CYBER INTELLIGENCE
.Institute

NIS 2: Verantwortlichkeit und Haftungsfragen

Prof. Dr. Dennis-Kenji Kipker

Lange Zeit war betriebliche Cybersecurity so:

Und nun ist betriebliche Cybersecurity so:

EU-REGULIERUNG

Cybersicherheit als Pflicht

Ein Gesetzentwurf sieht vor, dass Manager haften, wenn sie Cyberrisiken nicht prüfen. Das kann Führungskräfte abschrecken – und war auf EU-Ebene nicht vorgesehen.

Eren Basar

29.05.2023 - 10:29 Uhr • Kommentieren • 5 x geteilt

NIS 2: Viele denken zunächst nur an die Geldbußen...

Wesentliche Einrichtungen:

Entweder 10 Mio. Euro oder 2 % des weltweiten Jahresumsatzes, je nachdem, welcher Betrag höher ist

Wichtige Einrichtungen:

Entweder 7 Mio. Euro oder 1,4 % des weltweiten Jahresumsatzes, je nachdem, welcher Betrag höher ist

Dabei reicht die Verantwortlichkeit jedoch viel weiter...

Artikel 32

Aufsichts- und Durchsetzungsmaßnahmen in Bezug auf wesentliche Einrichtungen

(5) Erweisen sich die gemäß Absatz 4 Buchstaben a bis d und f ergriffenen Durchsetzungsmaßnahmen als unwirksam, so stellen die Mitgliedstaaten sicher, dass ihre zuständigen Behörden befugt sind, eine Frist festzusetzen, innerhalb derer die wesentliche Einrichtung die erforderlichen Maßnahmen ergreifen muss, um die Mängel zu beheben oder die Anforderungen dieser Behörden zu erfüllen. Für den Fall, dass die geforderten Maßnahmen nicht innerhalb der gesetzten Frist ergriffen werden, stellen die Mitgliedstaaten sicher, dass ihre zuständigen Behörden befugt sind,

a) die Zertifizierung oder Genehmigung für einen Teil oder alle von der wesentlichen Einrichtung erbrachten einschlägigen Dienste oder Tätigkeiten vorübergehend auszusetzen oder eine Zertifizierungs- oder Genehmigungsstelle oder ein Gericht im Einklang mit dem nationalen Recht aufzufordern, die Zertifizierung oder Genehmigung vorübergehend auszusetzen;

b) zu verlangen, dass die zuständigen Stellen oder Gerichte im Einklang mit dem nationalen Recht natürlichen Personen, die auf Geschäftsführungs- bzw. Vorstandsebene oder Ebene des rechtlichen Vertreters für Leitungsaufgaben in dieser wesentlichen Einrichtung zuständig sind, vorübergehend untersagen, Leitungsaufgaben in dieser Einrichtung wahrzunehmen.

(6) Die Mitgliedstaaten stellen sicher, dass jede natürliche Person, die für eine wesentliche Einrichtung verantwortlich ist oder auf der Grundlage ihrer Vertretungsbefugnis, der Befugnis, im Namen der Einrichtung Entscheidungen zu treffen, oder ihrer Kontrollbefugnis über die Einrichtung als Vertreterin der wesentlichen Einrichtung handelt, befugt ist zu gewährleisten, dass die Einrichtung diese Richtlinie erfüllt. Die Mitgliedstaaten stellen sicher, dass diese natürlichen Personen für Verstöße gegen ihre Pflichten zur Gewährleistung der Einhaltung dieser Richtlinie haftbar gemacht werden können.

§ 38

Umsetzungs-, Überwachungs- und Schulungspflicht für Geschäftsleitungen besonders wichtiger Einrichtungen und wichtiger Einrichtungen

(1) Geschäftsleitungen besonders wichtiger Einrichtungen und wichtiger Einrichtungen sind verpflichtet, die von diesen Einrichtungen nach § 30 zu ergreifenden Risikomanagementmaßnahmen umzusetzen und ihre Umsetzung zu überwachen.

(2) Geschäftsleitungen, die ihre Pflichten nach Absatz 1 verletzen, haften ihrer Einrichtung für einen schuldhaft verursachten Schaden nach den auf die Rechtsform der Einrichtung anwendbaren Regeln des Gesellschaftsrechts. Nach diesem Gesetz haften sie nur, wenn die für die Einrichtung maßgeblichen gesellschaftsrechtlichen Bestimmungen keine Haftungsregelung nach Satz 1 enthalten.

(3) Die Geschäftsleitungen besonders wichtiger Einrichtungen und wichtiger Einrichtungen müssen regelmäßig an Schulungen teilnehmen, um ausreichende Kenntnisse und Fähigkeiten zur Erkennung und Bewertung von Risiken und von Risikomanagementpraktiken im Bereich der Sicherheit in der Informationstechnik zu erlangen sowie um die Auswirkungen von Risiken sowie Risikomanagementpraktiken auf die von der Einrichtung erbrachten Dienste beurteilen zu können.

Bis hinein in das Vertrags- und Haftungsrecht:

Bürgerliches Gesetzbuch (BGB)
§ 241 Pflichten aus dem Schuldverhältnis

(1) Kraft des Schuldverhältnisses ist der Gläubiger berechtigt, von dem Schuldner eine Leistung zu fordern. Die Leistung kann auch in einem Unterlassen bestehen.

(2) Das Schuldverhältnis kann nach seinem Inhalt jeden Teil zur Rücksicht auf die Rechte, Rechtsgüter und Interessen des anderen Teils verpflichten.

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.

Bürgerliches Gesetzbuch (BGB)
§ 280 Schadensersatz wegen Pflichtverletzung

(1) Verletzt der Schuldner eine Pflicht aus dem Schuldverhältnis, so kann der Gläubiger Ersatz des hierdurch entstehenden Schadens verlangen. Dies gilt nicht, wenn der Schuldner die Pflichtverletzung nicht zu vertreten hat.

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.

Cybersecurity nach NIS 2 darf deshalb aber nicht darauf reduziert werden:

ANZEIGE

NIS2: Strenge Strafen für Verstöße gegen die Cybersicherheit

Die NIS2-Richtlinie sieht strenge Strafen für kritische Unternehmen vor, darunter Geldbußen von bis zu zehn Millionen Euro oder zwei Prozent des weltweiten Umsatzes sowie nicht-monetäre Strafen wie Compliance-Anordnungen und die öffentliche Bekanntgabe von Verstößen.

Sponsored Post von Kingston Technology 29. Oktober 2024, 9:00 Uhr

in Pocket speichern | merken

(Bild: Kingston Technology)

Kingston IronKey Keypad 200 erfüllt jetzt die NIST-Spezifikation FIPS 140-3 Level 3.

NIS 2: 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, insb. auch vor dem Kontext von KMU
Aktiver Cyberschutz	SzA, Verschlüsselung, Netzwerksegmentierung, Zugriffsregelung, Schwachstellenmanagement
Cyberhygiene	Zero-Trust, Update-Policy, Awareness, Netzwerkkartografie
Wirtschaftsspionage/Geschäftsgeheimnisschutz	Risikomanagement in der Beziehung mit Externen im weiter gefassten Ökosystem jenseits reiner Cybersicherheit
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

Die zentrale Frage: Welcher Sorgfaltsmaßstab gilt?

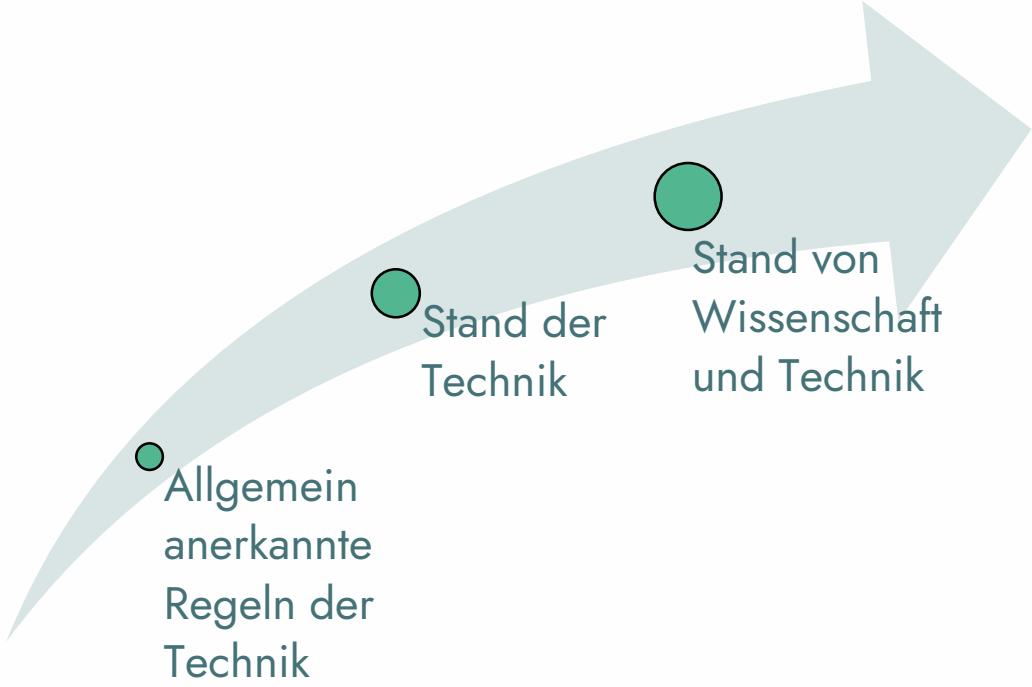
§ 30

Risikomanagementmaßnahmen besonders wichtiger Einrichtungen und wichtiger Einrichtungen

(1) Besonders wichtige Einrichtungen und wichtige Einrichtungen sind verpflichtet, geeignete, verhältnismäßige und wirksame technische und organisatorische Maßnahmen, die nach Absatz 2 konkretisiert werden, zu ergreifen, um Störungen der Verfügbarkeit, Integrität und Vertraulichkeit der informationstechnischen Systeme, Komponenten und Prozesse, die sie für die Erbringung ihrer Dienste nutzen, zu vermeiden und Auswirkungen von Sicherheitsvorfällen möglichst gering zu halten. Bei der Bewertung der Verhältnismäßigkeit der Maßnahmen nach Satz 1 sind das Ausmaß der Risikoexposition, die Größe der Einrichtung, die Umsetzungskosten und die Eintrittswahrscheinlichkeit und Schwere von Sicherheitsvorfällen sowie ihre gesellschaftlichen und wirtschaftlichen Auswirkungen zu berücksichtigen. Die Einhaltung der Verpflichtung nach Satz 1 ist durch die Einrichtungen zu dokumentieren.

(2) Maßnahmen nach Absatz 1 sollen den Stand der Technik einhalten, die einschlägigen europäischen und internationalen Normen berücksichtigen und müssen auf einem gefahrenübergreifenden Ansatz beruhen. Die Maßnahmen müssen zumindest Folgendes umfassen:

1. Konzepte in Bezug auf die Risikoanalyse und auf die Sicherheit in der Informationstechnik,
2. Bewältigung von Sicherheitsvorfällen,
3. Aufrechterhaltung des Betriebs, wie Backup-Management und Wiederherstellung nach einem Notfall, und Krisenmanagement,



Risikomanagement zur Cybersicherheit: Verhältnismäßigkeit

Welche Kritikalität besitzt eine Einrichtung? Ist sie in der Öffentlichkeit besonders exponiert?

Inwieweit ist eine Einrichtung in ihrer Funktion von vernetzten IT-Systemen abhängig?

Ist das Funktionieren der Einrichtung abhängig vom Funktionieren digitaler Lieferketten?

Hat es bereits Vorfälle in der Vergangenheit gegeben bzw. ist anzunehmen, dass sich Angriffe in Zukunft häufen werden?

Was könnten potenzielle Angreifer infolge einer erfolgreichen Kompromittierung der Einrichtung erlangen?

Was bedeutet das konkret?

Schutzschild gegen Haftungsrisiken

Wie die Rolle des CISO unter NIS-2 neu gedacht werden muss

Die sich ändernden Regelungen zur Haftung der Geschäftsführung im Cybersicherheitsumfeld führen auch zu veränderten Aufgaben bei den Verantwortlichen für Informationssicherheit im Unternehmen. Das kann für CISO &Co. aber durchaus auch positive Seiten haben, argumentieren unsere Autoren.

Recht §

Von Dennis-Kenji Kipker, Frankfurt/Main, und Julian Zaudig, Köln

In einer zunehmend digitalisierten Wirtschaft hat sich die Regulierung der IT-Sicherheit rasant entwickelt. Von der anfänglichen Fokussierung auf kritische Infrastrukturen (KRITIS) bis zur aktuellen NIS-2-Richtlinie und dem nationalen deutschen Umsetzungsgesetz (NIS2UmsuCG) hat sich der Anwendungsbereich deutlich erweitert und erfasst nun weite Teile der deutschen und europäischen Wirtschaft (vgl. [1,2]). Kernpunkt dieser neuen Regulierungsansätze ist die persönliche Verantwortung der Geschäftsführung und betrieblichen Verantwortungsträger für IT-Sicherheitsmaßnahmen.

zum Schlüssel zur Vermeidung von Haftungsrisiken wird. Die Autoren zeigen auf, wie ein strategisch positionierter CISO nicht nur zur rechtlichen Compliance beiträgt, sondern auch die Digitalisierung im Unternehmen aktiv unterstützt. In der neuen Ära der IT-Sicherheit wird der interdisziplinär agierende CISO zum unverzichtbaren Partner der Geschäftsleitung, indem er ein ganzheitliches, rechtlich konformes IT-Sicherheitskonzept gewährleistet.

Geschäftsleitung in der Haftung

bleiben – wie jeder Branchenstandard und jede technische Norm zur IT-Sicherheit – hochgradig abstrakt und damit juristisch unbestimmt. Deshalb hat auch der Gesetzgeber den „Heiligen Gral der IT-Sicherheit" noch nicht gefunden (vgl. [3]).

Toxische Mischung aus Legalitätspflicht und unbestimmten Rechtsvorschriften

Das NIS2UmsuCG will nunmehr den Geschäftsleitern mehr Verantwortung aufbürden: Durch die Diskussion um NIS-2 wird dabei auch außerhalb der juristischen Welt

Fallbeispiele

Aufgrund der zu erwartenden Rechtslage nach NIS-2, aber auch schon nach geltendem IT-Sicherheitsrecht lassen sich verschiedene Fallgestaltungen antizipieren, in denen eine Haftung klar ausscheidet oder gerade in Betracht kommt:

_____ *Augenblicksversagen:* keine Haftung. Eine Haftung entsteht nicht alleine dadurch, dass ein Schaden eingetreten ist oder dass auf der Arbeitsebene ein Fehler geschehen ist (so auch: EuGH C-687/21 Tz. 35ff.). IT-Sicherheit ist kein Zustand; der PDCA-Kreislauf nimmt Fehler zugunsten kontinuierlicher Selbstverbesserung hin.

_____ *Folgenloser Fehler:* keine Haftung. Es reicht ferner nicht aus, dass das ISMS in irgendeiner Weise fehlerhaft oder rechtswidrig war. Ein Schaden muss gerade kausal auf einer fehlerhaften und/oder rechtswidrigen Sicherheitsmaßnahme beruhen. Dieser Nachweis ist nicht trivial und ein fähiger Rechtsanwalt kann hier wirksam verteidigen.

Was bedeutet das konkret?

_____ *Fehlender Überblick und Schatten-IT:* klare Haftung. Eine Haftung kam schon allgemein in Betracht, wenn ein Geschäftsleiter sich keinen ausreichenden Überblick über die eigene IT und die daraus entstehenden Risiken verschaffte. Dies folgte früher – auch in der GmbH – aus § 91 Abs. 2 AktG, nun ist mit NIS-2 die Sicherheitsorganisation nach § 38 Abs. 1 BSIG-E erforderlich.

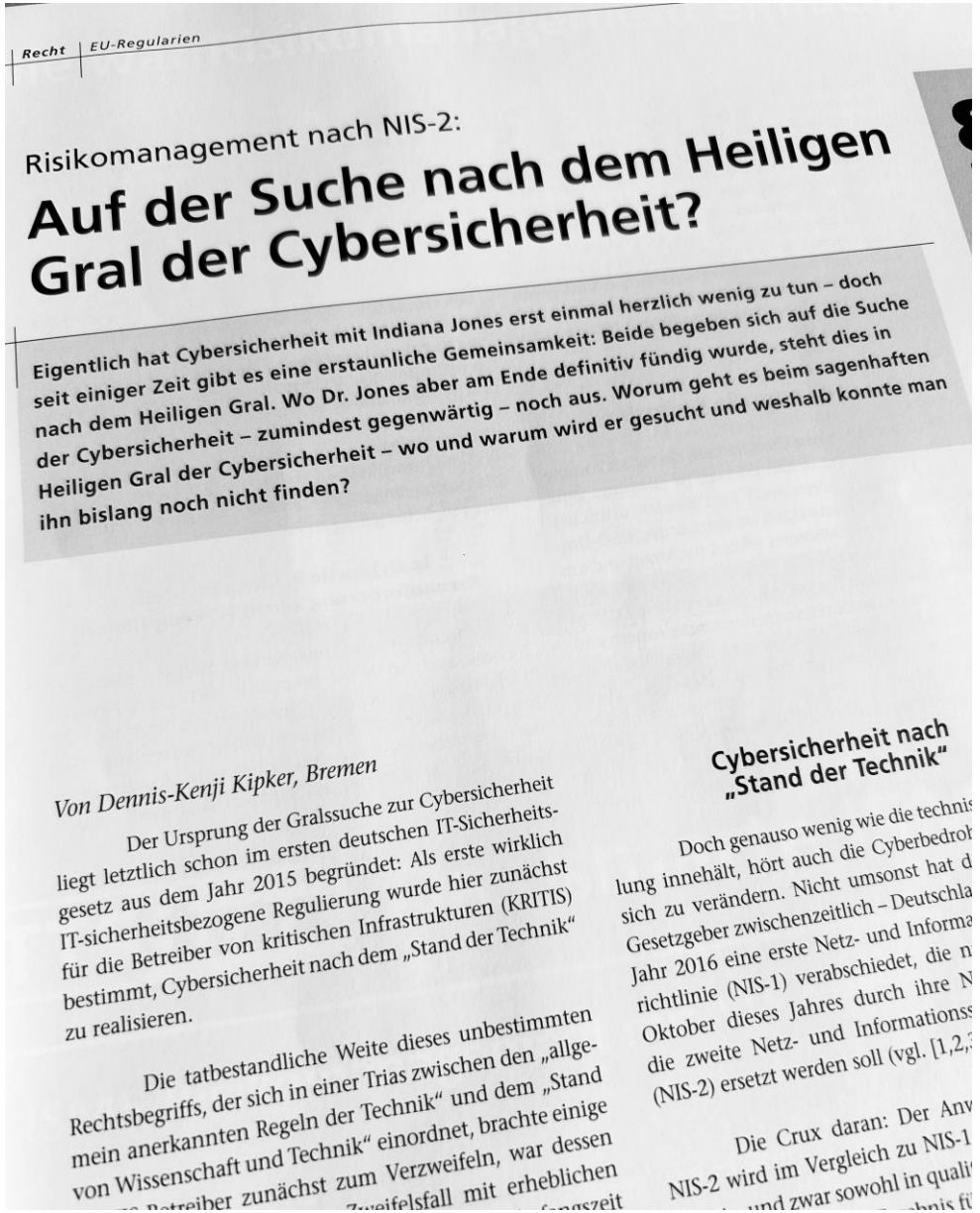
_____ *Unerkannter oder geduldeter „Schlendrian" im Betrieb:* klare Haftung. Die Umsetzung und Wirksamkeit von Maßnahmen ist zu überwachen. Dies war schon immer Teil einer gesellschaftsrechtlich korrekten Delegation von Aufgaben – nun ergibt sich das mit NIS-2 zusätzlich aus § 38 Abs. 1 BSIG-E. Auch regelmäßige Audits sind hier nicht ausreichend: Im rechtlich normierten Bereich fordert die Rechtsprechung nach ihrer wiederholt verwendeten Formel überraschende, stichprobenartige Kontrollen (BGH KRB 4/80), damit sich Mitarbeiter auf die Kontrollen nicht einstellen können.

_____ *„Das betrifft uns nicht!":* klare Haftung seit dem IT-SiG. Schon seit dem IT-SiG obliegt es jedem Unternehmen, selbst zu prüfen, ob Systeme reguliert sind oder nicht. Irrt sich ein Geschäftsleiter an dieser Stelle, verstößt er gegen seine Legalitätspflicht und müsste sich enthaften. Diese Enthaftung setzt die Einholung von Rechtsrat zu dieser Frage voraus.

_____ *„Das lohnt sich nicht!":* klare Haftung seit dem IT-SiG. Seit dem IT-Sicherheitsgesetz müssen sich regulierte IT-Sicherheitsmaßnahmen nicht mehr „lohnen" – stattdessen müssen sie den Ausfallfolgen von kritischer Infrastruktur angemessen sein (§ 8a Abs. 1 Satz 3 BSIG). Es sind also externalisierte Risiken in die eigene Risikoneigung einzustellen – die Gewichtung dieser Risiken zueinander ist rechtlich geprägt. Auch hier fällt ein Irrtum dem Geschäftsleiter im Grundsatz zur Last.

_____ *„Das muss keiner wissen!":* klare Haftung – auch gegenüber Dritten. Erhebliche Sicherheitsvorfälle müssen jetzt und in Zukunft gemeldet werden. Wer dies unterlässt oder nicht ausreichend sicherstellt – gleich ob aus Sorge um die Reputation des eigenen Unternehmens oder aufgrund einer fehlerhaften rechtlichen Einschätzung – riskiert eine persönliche Haftung, auch gegenüber Dritten. Jeder Geschäftsführer ist gut beraten, eher eine Meldung zu viel abzugeben als eine Meldung zu wenig.

Die definitive Erkenntnis: Compliance ja, aber auch nach NIS 2 kein “Heiliger Gral” der Cybersicherheit!



Recht | EU-Regularien

Risikomanagement nach NIS-2:

Auf der Suche nach dem Heiligen Gral der Cybersicherheit?

Eigentlich hat Cybersicherheit mit Indiana Jones erst einmal herzlich wenig zu tun – doch seit einiger Zeit gibt es eine erstaunliche Gemeinsamkeit: Beide begeben sich auf die Suche nach dem Heiligen Gral. Wo Dr. Jones aber am Ende definitiv fündig wurde, steht dies in der Cybersicherheit – zumindest gegenwärtig – noch aus. Worum geht es beim sagenhaften Heiligen Gral der Cybersicherheit – wo und warum wird er gesucht und weshalb konnte man ihn bislang noch nicht finden?

Von Dennis-Kenji Kipker, Bremen

Der Ursprung der Gralssuche zur Cybersicherheit liegt letztlich schon im ersten deutschen IT-Sicherheitsgesetz aus dem Jahr 2015 begründet: Als erste wirklich IT-sicherheitsbezogene Regulierung wurde hier zunächst für die Betreiber von kritischen Infrastrukturen (KRITIS) bestimmt, Cybersicherheit nach dem „Stand der Technik“ zu realisieren.

Die tatbestandliche Weite dieses unbestimmten Rechtsbegriffs, der sich in einer Trias zwischen den „allgemein anerkannten Regeln der Technik“ und dem „Stand von Wissenschaft und Technik“ einordnet, brachte einige

Cybersicherheit nach „Stand der Technik“

Doch genauso wenig wie die technis
lung innehält, hört auch die Cyberbedroh
sich zu verändern. Nicht umsonst hat d
Gesetzgeber zwischenzeitlich – Deutschla
Jahr 2016 eine erste Netz- und Informa
richtlinie (NIS-1) verabschiedet, die n
Oktober dieses Jahres durch ihre N
die zweite Netz- und Informationss
(NIS-2) ersetzt werden soll (vgl. [1,2,

Die Crux daran: Der Anw
NIS-2 wird im Vergleich zu NIS-1
und zwar sowohl in quali

Entscheidend ist somit auch für NIS 2:

Bürgerliches Gesetzbuch (BGB)
§ 276 Verantwortlichkeit des Schuldners

(1) Der Schuldner hat Vorsatz und Fahrlässigkeit zu vertreten, wenn eine strengere oder mildere Haftung weder bestimmt noch aus dem sonstigen Inhalt des Schuldverhältnisses, insbesondere aus der Übernahme einer Garantie oder eines Beschaffungsrisikos, zu entnehmen ist. Die Vorschriften der §§ 827 und 828 finden entsprechende Anwendung.

(2) Fahrlässig handelt, wer die im Verkehr erforderliche Sorgfalt außer Acht lässt.

(3) Die Haftung wegen Vorsatzes kann dem Schuldner nicht im Voraus erlassen werden.

„Wer sich ehrlich um Compliance bemüht, muss keine Sorge vor Bußgeldern haben. Denn auch ein reguliertes ISMS nimmt einzelne Fehler hin und verlangt keine Perfektion – denn das ist ja gerade der betriebsorganisatorische Ansatz des ISMS – auch nach NIS 2.“

Vielen Dank!

Prof. Dr. Dennis-Kenji Kipker

cyberintelligence.institute
Research Director

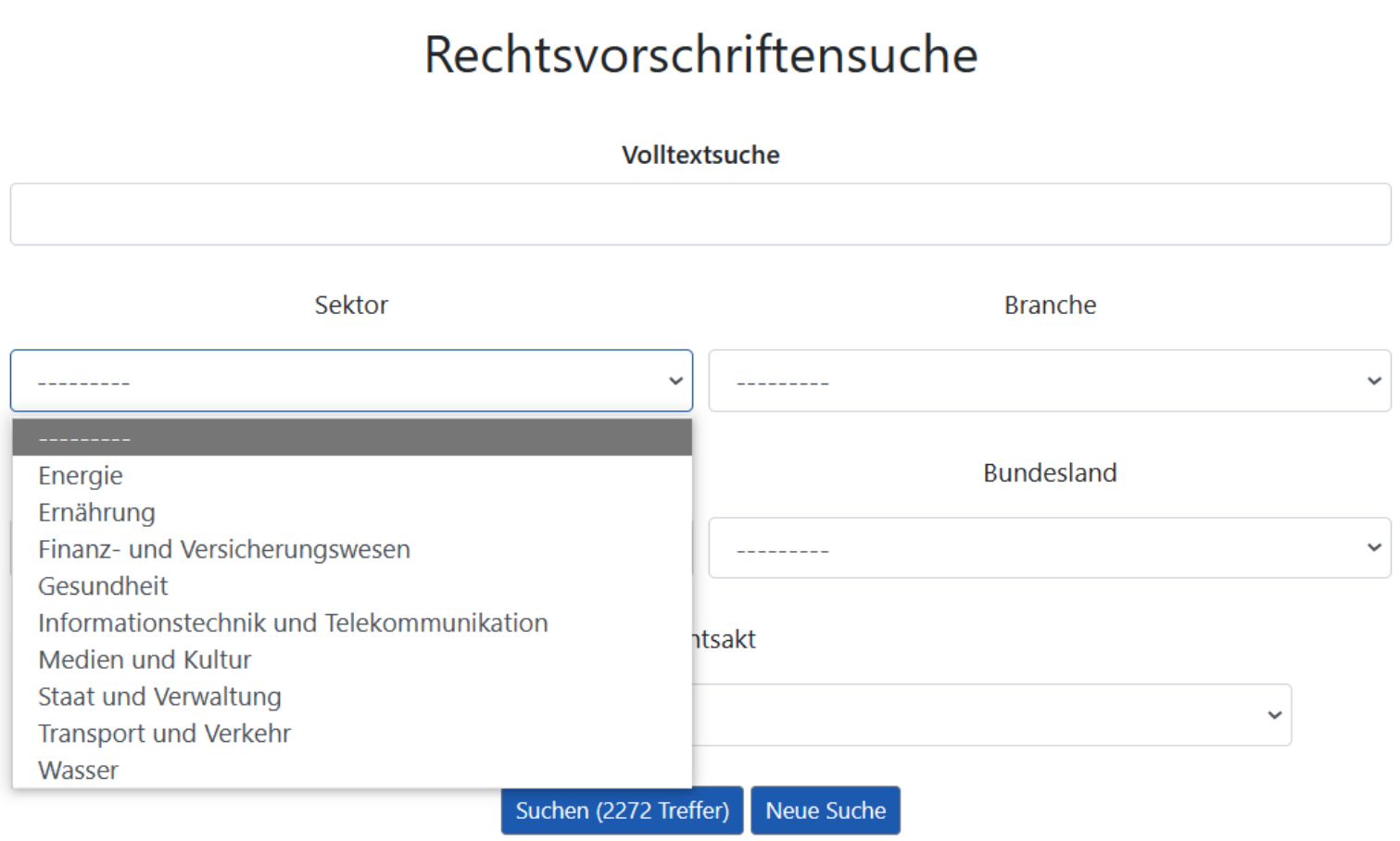
MesseTurm
Friedrich-Ebert-Anlage 49
60308 Frankfurt a.M.
GERMANY

dennis.kipker@cyberintelligence.institute

Cybersecurity Navigator

CYBERSECURITY
NAVIGATOR

https://cybersecurity-navigator.de



Weiterführende Literatur