CYBER|NTELLIGENCE
.Institute

Quo vadis, Cybersecurity? Einblicke und Ausblicke auf die aktuelle und künftige EU Cybersicherheitsregulierung

Prof. Dr. jur. Dennis-Kenji Kipker

Der Wandel des Cybersecurity-Rechts

Tagesspiegel

Background Cybersecurity, 27.04.2023

Cybersecurity ohne Cybersecurity?! Der Weg der Generalklauseln

Gesetz betreffend die Gesellschaften mit beschränkter Haftung (GmbHG)
§ 43 Haftung der Geschäftsführer

(1) Die Geschäftsführer haben in den Angelegenheiten der Gesellschaft die Sorgfalt eines ordentlichen Geschäftsmannes anzuwenden.
(2) Geschäftsführer, welche ihre Obliegenheiten verletzen, haften der Gesellschaft solidarisch für den entstandenen Schaden.

Aktiengesetz
§ 91 Organisation. Buchführung

(1) Der Vorstand hat dafür zu sorgen, daß die erforderlichen Handelsbücher geführt werden.
(2) Der Vorstand hat geeignete Maßnahmen zu treffen, insbesondere ein Überwachungssystem einzurichten, damit den Fortbestand der Gesellschaft gefährdende Entwicklungen früh erkannt werden.
(3) Der Vorstand einer börsennotierten Gesellschaft hat darüber hinaus ein im Hinblick auf den Umfang der Geschäftstätigkeit und die Risikolage des Unternehmens angemessenes und wirksames internes Kontrollsystem und Risikomanagementsystem einzurichten.

Cybersecurity ohne Cybersecurity?! Der Weg der Generalklauseln

Bürgerliches Gesetzbuch (BGB)
§ 823 Schadensersatzpflicht

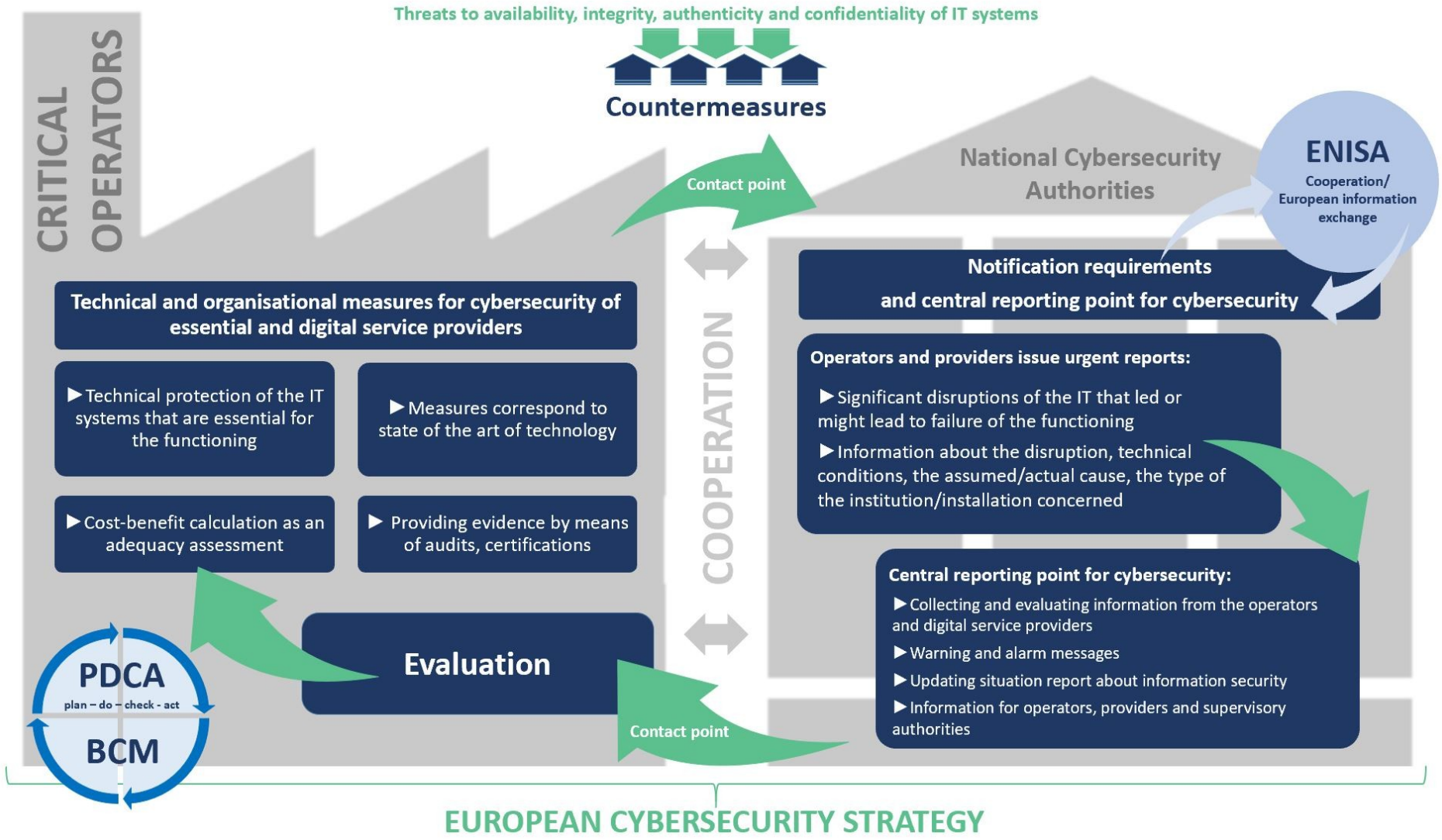
(1) Wer vorsätzlich oder fahrlässig das Leben, den Körper, die Gesundheit, die Freiheit, das Eigentum oder ein sonstiges Recht eines anderen widerrechtlich verletzt, ist dem anderen zum Ersatz des daraus entstehenden Schadens verpflichtet.
(2) Die gleiche Verpflichtung trifft denjenigen, welcher gegen ein den Schutz eines anderen bezweckendes Gesetz verstößt. Ist nach dem Inhalt des Gesetzes ein Verstoß gegen dieses auch ohne Verschulden möglich, so tritt die Ersatzpflicht nur im Falle des Verschuldens ein.

Gesetz über die Haftung für fehlerhafte Produkte (Produkthaftungsgesetz - ProdHaftG)
§ 1 Haftung

(1) Wird durch den Fehler eines Produkts jemand getötet, sein Körper oder seine Gesundheit verletzt oder eine Sache beschädigt, so ist der Hersteller des Produkts verpflichtet, dem Geschädigten den daraus entstehenden Schaden zu ersetzen. Im Falle der Sachbeschädigung gilt dies nur, wenn eine andere Sache als das fehlerhafte Produkt beschädigt wird und diese andere Sache ihrer Art nach gewöhnlich für den privaten Ge- oder Verbrauch bestimmt und hierzu von dem Geschädigten hauptsächlich verwendet worden ist.

Und das Ergebnis davon?
Lange Zeit war Cybersecurity so:

Der Ursprung: Cybersecurity als KRITIS-Aufgabe



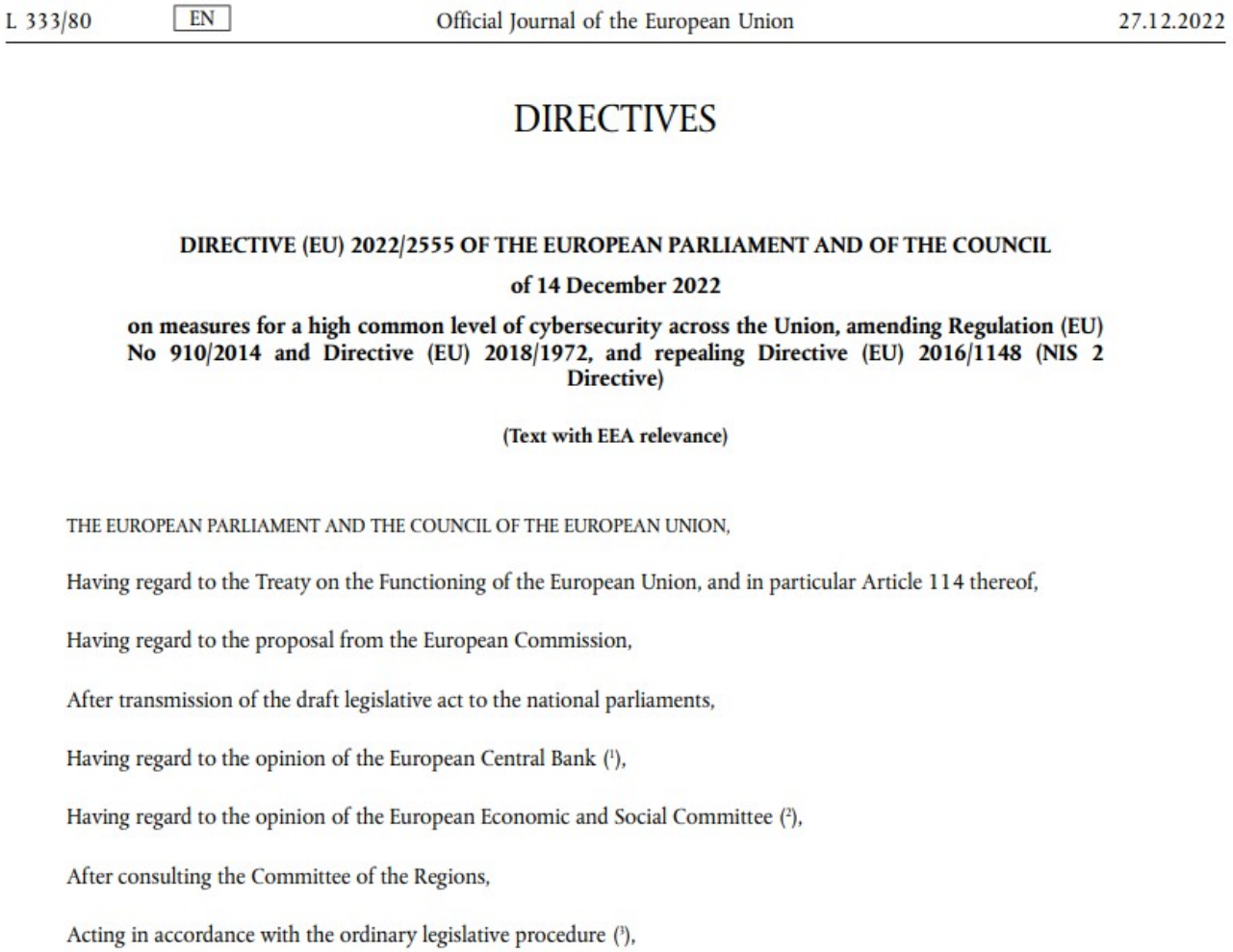
Die Welt besteht aber nicht nur aus KRITIS…

13. September 2017, State of the Union Address, former President Jean-Claude Juncker:

"*In the past three years, we have made progress in keeping Europeans safe online. But Europe is still not well equipped when it comes to cyber attacks. This is why, today, the Commission is proposing new tools, including a European Cybersecurity Agency, to help defend us against such attacks.*"

Cybersecurity Compliance: Warum sich der ganzheitliche Blick lohnt!

- **EU NIS-RL** (2016)
- **EU Cybersecurity Verordnung/Act** (2019): Befugnisausbau der ENISA, einheitlicher europäischer Zertifizierungsrahmen
- **EU NIS 2-RL** (2022)
- **EU Cyber Resilience Act** (CRA, Frühjahr 2024)
- **IT-SiG** (2015) und **BSI-KritisV** (2016, 2017, …, 2023)
- **IT-SiG 2.0** (2021)
- **NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz - NIS2UmsuCG** (vermutlich Ende 2024)
- **(KRITIS-Dachgesetz (KRITIS-DachG))**



L 333/80 EN Official Journal of the European Union 27.12.2022

DIRECTIVES

DIRECTIVE (EU) 2022/2555 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 14 December 2022

on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)

(Text with EEA relevance)

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 114 thereof,

Having regard to the proposal from the European Commission,

After transmission of the draft legislative act to the national parliaments,

Having regard to the opinion of the European Central Bank (1),

Having regard to the opinion of the European Economic and Social Committee (2),

After consulting the Committee of the Regions,

Acting in accordance with the ordinary legislative procedure (3),

NIS 2 im Überblick

- **Richtlinie (EU) 2022/2555** des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148
- Verkündung im **EU-Amtsblatt am 27.12.2022**
- Richtlinie = Umsetzungsfrist für Mitgliedstaaten in **nationales Recht bis 17.10.2024**
- Aufhebung der Vorgängerregelung **NIS 1 zum 18.10.2024**
- Unterscheidung zwischen **„wesentlichen“** und **„wichtigen“** Einrichtungen
- Grundsatz der **Mindestharmonisierung**
- **Abgrenzung zu bereichsspezifischen Rechtsakten** wie z.B. DORA zu beachten

NIS 2 im Überblick

- Cybersicherheit nicht nur für Kritische Infrastrukturen, sondern flächendeckend als **allgemeine Compliance-Anforderung für die Wirtschaft** (vgl. bereits nationales **IT-SiG 2.0**)
- NIS 2 grds. anwendbar auf **öffentliche + private Einrichtungen**, die ihre Dienste in der Union erbringen oder ihre Tätigkeiten dort ausüben
- **Einschränkungen + Bereichsausnahmen** für öffentlichen Sektor
- Weitere Konkretisierung durch:
  - **Anhang I** (Sektoren mit hoher Kritikalität)
  - **Anhang II** (Sonstige kritische Sektoren)
- Mitgliedstaaten erstellen bis zum **17.04.2025** eine Liste wesentlicher und wichtiger Einrichtungen
- **„Europäische Überformung mit nationalstaatlichem Beurteilungsspielraum“**

NIS 2 setzt mit einheitlichen Schwellenwerten europäische Standards

Mittlere Unternehmen gem. Empfehlung 2003/361/EG: Beschäftigung von min. 50 Personen und Jahresumsatz/Jahresbilanz übersteigt 10 Mio. EUR

Unternehmen, die die Schwellenwerte für mittlere Unternehmen nach EU-Recht überschreiten (min. 250 Beschäftigte und Jahresumsatz von mehr als 50 Mio. EUR oder Jahresbilanz von mehr als 43 Mio. EUR)

Von Unternehmensgröße unabhängig, soweit qualifizierende Faktoren erfüllt sind, z.B. wegen kritischer Tätigkeit, Auswirkungen auf öff. Ordnung, Systemrisiken, grenzüberschreitenden Auswirkungen

Europäische kritische Sektoren nach NIS 2

Sektoren nach Anhang I	Sektoren nach Anhang II
Energie	Post- und Kurierdienste
Verkehr	Abfallbewirtschaftung
Bankwesen	Produktion, Herstellung und Handel mit chem. Stoffen
Finanzmarktinfrastrukturen	Produktion, Verarbeitung und Vertrieb von Lebensmitteln
Gesundheitswesen	**Verarbeitendes Gewerbe/Herstellung von Waren, u.a. Datenverarbeitungsgeräte, elektronische und optische Erzeugnisse und Ausrüstungen, Maschinenbau, Kraftwagen, Kraftwagenteile, Fahrzeugbau**
Trinkwasser	Anbieter digitaler Dienste
Abwasser	Forschungseinrichtungen
Digitale Infrastruktur	
Verwaltung von IKT-Diensten	
Öffentliche Verwaltung	
Weltraum	

NIS 2: Diskussion und Stand der Umsetzung in Deutschland

Bearbeitungsstand: 03.07.2023 15:45

Referentenentwurf

des Bundesministeriums des Innern und für Heimat

Entwurf eines Gesetzes zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung

(NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz – NIS2UmsuCG)

A. Problem und Ziel

Die moderne Wirtschaft Deutschlands ist für ihr Funktionieren, die Generierung von Wohlstand und Wachstum und auch für ihre Adaptionsfähigkeit auf geänderte wirtschaftspolitische und geopolitische Rahmenbedingungen angewiesen auf funktionierende und resiliente Infrastrukturen, sowohl im physischen als auch im digitalen Bereich. Diese Faktoren haben i
sich nic
rung vo
führen
schaftsb
toren. I
dabei e
Versorg
fällen. C
nenmar
innerha
der Cyb
rungen
tigkeiter
und des
Cybersi
der Rich
333 vor
päische

DENNIS-KENJI KIPKER / TILMANN DITTRICH

Rolle der Kritischen Infrastrukturen nach dem neuen NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz

Nationale Besonderheiten und europäische Überformung

Der Schutz von für die Gemeinschaft elementar-notwendigen Einrichtungen vor Cybergefahren stellt eine der größten Herausforderungen der aktuellen Zeit dar – und das nicht erst seit Beginn des Russland-Ukraine-Kriegs. Bislang maßgeblich war hier in Deutschland das BSIG und die dessen Anwendungsbereich konkretisierende BSI-KritisV, ergänzt um die 2016 hinzugetretenen europäischen Anforderungen der ersten NIS-RL. Doch hat das IT-Sicherheitsrecht umfassende Überarbeitungen erfahren, indem nicht nur die europäischen Vorgaben in

das nationale Recht implementiert wurde. Mit neues IT-Sicherheitsgesetz 2.0 in 2021 die Vorgaben des ersten deutschen IT-Si 2015 an die gegenwärtige Bedrohungs tualisiert. Der nachfolgende Beitrag gibt neuen NIS-2-RL und deren Umsetzung e über die umfassenden Änderungen für schen Infrastrukturen und zeigt dabei U gleich zur geltenden Rechtslage auf. Les

rung und rechtspolitischer und

die EU-Kommission und der Europäische Auswärtige neue europäische Cybersicherheitsstrategie vor, rch die Verwerfun- h die Resilienz zu urde.[1] Die aktuel- neue Richtlinien den NIS-RL[3] und RL genannt), die Oktober 2024 r die Resilienz- or physischen ckpunktepa- IS-2-RL wird gs- und Cy- nationale zentwurf[6] verschie- alen Cy- e zusätz- womit in die-

II. Sicherheit in der Information Betreibern und Einrichtungen

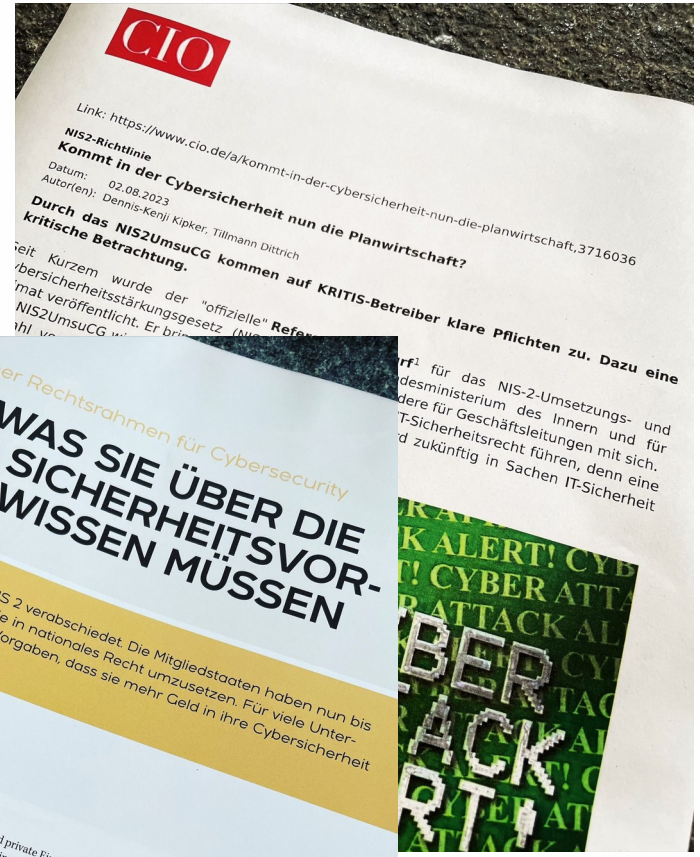
Bislang sind die Vorschriften für Kritische Infra lem in den §§ 8a, 8b BSIG[7] zu finden. Diese ar KRITIS bemessene knappe Darstellung dürfte Bestand mehr haben. So wird in Teil 3 des BSI heit in der Informationstechnik von Einrichtu adressiert und bringt erhebliche Neuerungen

1. Neuer Anwendungsbereich des BSI Abgrenzung zu weiteren Rechtsakten

Die gesetzlichen Vorschriften zur IT-Sicherheit nach § 28 Abs. 1 BSIG-E zukünftig auf Betreiber gen, besonders wichtige Einrichtungen und „le ge Einrichtungen, soweit dies durch die BSI-K Abs. 1 BSIG-E[8] entsprechend festgelegt wurde. S Untergliederung wird deutlich, dass der deutsch den in NIS-2 verwendeten Wortlaut und die dorti dung zwischen „wesentlichen“ und „wichtigen“ für irreführend hielt und deshalb eine begriffliche und Klarstellung zum europäischen Recht vornimm ber der „Kritischen Anlagen“ sind in diesem Zusam höchste Qualifikationsstufe zu sehen. rungen zu den Unte

Bundesministerium des Innern und für Heimat

Werkstattgespräch– Diskussionspapier des BMI für wirtschaftsbezogene Regelungen zur Umsetzung der NIS-2-RL



CIO

Link: https://www.cio.de/a/kommt-in-der-cybersicherheit-nun-die-planwirtschaft,3716036

NIS2-Richtlinie

Kommt in der Cybersicherheit nun die Planwirtschaft?

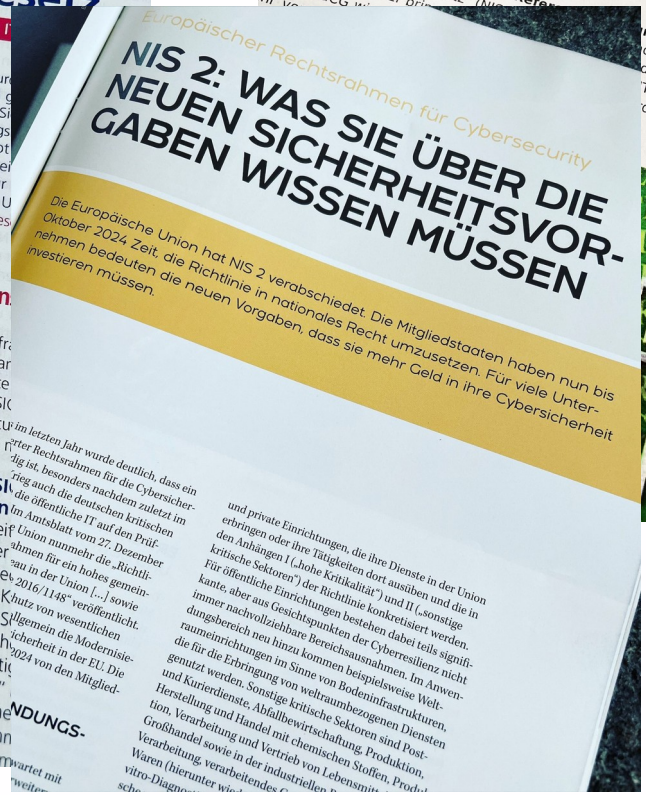
Datum: 02.08.2023

Autor(en): Dennis-Kenji Kipker, Tillmann Dittrich

Durch das NIS2UmsuCG kommen auf KRITIS-Betreiber klare Pflichten zu. Dazu eine kritische Betrachtung.

Seit Kurzem wurde der "offizielle" Refer
Cybersicherheitsstärkungsgesetz
mat veröffentlicht. Er bri
NIS2UmsuCG

rf[1] für das NIS-2-Umsetzungs- und desministerium des Innern und für dere für Geschäftsleitungen mit sich. T-Sicherheitsrecht führen, denn eine d zukünftig in Sachen IT-Sicherheit



Europäischer Rechtsrahmen für Cybersecurity

NIS 2: WAS SIE ÜBER DIE NEUEN SICHERHEITSVORGABEN WISSEN MÜSSEN

Die Europäische Union hat NIS 2 verabschiedet. Die Mitgliedstaaten haben nun bis Oktober 2024 Zeit, die Richtlinie in nationales Recht umzusetzen. Für viele Unternehmen bedeuten die neuen Vorgaben, dass sie mehr Geld in ihre Cybersicherheit investieren müssen.

im letzten Jahr wurde deutlich, dass ein erter Rechtsrahmen für die Cybersicher- dig ist, besonders nachdem zuletzt im rieg auch die deutschen kritischen die öffentliche IT auf den Prüf- im Amtsblatt vom 27. Dezember Union nunmehr die „Richtli- ahmen für ein hohes gemein- au in der Union [...] sowie 2016/1148“ veröffentlicht. hutz von wesentlichen llgemein die Modernisie- icherheit in der EU. Die 2024 von den Mitglied- NDUNGS- wartet mit

und private Einrichtungen, die ihre Dienste in der Union erbringen oder ihre Tätigkeiten dort ausüben und die in den Anhängen I („hohe Kritikalität“) und II („sonstige kritische Sektoren“) der Richtlinie konkretisiert werden. Für öffentliche Einrichtungen bestehen dabei teils signifikante, aber aus Gesichtspunkten der Cyberresilienz nicht immer nachvollziehbare Bereichsausnahmen. Im Anwendungsbereich neu hinzu kommen beispielsweise Weltraumeinrichtungen im Sinne von Bodeninfrastrukturen, die für die Erbringung von weltraumbezogenen Diensten genutzt werden. Sonstige kritische Sektoren sind Post- und Kurierdienste, Abfallbewirtschaftung, Produktion, Herstellung und Handel mit chemischen Stoffen, Produktion, Verarbeitung und Vertrieb von Lebensmitteln, Großhandel sowie in der industriellen Verarbeitung, verarbeitendes Waren (hierunter

Konkretisierung der neuen europäischen Vorgaben durch NIS2UmsuCG

- NIS2UmsuCG: „**NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz**“
- NIS2UmsuCG nicht nur als Umsetzung von NIS 2, sondern zahlreiche **Neuerungen auch im allgemeinen nationalen Cybersicherheitsrecht** (z.B. bei BSI-Befugnissen)
- **Bislang veröffentlichte Fassungen:**
  - **03.04.2023:** BMI-RefE (3-Spalten-Dokument mit Vergleich der aktuellen Gesetzesfassung/Änderungen)
  - **03.07.2023:** BMI-RefE schlägt umfassende Änderungen im BSIG vor
  - **27.09.2023:** Diskussionspapier des BMI für wirtschaftsbezogene Regelungen der NIS-2-Richtlinie in Deutschland
  - **26.10.2023:** Werkstattgespräch des BMI für wirtschaftsbezogene Regelungen zur Umsetzung der NIS-2-RL
  - **…?**

NIS2UmsuCG-E: Anwendungsbereich und Kategorien der betroffenen Einrichtungen

Kritische Anlagen	Besonders wichtige Einrichtungen	Wichtige Einrichtungen
▪ Ersetzt „Kritische Infrastruktur“ ▪ Anlage, die für das Funktionieren des Gemeinwesens von hoher Bedeutung ist, da durch ihren Ausfall oder ihre Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit eintreten würden ▪ Wesentliches Kriterium: „Bestimmender Einfluss“ auf die Anlage	▪ „Kritische Anlage“ ist ebenfalls Subkategorie der besonders wichtigen Einrichtung ▪ Inhaltliche Überschneidungen zu KRITIS im qualitativen/sektorbezogenen Bereich ▪ Quantitativ dreiteilige Abstufung von Unternehmen jedweder Größe, mittleren Unternehmen und Großunternehmen anhand Empfehlung 2003/361/EG	▪ Sehr weit gefasst und führen voraussichtlich zum größten Zuwachs an neuen Anwendungsfällen nach NIS2UmsuCG ▪ „KRITIS-Versorgungsgrenze“ spielt keine Rolle mehr ▪ Z.B. auch mittlere Unternehmen/Großunternehmen in Produktion, Chemie, Ernährung, verarbeitendes Gewerbe betroffen

NIS2UmsuCG-E: Risikomanagement zur Cybersicherheit

Anforderung	Umsetzung
Kohärenz zwischen physischer Sicherheit und Cybersicherheit	Berücksichtigung von Cybersicherheit und nicht cyberbezogenen Risiken
Einsatz von Künstlicher Intelligenz	Verwendung von KI-Tools zur ressourcenwirksameren Abwehr von Cyberangriffen
KMU-zentrierte Cybersicherheit	Maßnahmen, die begrenzten personellen und wirtschaftlichen Ressourcen Rechnung tragen
Aktiver Cyberschutz	SzA, Verschlüsselung, Netzwerksegmentierung, Zugriffsregelung
Schwachstellenmanagement	Entgegennahme von Schwachstelleninformationen von Dritten
Wirtschaftsspionage/Geschäftsgeheimnisschutz	Risikomanagement in der Beziehung mit Externen im weiter gefassten Ökosystem jenseits reiner Cybersicherheit
Cyberhygiene	Zero-Trust, Update-Policy, Awareness, Netzwerkkartografie
Governance auf Unternehmensleitungsebene	Leitungspersonen mit eigenem Know-how/Verantwortlichkeit
Dokumentation	Nachweis von Cybersicherheit als Prozessmanagement
Lieferkettenschutz	Untersuchung der Beziehungen zu externen IT-Lieferanten
Einbeziehung nichttechnischer Risikofaktoren	Rechtliche, politische und geostrategische Auswirkungen

Der Entwurf des EU Cyber Resilience Act (CRA)

- Stärkung der **horizontalen Cybersecurity** auf EU-Ebene schon lange Thema/von Branchenverbänden als bislang unzureichend kritisiert → vgl. Diskussion um **EU CSA (2019)**
- **Horizontale Regelungen** sollen vertikalen und produktgruppenspezifischen Rechtsakten vorgezogen werden → **Ziel:** Verhinderung von Fragmentierung/mehr Kohärenz in Anforderungen
- **Cyber Resilience Act (CRA):** Kommissionsentwurf vorgestellt Mitte September 2022, Trilog Ende November 2023 abgeschlossen
- Die „Spinne im Netz“: Umfassende **Bezugspunkte zu weiteren EU-Rechtsakten** (z.B. NIS 2, AIA, CSA, MaschinenVO)

Der Entwurf des EU Cyber Resilience Act (CRA)

Zentrale regulatorische Aspekte des künftigen EU-Rechtsaktes:

- Breites Spektrum: Materielle digitale Produkte (drahtlos/drahtgebunden), nicht eingebettete Software → **„Produkte mit digitalen Elementen“** → vernetzte Produkte/IoT
- **„Security by Design“** als Lebenszyklusanforderung, Risikobewertung, Dokumentationspflichten
- **Schutz der Lieferkette** unter Einbeziehung von Produkten aus Drittstaaten
- **Anlehnung an EU-Produkthaftung:** Verantwortlichkeit von Herstellern, Importeuren und Vertrieb
- Pflicht zu **Sicherheitsaktualisierungen** „by default“ angelehnt an Produktlebenszyklus → **Herstelleranforderungen zu EoL branchenspezifisch neu zu bestimmen!**

Abgrenzung NIS 2 und CRA

Cybersecurity Compliance als neuer Generalstandard

„Gefahrenabwehr“	„Compliance“	„Cybercrime“
▪ Schutz von KRITIS ▪ Gefahrenabwehr als vornehmlich staatlich geprägte Aufgabe ▪ „KRITIS-Dachgesetz“	▪ Produktsicherheitsanforderung für die Wirtschaft ▪ Entwicklung, Herstellung und Inverkehrbringung (cyber)sicherer Produkte jedweder Art ▪ Marktzulassung und Marktüberwachung	▪ Abwehr von Straftaten mit Cyberbezug ▪ Kontext: (Industrie)spionage ▪ Prävention als Bestandteil interner Unternehmenssicherheit

DENNIS-KENJI KIPKER / TILMANN DITTRICH

Rolle der Kritischen Infrastrukturen nach dem neuen NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz

Nationale Besonderheiten und europäische Überformung

IT-Sicherheitsrecht

Der Schutz von für die Gemeinschaft elementar-notwendigen Einrichtungen vor Cybergefahren stellt eine der größten Herausforderungen der aktuellen Zeit dar – und das nicht erst seit Beginn des Russland-Ukraine-Kriegs. Bislang maßgeblich waren hier in Deutschland das BSIG und die dessen Anwendungsbereich konkretisierende BSI-KritisV, ergänzt um die 2016 hinzugetretenen europäischen Anforderungen der ersten NIS-RL. Seither hat das IT-Sicherheitsrecht umfassende Überarbeitungen erfahren, indem nicht nur die europäischen Vorgaben in das nationale Recht implementiert wurden, sondern auch ein neues IT-Sicherheitsgesetz 2.0 in 2021 geschaffen wurde, das die Vorgaben des ersten deutschen IT-Sicherheitsgesetzes aus 2015 an die gegenwärtige Bedrohungslage anpasst und aktualisiert. Der nachfolgende Beitrag gibt nun auf Grund einer neuen NIS-2-RL und deren Umsetzung einen ersten Überblick über die umfassenden Änderungen für die bisherigen Kritischen Infrastrukturen und zeigt dabei Unterschiede im Vergleich zur geltenden Rechtslage auf. Lesedauer: 26 Minuten

I. Einführung und rechtspolitischer Hintergrund

2020 stellten die EU-Kommission und der Europäische Auswärtige Dienst die neue europäische Cybersicherheitsstrategie vor, die bereits in nicht unerheblichem Maße durch die Verwerfungen der Corona-Krise geprägt war, wodurch die Resilienz zu einem wesentlichen regulatorischen Aspekt wurde.[1] Die aktuelle EU-Cybersicherheitsstrategie brachte zwei neue Richtlinien mit sich: die NIS-2-RL[2] zur Ablösung der geltenden NIS-RL[3] und eine neue europäische Resilienz-RL[4] (auch CER-RL genannt), die beide Ende 2022 verabschiedet wurden und bis Oktober 2024 in den Mitgliedstaaten umgesetzt sein müssen. Für die Resilienz-RL, die Kritische Infrastrukturen (KRITIS) primär vor physischen Gefahren schützen soll, liegt bislang nur ein BMI-Eckpunktepapier für ein sog. „KRITIS-Dachgesetz" vor.[5] Die NIS-2-RL wird voraussichtlich durch das nationale NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS2UmsuCG) in das nationale Recht übertragen – Besonderheit dabei: Der Gesetzentwurf[6] geht über die EU-Vorgaben hinaus und bringt ebenso verschiedene spezifische Neuerungen ausschließlich im nationalen Cybersicherheitsrecht mit sich. Daraus ergibt sich auch die zusätzliche Bezeichnung „Cybersicherheitsstärkungsgesetz", womit klar wird, dass das vielzitierte „IT-Sicherheitsgesetz 3.0" in dieser Form erst einmal nicht kommen wird.

II. Sicherheit in der Informationstechnik von Betreibern und Einrichtungen

Bislang sind die Vorschriften für Kritische Infrastrukturen vor allem in den §§ 8a, 8b BSIG[7] zu finden. Diese an der Relevanz von KRITIS bemessene knappe Darstellung dürfte zukünftig keinen Bestand mehr haben. So wird in Teil 3 des BSIG-RefE die Sicherheit in der Informationstechnik von Einrichtungen umfassend adressiert und bringt erhebliche Neuerungen mit sich.

1. Neuer Anwendungsbereich des BSIG und Abgrenzung zu weiteren Rechtsakten

Die gesetzlichen Vorschriften zur IT-Sicherheit beziehen sich nach § 28 Abs. 1 BSIG-E zukünftig auf Betreiber Kritischer Anlagen, besonders wichtige Einrichtungen und „lediglich" wichtige Einrichtungen, soweit dies durch die BSI-KritisV iSd § 57 Abs. 1 BSIG-E[8] entsprechend festgelegt wurde. Schon bei dieser Untergliederung wird deutlich, dass der deutsche Gesetzgeber den in NIS-2 verwendeten Wortlaut und die dortige Unterscheidung zwischen „wesentlichen" und „wichtigen" Einrichtungen für irreführend hielt und deshalb eine begriffliche Abweichung und Klarstellung zum europäischen Recht vornimmt. Die Betreiber der „Kritischen Anlagen" sind in diesem Zusammenhang als höchste Qualifikationsstufe zu sehen. Die bisherigen Anforderungen zu den „Unternehmen im besonderen öffentlichen Interesse" (UBI) aus IT-SiG 2.0 gem. § 2 Nr. 14 BSIG geltende Fassung gehen zukünftig in den besonders wichtigen und wichtigen Einrichtungen auf.

a) Kritische Anlage

Die Kritische Anlage ersetzt den bisherigen Begriff der Kritischen Infrastrukturen iSd BSIG, der sich im RefE zum NIS2UmsuCG nicht mehr wiederfindet. Die Definition nach neuem Recht ist bislang komplex und mehrstufig-verweisungslastig. Ausgangspunkt sind wie nach geltendem Recht die Begriffsdefinitionen zu Beginn des BSIG. Demnach ist nach § 2 Abs. 1 Nr. 19 BSIG-E eine Anlage, die für das Funktionieren des Gemeinwesens von hoher Bedeutung ist, als Kritische Anlage zu qualifizieren, da durch ihren Ausfall oder ihre Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit eintreten würden. Zur weiteren Konkretisierung wird sodann auf § 28 Abs. 2a BSIG-E verwiesen – hier finden sich in

1 Abrufbar unter: https://www.consilium.europa.eu/de/policies/cybersecurity/.
2 RL (EU) 2022/2555 des Europäischen Parlaments und des Rates v. 14.12.2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der VO (EU) Nr. 910/2014 und der RL (EU) 2018/1972 sowie zur Aufhebung der RL (EU) 2016/1148 (NIS-2-RL), ABl. L 333/80.
3 RL (EU) 2016/1148 des Europäischen Parlaments und des Rates v. 6.7.2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union, ABl. L 194/1.
4 RL (EU) 2022/2557 des Europäischen Parlaments und des Rates v. 14.12.2022 über die Resilienz kritischer Einrichtungen und zur Aufhebung der RL 2008/114/EG des Rates, ABl. L 333/164.
5 Kipker/Dittrich MMR-Aktuell 2022, 454186.
6 Der Beitrag bezieht sich auf eine Synopse eines Referentenentwurfs, abrufbar unter: https://intrapol.org/2023/05/10/refe-fuer-ein-nis-2-umsetzungs-und-cybersicherheitsstaerkungsgesetz-nis2umsucg/.
7 Gesetz über das Bundesamt für Sicherheit in der Informationstechnik v. 14.8.2009, BGBl. I 2821.
8 Gegenwärtig § 10 Abs. 1 S. 1 BSIG.

Fazit und Ausblick: Den digitalen Infrastrukturschutz im Ganzen betrachten!

- **EU KOM Impact Assessment:** Erhöhung des unternehmerischen Cybersecurity-Budgets um 22% (neue Unternehmen) bzw. 12% (Bestandsunternehmen)
  - **Konkret:** ca. 30.000 betroffene Unternehmen/Einrichtungen mehr (sehr vorsichtige Schätzung)
  - **Wirtschaftlicher Mehrerfüllungsaufwand** ca. 1,65 Milliarden EUR jährlich
- **NIS-2:** Zwar erhebliche Ausdehnung des Anwendungsbereichs und deutlich stärkere europäische Überformung, eigentlich zu treffende TOM jedoch wenig überraschend (vgl. auch **IT-SiG 2.0, 2021**)
- **Komplexes Zusammenspiel mit weiteren Regelungen:** KRITIS-DachG, CRA, CSA, DORA, AIA, DS-GVO, Produkthaftungs- und Produktsicherheitsrecht, Durchführungsrechtsakte, Standardisierung
- ☾ **Prognose: 2024 ff. als „Cybersecurity-Jahre" mit Impact Factor mindestens ähnlich wie DS-GVO in 2018**

Vielen Dank!

Prof. Dr. Dennis-Kenji Kipker

cyberintelligence.institute

Research Director

MesseTurm

Friedrich-Ebert-Anlage 49

60308 Frankfurt a.M.

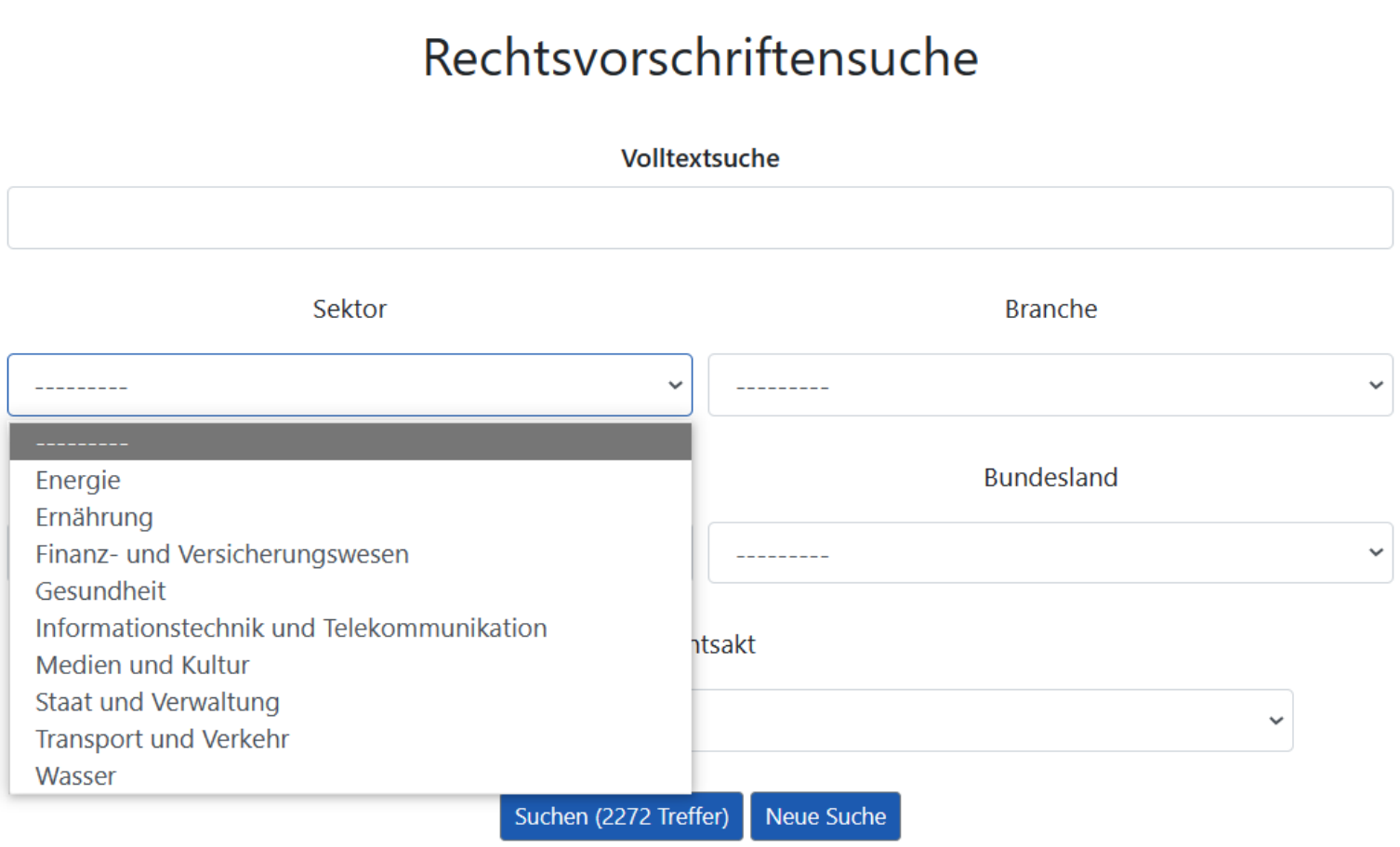
GERMANY

dennis.kipker@cyberintelligence.institute

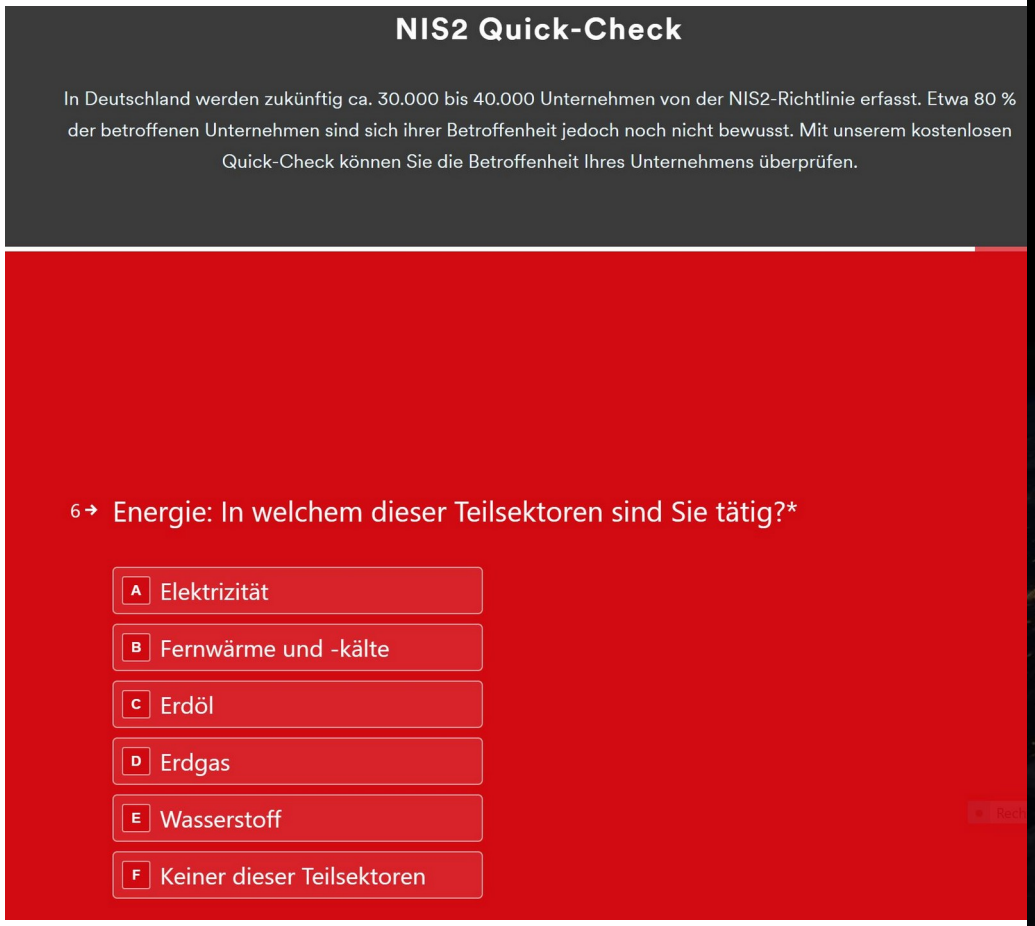
Cybersecurity Navigator

CYBERSECURITY
NAVIGATOR

https://cybersecurity-navigator.de



NIS2 Quick-Check: www.nis2-check.de



Weiterführende Literatur