

Die deutsche Industrie liefert mit nachfolgendem Vorschlag einen wichtigen Beitrag zur Umsetzung der neuen EU-Cybersicherheitsstrategie, um Europas Zukunft digital, resilient und sicher zu gestalten. Deutsche Unternehmen sind bestrebt, risikoadäquat cyberresiliente Produkte, Prozesse und Dienstleistungen anzubieten. Dafür ist es wichtig, dass ihre Bemühungen zur Stärkung der Cyberresilienz durch konsistente und EU-weit einheitliche Anforderungen unterstützt werden. Da auf Produkte regelmäßig mehr als eine Vorschrift anzuwenden ist, sind insbesondere widerspruchsfreie und kohärente Anforderungen essenziell für den Erhalt der internationalen Wettbewerbsfähigkeit.

Anforderungen der Industrie an eine konsistente Cyberregulierung für Europa

Die deutsche Industrie unterstützt ausdrücklich die aktuell seitens der Europäischen Kommission laufenden und durch den Europäischen Rat unterstützten Überlegungen über die Einführung verpflichtender, horizontaler Cybersicherheitsanforderungen nach den Grundsätzen des New Legislative Framework (NLF). Aus Industriesicht sollten folgende Faktoren berücksichtigt werden:

1) Um eine übergreifende Cyberresilienz zu erreichen, sollten ***allgemeinverbindliche Schutzziele*** gesetzlich definiert und diese dann durch ***harmonisierte Europäische Normen (hEN)***, die die dynamische Entwicklung des Stands der Technik widerspiegeln, konkretisiert werden.
2) Schutzmaßnahmen und die Widerstandfähigkeit gegen Cyberangriffe müssen sich an der spezifischen Anwendung und der damit verbundenen Bedrohungslage orientieren. Das NLF erlaubt die ***Abdeckung unterschiedlicher Risikolevel*** und folgt dem notwendigen ***risikobasierten Ansatz***. Dabei ist es Aufgabe des Herstellers als Inverkehrbringer, den bestimmungsgemäßen Einsatzbereich (und damit die Bedrohungslage) des Produkts festzulegen.
3) Die ***CE-Kennzeichnung*** wirkt durch die Kombination aus Konformitätsbewertung und Marktüberwachung als Vertrauensanker für private und gewerbliche Kunden gleichermaßen.
4) Der Digitale Binnenmarkt wird nur erfolgreich sein, wenn nationale Insellösungen vermieden werden und eine ***Anschlussfähigkeit zu internationalen Normen*** gewährleistet ist.
5) Mit einer ***Brücke*** zwischen den ***Cybersicherheitsanforderungen einer produktbezogenen horizontalen NLF-basierten EU-Rechtsvorschrift*** und einschlägigen ***Schemata*** unter dem ***EU-Cybersecurity Act*** (CSA) können sich beide Konzepte ergänzen. So können auch in der Verbindung der beiden Rechtsakte kohärente Cybersicherheitsanforderungen für die erfassten Produkte realisiert werden.
6) ***Kohärente Cybersicherheitsanforderungen*** erlauben dem Hersteller die ***Wahl zwischen harmonisierten Europäischen Normen (hEN) und CSA-Schemata***, um die Konformitätsbewertung auf der Grundlage der NLF-basierten EU-Rechtsvorschrift durchzuführen. Werden hEN angewendet, kann der Hersteller die Konformitätsvermutung nutzen.

BDI Bundesverband der Deutschen Industrie e.V.
DIN
DKE

Inhaltsverzeichnis

Notwendigkeit verpflichtender horizontaler Cybersicherheitsanforderungen

Durch die voranschreitende Verbreitung digitaler Technologien entstehen mannigfaltige neue Chancen – für private wie gewerbliche Nutzergruppen. Gleichzeitig ergeben sich mit der Digitalisierung auch zahlreiche Herausforderungen hinsichtlich Safety und Security sowie Privacy, die zusätzliche Risiken bedeuten können. Diesen Risiken kann mit zielgerichteten technischen, regulatorischen und verhaltensbezogenen Maßnahmen (beispielsweise Security-by-Design) entgegengewirkt werden. Durch die gezielte Anwendung des Standes der Technik bei den Maßnahmen zur Stärkung der Widerstandsfähigkeit lassen sich die verbleibenden Restrisiken entsprechend reduzieren.

Für das störungsfreie Funktionieren von in hohem Maße digitalisierten Prozessen, vernetzbaren Produkten und Dienstleistungen ist ein hoher Grad an Cyberresilienz eine Grundvoraussetzung. Kohärente gesetzliche Anforderungen sind der Schlüssel zum Erhalt der internationalen Wettbewerbsfähigkeit der deutschen und europäischen Industrie. Insbesondere gilt es zu berücksichtigen, dass Produkte – verstanden als Hardware, Software sowie als Kombination daraus – zu teils hochgradig komplexen Systemen integriert werden und es folglich auch der Beachtung von Wechselwirkungen in der Regulierung bedarf. Übereilte gesetzliche Ergänzungen und Erweiterungen bei gesetzlichen Anforderungen zur Cyberresilienz gilt es wirksam zu vermeiden. In diesem Zusammenhang begrüßen BDI, DIN und DKE ausdrücklich, dass der Europäische Rat die Notwendigkeit für komplementäre und vergleichbare Anforderungen an Cybersicherheitsfunktionalitäten von IT-Systemen und IT-Komponenten in den Ratsschlussfolgerungen vom 2. Dezember 2020 zur Cybersicherheit vernetzbarer IT-Produkte unterstreicht.

Gleichzeitig müssen Anforderungen an die Widerstandfähigkeit gegen Cyberangriffe den veränderten Bedrohungsszenarien und -intensitäten immer wieder angepasst werden. Starre gesetzliche Bestimmungen allein können das nicht leisten. Vielmehr müssen Gesetze und harmonisierte technische Europäische Normen (hEN) zusammenwirken, um den dynamischen Anforderungen an die Cyberresilienz gerecht zu werden.

Einführung horizontal verpflichtender Cybersicherheitsanforderungen nach den Grundsätzen des NLF

Aktuell gibt es einige Vorhaben, Cybersicherheitsanforderungen in verschiedene produktgruppenspezifische Richtlinien (RL) aufzunehmen, darunter insbesondere entsprechende Überlegungen zur Maschinen-RL sowie die in Vorbereitung befindlichen delegierten Rechtsakte der Radio Equipment Directive (RED). Die deutsche Industrie unterstützt den von der Europäischen Kommission verfolgten Ansatz, einen horizontalen verpflichtenden Cybersicherheitsrechtsakt nach den Grundsätzen des New Legislative Frameworks (NLF) einzuführen. BDI, DIN und DKE begrüßen ausdrücklich die grundsätzliche Unterstützung des Europäischen Rats für dieses Vorhaben.[1] Auch der Zeitplan, spätestens im vierten Quartal 2021 den Entwurf eines entsprechenden Binnenmarktrechtsakt unter dem NLF vorzulegen, findet unsere volle Unterstützung. Ein solcher horizontaler Ansatz ist der Einführung von Cybersicherheitsanforderungen in verschiedene produktspezifische Rechtsakte vorzuziehen, da dieser auch eine Fragmentierung der Cybersicherheitsanforderungen vermeidet. Anders als in Punkt 12 der Ratsschlussfolgerungen vom 2. Dezember 2020 dargestellt, sollte das vordergründige Ziel der kommenden Monate die Entwicklung verpflichtender, horizontaler Cybersicherheitsanforderungen nach den

[1] Vergleich die Schlussfolgerungen des Europäischen Rats vom 2. Dezember 2020 zur Cybersicherheit vernetzbarer IT-Produkte (13629/20).

Grundsätzen des NLF und nicht eine Entwicklung von freiwilligen Schemata für vernetzbare Produkte und Dienstleistungen auf Basis des EU-Cybersecurity Acts (CSA) sein, da hierfür zukünftig die horizontalen NLF-basierten Cybersicherheitsanforderungen dienen werden.

Folgende sechs Faktoren sprechen aus Sicht der deutschen Industrie für einen horizontalen NLF-basierten Ansatz für das Themenfeld Cybersicherheit:

1) Schutzziele gesetzlich definieren, Details in harmonisierten Europäischen Normen regeln

Während die Erfüllung der Anforderungen aus den Schemata des EU-Cybersecurity Acts (CSA) a priori freiwillig ist, sind verpflichtende Anforderungen für Produkte nur über eine NLF-basierte Verordnung (gemäß Beschluss 768/2008) möglich. Dabei sind horizontale Anforderungen grundsätzlich dem Hinzufügen von Cybersicherheitsanforderungen in vertikale Rechtsakte vorzuziehen, da dadurch eine Fragmentierung der Cybersicherheitsanforderungen vermieden und zudem die Kohärenz der Anforderungen gewährleistet werden kann.

Die Stärke des NLF liegt insbesondere im Zusammenspiel von gesetzlichen Vorgaben und harmonisierten Europäischen Normen (hEN), also den von den europäischen Normungsorganisationen auf Grundlage eines Auftrages der Kommission zur Durchführung von Harmonisierungsvorschriften nach Verordnung (EU) 1025/2012 erarbeiteten Normen, die nach Prüfung durch die Kommission im EU-Amtsblatt („Official Journal“) gelistet werden. Die EU-Institutionen legen die grundlegenden Anforderungen für Produkte in Richtlinien und Verordnungen fest. Beispiele dafür sind die Elektromagnetische-Verträglichkeits-Richtlinie, die Niederspannungs-Richtlinie und die Maschinen-Richtlinie. Die inhaltlich-technische Ausgestaltung erfolgt dann durch die Fachexperten in den Normungsgremien, entsandt beispielsweise von der öffentlichen Hand, der Wirtschaft, der Forschung sowie Organisationen des Verbraucher-, Gesundheits-, Umwelt- und Arbeitsschutzes. Diese erarbeiten europaweit harmonisierte technische Normen. Die europäischen Normungsorganisationen CEN, CENELEC und ETSI dienen in dem Prozess als offene Moderationsplattformen zur Erarbeitung dieser hEN. Der Prozess steht über die nationalen Spiegelgremien allen interessierten Stakeholdern offen. Der Fortschritt der Normung ist für alle transparent, sodass eine hohe Planbarkeit auf allen Seiten vorliegt. Die Entscheidungen werden im Konsens getroffen, erfreuen sich breiter Akzeptanz und haben Relevanz für den gesamten Binnenmarkt. Durch diese Arbeitsteilung wird der europäische Gesetzgeber von der Erarbeitung der Detailregelungen entlastet, der Rechtsrahmen wird flexibel gehalten und die so entstehenden Normen sind praxisnah und damit leicht durch Unternehmen zu implementieren. Nach einer Bewertung der Konformität durch den Hersteller oder durch Dritte können die Produkte nach dem Prinzip „one standard, one test, accepted everywhere” auf dem gesamten Binnenmarkt frei vermarktet werden.

Aus dem Zusammenspiel von harmonisierten Europäischen Normen und gesetzlichen Vorgaben folgt, dass sich der Gesetzgeber auf Schutzziele beschränken kann und technische Details zur Umsetzung dieser Schutzziele erst durch die Normung konkretisiert werden. Dadurch wird der Weiterentwicklung des Stands der Technik effizient Rechnung getragen. Dieses Zusammenspiel hat sich seit der Einführung des New Approach im Jahr 1985 und mit dessen Weiterentwicklung in das New Legislative Framework mittels EG-Verordnung 765/2008 über die letzten 30 Jahre hervorragend bewährt und ist auch prädestiniert für die neuen Herausforderungen der Cybersicherheit im Rahmen der Digitalisierung. Der BDI ist überzeugt, dass das NLF einen geeigneten Ansatz bietet, um eine regulatorische Basis für vernetzbare Cyberprodukte im EU-Binnenmarkt zu schaffen.

Der BDI spricht sich daher für die Definition horizontaler Cybersicherheitsanforderungen über das NLF im Sinne von grundlegenden Anforderungen aus. Die konkrete Ausgestaltung der gesetzlichen

Anforderungen würde wie beschrieben über Normen erfolgen. Dafür kann auf die jeweiligen Normungsgremien für die Entwicklung von hEN im Bereich Cybersicherheit, in denen die Experten aktiv sind, zurückgegriffen werden.

Als Best-Practice-Beispiel für die Definition horizontaler, produktgruppenübergreifender Anforderungen lässt sich die EMV-Richtlinie anführen. Sie regelt die elektromagnetische Verträglichkeit horizontal als Phänomenrichtlinie, unabhängig davon, wo das Phänomen elektromagnetische Verträglichkeit zu beachten ist. Als sogenannte „Auffang-Richtlinie“ erfasst die EMV-RL mithin alle Endprodukte mit dem Hintergrund elektromagnetischer Verträglichkeit. Spiegelbildlich hierzu sollten die horizontalen Cybersicherheitsanforderungen auf Basis des NLF, Aspekte des Phänomens „Cybersicherheit“ produktgruppenunabhängig regeln und als Anforderungen für die Vermarktung auf dem Binnenmarkt verstanden werden. Hierzu zählen z.B. die Implementierung von Security-by-Design, eine ordentliche Verschlüsselung sowie sichere Passwörter.

2) Innovationsfreundlicher und technologieoffener Ansatz: Stand der Technik anwenden

Nicht nur potenzielle Angriffsvektoren, Schwachstellen und Bedrohungsszenarien wandeln sich beständig, auch werden Schutzmaßnahmen durch Unternehmen und die Cybersicherheitsforschung konstant weiterentwickelt. Gerade für Anforderungen an die Cyberresilienz ist der innovationsfreundliche und technologieoffene Ansatz des NLF prädestiniert, um praxisnahe Anforderungen zu entwickeln.

3) Abdeckung unterschiedlicher Risikolevel

Schutzmaßnahmen und die Widerstandfähigkeit gegen Cyberangriffe müssen sich jedoch stets an der Anwendung und der damit verbundenen Bedrohungslage orientieren. Es wäre weder technologisch noch ökonomisch zielführend, wenn Smart-Home-Lösungen den gleichen Anforderungen Genüge tun müssten, wie Komponenten, die in Kritischen Infrastrukturen für deren Integrität und Verfügbarkeit von herausgehobener Bedeutung sind (vgl. Kritische Komponenten gemäß § 2 Abs. 13 IT-SiG 2.0-E). Eine „one-size-fits-all“-Lösung wäre somit der falsche Ansatz. Die Durchführung der Konformitätsbewertung und die CE-Kennzeichnung nach den Anforderungen aus den Vorschriften unter dem NLF sind eingeübte Praxis in Unternehmen. Sie ermöglichen zudem risikobasierte Konformitätsbewertungsverfahren (von der Herstellerselbsterklärung bis zur Einzelprüfung (Modul A bis G)) und ist damit für ein breites Spektrum an Produkten und Anwendungsfeldern geeignet.

4) Pflichten der Wirtschaftsakteure

Der NLF-Beschluss 768/2008/EG legt allgemeine Verpflichtungen für alle Wirtschaftsakteure entlang der gesamten Lieferkette – dies sind Hersteller, Bevollmächtigte, Einführer und Händler, einschließlich der Akteure des Onlinehandels – fest. Alle Wirtschaftsakteure müssen die erforderlichen Maßnahmen ergreifen, um zu gewährleisten, dass nur Produkte auf den EU-Markt gelangen, die mit den geltenden Rechtsvorschriften übereinstimmen. Hersteller und Einführer müssen die geltenden Anforderungen einhalten, wenn sie Produkte zum Verkauf anbieten oder in Verkehr bringen.

Das Schutzziel Cyberresilienz erfordert einen ganzheitlichen Ansatz. Die Einführung von Cybersicherheitsanforderungen in einer Richtlinie nach den Grundsätzen des NLF richtet sich an die Hersteller als Inverkehrbringer und sollte durch komplementäre Regelungen – außerhalb des NLF – für entsprechende Betreiberpflichten ergänzt werden.

5) Inverkehrbringen, CE-Kennzeichnung und Marktüberwachung

Das NLF ist dabei insbesondere auf das Inverkehrbringen, also die erstmalige Bereitstellung eines Produkts auf dem Europäischen Binnenmarkt ausgerichtet. Ziel ist es, dass alle von Herstellern und Einführern auf dem Europäischen Binnenmarkt in Verkehr gebrachten Produkte und Dienstleistungen die Anforderungen an Safety und Security erfüllen und dadurch eine sichere Inbetriebnahme gewährleistet ist.

Die CE-Kennzeichnung ist die Konformitätskennzeichnung des NLF-Ansatzes. Das NLF liefert nachvollziehbare Bedingungen für Konformitätskennzeichnung und Konformitätserklärung. Die Anwendung der CE-Kennzeichnung ist langjährig erprobt und etabliert. Private und gewerbliche Nutzer erkennen an der CE-Kennzeichnung die Einhaltung entsprechender Anforderungen. So wirkt die CE-Kennzeichnung durch die Kombination aus Konformitätsbewertung und Marktüberwachung als Vertrauensanker für private und gewerbliche Kunden gleichermaßen.

Zentraler Bestandteil des NLF-Ansatzes ist die Marktüberwachung. Sie erfolgt in Deutschland beispielsweise für die EMV- und Funkanlagenrichtlinie über die Bundesnetzagentur. Die Marktüberwachung stell sicher, dass im Binnenmarkt nur solche Produkte mit der CE-Kennzeichnung in Verkehr gebracht werden, die die entsprechenden Anforderungen erfüllen. Der Gesetzgeber muss folglich die zuständigen Behörden für die Marktüberwachung auch hinsichtlich des Bereichs „Cybersicherheit“ ertüchtigen, Prüfungen im Hinblick auf die Einhaltung der geforderten Schutzziele kompetent vornehmen und/oder beauftragen zu können. Aus Sicht der deutschen Industrie kann die Rolle der Bundesnetzagentur als kompetente Stelle der Marktüberwachung als Best Practice angesehen werden.

6) Nationale Insellösungen vermeiden, internationale Anschlussfähigkeit wahren

Cybersecurity ist eine globale Herausforderung. Folglich sind nationale Alleingänge nicht zielführend. Der Europäische Binnenmarkt ist ein Erfolgsmodell, das es gilt, weiterzuführen – gerade im digitalen Zeitalter. Der Binnenmarkt ist Vorbild für andere Märkte und setzt Maßstäbe für Produktanforderungen und Konformitätsbewertungsverfahren, die einen schnellen Marktzugang erlauben und innovationsfreundlich sind. Daher sprechen sich BDI, DIN und DKE gegen eine regulatorische Fragmentierung des europäischen Binnenmarktes sowie gegen nationale Sonderwege aus. Die Wahrung der Cyberresilienz von Produkten, Prozessen und Systemen verlangt europäische Regulierungsansätze, die global anschlussfähig sind. Daher sollten die Anforderungen soweit als möglich auf international einheitlichen technischen Normen basieren. Dies entspräche in hohem Maße den Interessen der stark auf globalisierte Wertschöpfung ausgerichteten deutschen Industrie.

Aus der Gesamtschau der oben genannten Vorteile ergibt sich für die deutsche Industrie die Notwendigkeit, rasch horizontal verpflichtende Cybersicherheitsanforderungen auf Basis des NLF einzuführen und spätestens 2023 in Kraft treten zu lassen, um – unter Einhaltung angemessener Übergangsfristen – baldmöglichst Effekte zu erzielen. Ziel muss es sein, grundlegende Anforderungen an die Cyberresilienz für alle für den Europäischen Binnenmarkt bestimmten Produkte (in dem noch zu bestimmenden Anwendungsbereich) zu definieren. Nur so wird Europa langfristig die Potenziale der Digitalisierung nutzen und gleichzeitig die damit verbundenen Risiken proaktiv managen können.

Brücke zwischen horizontalem NLF-Rechtsakt und CSA-Schemata

Nur durch inhaltlich kohärente gesetzliche Anforderungen kann sichergestellt werden, dass die Wirtschaftsakteure diese auf ihre Produkte, Prozesse, Dienstleistungen und Systeme anwenden können.

Die deutsche Industrie spricht sich dezidiert für die Einführung horizontal verpflichtender Cybersicherheitsanforderungen nach den Grundsätzen des NLF aus. Dem gegenüber verfolgt der CSA die Entwicklung EU-weit harmonisierter Zertifizierungsschemata zur freiwilligen Zertifizierung. Unter bestimmten Bedingungen sieht der CSA auch die Möglichkeit vor, die Zertifizierung nach einzelnen Schemata verpflichtend vorzuschreiben, was jedoch im Konflikt zum NLF-Beschluss (768/2008) stehen würde. Der CSA sieht aber auch den Fall vor, dass Schemata im Rahmen eines Rechtsakts für das Konformitätsbewertungsverfahren angewendet werden können. Damit ist eine Brücke zwischen dem horizontalen Cybersicherheitsrechtsakt auf Basis des NLF und den Schemata des CSA gegeben. Artikel 54 Absatz 3 CSA (EU 2019/881) bietet hierfür die rechtliche Grundlage:

"Soweit dies in einem bestimmten Rechtsakt der Union so festgelegt ist, kann eine Zertifizierung oder eine EU- Konformitätserklärung, die auf der Grundlage eines europäischen Schemas für die Cybersicherheitszertifizierung ausgestellt wurde, dafür verwendet werden kann, die Vermutung zu begründen, dass eine Übereinstimmung mit den Anforderungen jenes Rechtsakts gegeben ist."[2]

Für Produktgruppen, für die basierend auf dem CSA bereits ein freiwilliges Cybersicherheitszertifizierungsschema erarbeitet wurde, könnte folglich dieses wahlweise und alternativ zum Nachweis der Konformität mit den horizontalen Cybersicherheitsanforderungen des NLF-Rechtsaktes genutzt werden, sofern es keine Widersprüche in den Anforderungen gibt. Die Anwendung eines Schemas als Teil eines Konformitätsbewertungsverfahrens würde demnach zur Erfüllung des NLF-Rechtsaktes führen, wobei im Falle eines Widerspruchs der NLF-Rechtsakt Priorität haben muss.

Dabei muss betont werden, dass dieses Vorgehen umso leichter zu realisieren ist, je ähnlicher die inhaltlichen Anforderungen eines Schemas mit bestehenden und künftigen harmonisierten Europäischen Normen sind. Die Verantwortungsträger im CSA-Prozess sind daher aufgerufen, sich eng mit den Normungsvorhaben zu synchronisieren und vorrangig auf die „Europäisierung" bestehender nationaler Schemata zu konzentrieren. Ein Divergieren der inhaltlichen Anforderungen zwischen CSA-Schemata und im Rahmen des NLF anerkannter harmonisierter Europäischer Normen (hEN) muss aus oben gezeigten Gründen unbedingt vermieden werden. Vielmehr sollte, wie in Punkt 10 und 11 der Ratsschlussfolgerungen vom 2. Dezember 2020 betont, verstärkt auf die Entwicklung europäischer und internationaler Normen und Standards zur Cybersicherheit von vernetzbaren Produkten gesetzt werden.

Cybersecurity erfordert einen ganzheitlichen Ansatz unter Einbeziehung aller Akteure

Jeder muss seinen Betrag für die Cybersicherheit leisten: Hersteller sowie private und gewerbliche Anwender sind gleichsam gefragt. Dies wird auch dadurch deutlich, dass für den gewerblichen und den privaten Gebrauch bestimmte Produkte miteinander vernetzt werden. Der Erfolg, das heißt eine ganzheitliche Stärkung des Cybsicherheitsniveaus in Europa, kann sich folglich nur einstellen, wenn alle an einem Strang ziehen und die Maßnahmen aufeinander abgestimmt werden. Zudem muss ein abgestimmtes Vorgehen gesetzlich ermöglicht und in der Praxis umgesetzt werden. Durch ganzheitliche Cybersicherheitsstrategien mit effizienten Schutzmaßnahmen kann das Risiko von Cybersicherheitsvorfällen reduziert und dadurch die Cyberresilienz ganzheitlich gestärkt werden. Ziel muss es

[2] EN: "Where a specific Union legal act so provides, a certificate or an EU statement of conformity issued under a European cybersecurity certification scheme may be used to demonstrate the presumption of conformity with requirements of that legal act."

sein, gefährliche Lücken und Schwachstellen durch rasche und angemessene Maßnahmen zu schließen, damit potenzielle Angreifer diese nicht ausnutzen können. Der ganzheitliche Ansatz ist mehr als die Summe der Einzelmaßnahmen eines jeden Wirtschaftsakteurs. Jeder Akteur muss seinen vorab definierten Beitrag zu einem abgestimmten Gesamtergebnis beisteuern.

Neben der Wirtschaft sind jedoch auch Privatanwender sowie staatliche Stellen gefordert, ihren Beitrag zur Stärkung und Wahrung der Cyberresilienz von Produkten und Dienstleistungen zu leisten. So sind die ***Mitgliedsstaaten*** durch die im NLF implementierte Marktüberwachung verpflichtet, ihre zuständigen Behörden für die Marktüberwachung so zu ertüchtigen, dass diese Prüfungen im Hinblick auf die Einhaltung der geforderten Schutzziele kompetent vornehmen und/oder beauftragen können. Dies würde dann auch hinsichtlich des Bereichs Cybersicherheit gelten. Aus Sicht der deutschen Industrie kann die Rolle der Bundesnetzagentur als kompetente Stelle der Marktüberwachung als Best Practice angesehen werden.

Impressum

Bundesverband der Deutschen Industrie e.V. (BDI)
Breite Straße 29, 10178 Berlin
www.bdi.eu
T: +49 30 2028-0

Redaktion
Dr. Thomas Holtmann
Leiter Abteilung Umwelt, Technik, Nachhaltigkeit
T: +49302028-1550
T.Holtmann@bdi.eu

Dr. Thomas Koenen
Leiter Abteilung Digitalisierung und Innovation
T: +49 30 2028-1415
T.Koenen@bdi.eu

Steven Heckler
Referent Digitalisierung und Innovation
T: +49 30 2028-1523
S.Heckler@bdi.eu

Johannes Benjamin Helfritz
DIN e.V.
Projektkoordinator External Relations
T: +49302601-2791
Benjamin.Helfritz@din.de

Johannes Koch
DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE
Leiter Nationale Normungspolitik und Kooperationen
T: +49 69 6308-268
Johannes.Koch@vde.com

Katja Krüger
DIN e.V.
Senior Government Relations Manager
T: +49 30 2601-2439
Katja.Krueger@din.de

BDI Dokumentennummer: D 1248