Cybersicherheit wird zur Chefsache

Dr. Manfred Rack

Rechtsanwalt

RACK
RECHTSANWÄLTE

Inhaltsverzeichnis

Cybersicherheit wird zur Chefsache

1. Das ständig steigende Risiko von Cyberangriffen

Cyberangriffe können erheblichen **Schaden** verursachen. Laut einer Studie des Verbands der deutschen Informations- und Telekommunikationsbranche (bitkom) pendeln sich die jährlichen Schäden bei über **200 Milliarden** ein,[1] was etwa einem Viertel des Bundeshaushalts entspricht. Die Täter kommen öfter aus der organisierten Kriminalität. Drei Viertel der Schäden werden durch Cyberattacken verursacht. Erstmals fühlen sich 52 % der Unternehmen in ihrer Existenz bedroht, durch **Datenklau**, **Spionage** oder **Sabotage**, durch den A**usfall von Informations- und Produktionssystemen** sowie die **Störung von Betriebsabläufen**. Häufige Schäden entstehen durch Phishing, Passwortklau und Malware. Sie sind meist eine unmittelbare Folge von sogenannten **Ransomware-Angriffen**, bei denen Computer und andere Systeme blockiert werden und die Betreiber anschließend erpresst werden Presse und Internet berichten fast täglich über neue Cyberangriffe auf Unternehmen und sonstige Einrichtungen, auf Parlament, Kliniken und sogar auf politische Parteien. Die FAZ berichtet am 11.5.2024 in ihrem Leitartikel „Im digitalen Dauerfeuer“ über die hohe Zahl von 70 neuen Schwachstellen, die täglich erkannt werden.[2] Das Bundeskriminalamt hat am 13. Mai 2024 das Bundeslagebild Cybercrime von 2023 vorgestellt und den Gesamtjahresschaden mit 206 Milliarden angegeben. An Lösegeld für die Daten von Geschädigten wurden 16,1 Milliarden gezahlt. Das BKA weist daraufhin, dass die Dunkelziffer besonders hoch ist, weil viele Angriffe nicht angezeigt werden. Von einem Angriff wurden der Verbund von Krankenhäusern und eine Gruppe von 72 Kommunen blockiert.[3]

2. Die neue Geschäftsleiterverantwortung

Dieses steigende Risiko soll durch die neuen Regelungen der EU und des Bundes zur Cybersicherheit abgewendet werden. Wegen der Bedeutung des Risikos werden vor allem die Geschäftsleiter ausdrücklich verpflichtet. Sie haften in Zukunft persönlich,

[1]Pressemitteilung bitkom, Wirtschaftsschutz 2023, vom 1.9.2023, S. 4,7,9,12,13

[2] FAZ vom 11.5.2024, S.17, Im digitalen Dauerfeuer

[3] FAZ vom 14.5.2024 S. 5, Die Bedrohung durch Cyberangriffe wächst.

wenn sie ihre Pflichten verletzen gemäß § 38 BSIG[4] des Referentenentwurfs vom 7.5.2024 für Schadensersatzforderungen, die aus eigenem Vermögen zu leisten sind.[5] Die Aufmerksamkeit der Geschäftsleiter soll deshalb auf diese neue Rechtslage gelenkt werden.

Art. 17 der NIS-2-RL-E verpflichtet die leitenden Organe wesentlicher und wichtiger Einrichtungen zur Umsetzung der konkreten Sicherheitsanforderung, die in Art. 18 NIS-2-RL-E der Unternehmensführung vorgegeben sind, um einen angemessenen Sicherheitsstandard der von ihnen genutzten Netzwerk- und Informationssystemen zu erreichen.

Nach § 14 KRITIS-DachG (KRITIS-Dachgesetz) des Entwurfs eines Gesetzes zur Umsetzung der Richtlinie EU 2022/2557 und zur Stärkung der Resilienz von Betreibern kritischer Anlagen, sind Geschäftsleiter von Betreibern kritischer Anlagen verpflichtet, die von diesen Betreibern zur Einhaltung von § 10 KRITIS-DachG ergriffenen Maßnahmen zu billigen und zu überwachen. Ausdrücklich geregelt ist die Unwirksamkeit von Vereinbarungen mit den Betreibern, auf solche Ersatzansprüche zu verzichten. Die Geschäftsleiter von Betreibern kritischer Anlagen müssen nach § 14 II KRITIS-DachG regelmäßig an Schulungen teilnehmen, worüber die Aufsichtsbehörden Nachweise verlangen können. Bei der Einschaltung von Hilfspersonen bleiben die Leitungsorgane letztverantwortlich. Die Bedeutung dieser Pflicht wird durch die ausdrückliche Haftungsregelung unterstrichen.

Die gleiche Regelung zur Geschäftsleiterverantwortung findet sich in § 38 BSIG im Referentenentwurf des NIS-2-UmsuCG – NIS2 Umsetzungs- und Cybersicherheitsstärkungsgesetz. Nach § 39 Abs.1 BSIG haben die Betreiber kritischer Anlagen die Erfüllung der Anforderungen nach §§ 30,31 BSIG zum Risikomanagement besonders wichtiger und wichtiger Einrichtungen und zu den besonderen Anforderungen an die Risikomanagementmaßnahmen von Betreibern kritischer Anlagen nachzuweisen.

3. Das Organisationsrisikos der Verantwortungsdiffusion

Der Gesetzgeber hat offensichtlich das allgemeine Risiko der Verantwortungsdiffusion erkannt. Der BGH hat in seinem Schubstreben-Urteil entschieden, dass Pflichten an

[4] Gesetz über das Bundesamt für Sicherheit in der Informationstechnik und über die Sicherheit in der Informationstechnik von Einrichtungen. BSIG, BSI-Gesetz

[5] Plate, NIS2 – und jetzt?, in iX 2024 S. 53

namentlich benannte Mitarbeiter und an ebenfalls mit Namen benannte Vertreter zu delegieren sind.[6] Nach dieser Rechtsprechung schreibt das Gesetz vor, die Verantwortung für die Cybersicherheit eindeutig und nicht weiterdelegierbar an die Geschäftsleiter zu delegieren. Entgegen dieser Anforderung wird in der Unternehmenspraxis nämlich regelmäßig der Wunsch geäußert, die Pflichten mit Funktionen und nicht mit Namen zu verlinken. Dadurch wird die Verantwortung diffus und namenlos. Der BGH verpflichtet deshalb zur Delegation an namentlich benannte Pflichtenträger, weil nur so wirksame Kontrollen möglich sind. Die Verhaltensforschung erklärt diesen Vorbehalt gegen die Namensnennung mit dem Begriff der „Verantwortungsdiffusion“. Erwiesen ist in der Verhaltensforschung, dass die Bereitschaft, gegen Missstände oder Notfälle einzugreifen, höher ist, wenn ein Mitwisser oder Zuschauer allein ist, als wenn er in Gesellschaft anderer die Notsituation erlebt. Wenn mehrere Zeugen eines Missstands sind, ist sich jeder einzelne der Tatsache bewusst, dass andere eingreifen könnten. Der Prozess der Verantwortungsdiffusion wird verstärkt, wenn die Anzahl der Mitwisser zunimmt. So erklärt sich, dass Rechtsverstöße in Unternehmen bekannt sind, aber keiner einschreitet und sich einer auf den andern verlässt. Hinweisgebersysteme und namentliche Delegationen von Pflichten an Einzelpersonen können abhelfen.[7]

Die Verantwortung von Vorständen und Geschäftsführern für die Einhaltung der Legalitätspflicht ist vom BGH in ständiger Rechtsprechung entschieden. Danach kann das Organ einer Gesellschaft die Oberaufsicht über die Einhaltung aller einschlägigen Rechtsvorschriften nicht delegieren und nicht abbedingen.[8] Bei § 14 KRITIS-DachG und § 38 BSIG handelt es sich also um eine kodifizierte Rechtsprechung. Die ausdrückliche Regelung im Gesetz hat offenbar einen besonderen Grund, der sich aus der Stellungnahme und den Erfahrungen des BSI ergibt.

---

6 BGH vom 17.10.1967, NJW 1968,247

7 Jonas/Stroebe/Hewstone, Sozialpsychologie, 5.Aufl., S.302 unter Hinweis auf en Kitty Genovese Fall S. 298

8 RG, 14.12.1911 – VI 75/11, RGZ 78, 107 (Kutscher-Urteil); RG, 12.1.1938 – VI 172/37, RGJW 1938, 1651 (Kleinbahn-Urteil); RG, 25.2.1915 – VI 526/14, RGZ 87 (1916), 1 (Heilsalz-Urteil); BGH, 25.10.1951 – III ZR 95/50, BGHZ 4, 1 (Benzinfahrt-Urteil); BGH, 9.2.1960 – VIII ZR 51/59, BGHZ 32 (1960), 53 (Besitzdiener-Urteil).

Das Bundesamt für Sicherheit in der Informationstechnik – BSI – äußert sich skeptisch zur bisherigen Delegation der Verantwortung für Informationssicherheit.[9] Die Informationssicherheit werde häufig vernachlässigt und falle hinter dem Tagesgeschäft zurück. Durch die unklare Aufteilung von Zuständigkeiten werde die Verantwortung für Informationssicherheit zum „Problem anderer Leute“. Sie werde so lange hin- und hergeschoben, bis keiner sie mehr zu haben glaubt. Weil die Priorisierung der Cybersicherheit oft fehlt, komme es zu Cybervorfällen in Unternehmen.

Dieses Risiko hat das BSI offenbar erkannt und den Gesetzgeber von der Notwendigkeit einer neuen ausdrücklichen gesetzlichen Regelung der Geschäftsleiterverantwortung überzeugt.
Es fehlt bisher an IT-Governance und der klaren Delegation der Pflichten zur Cybersicherheit. Es reicht offenbar nicht aus, sich auf IT-Abteilungen zu verlassen. Cybersicherheit muss deshalb zur Chefsache gemacht werden. Ein Cybervorstand muss mit der Bereitschaft zum Managementsystem für Informationssicherheit – ISMS - eingesetzt werden. Die meisten Hacker kommen über interne Türen in IT-System, indem unbesorgt auf nicht erkannte Phishing-Mails geklickt wird. Auch das bewusste Öffnen digitaler Türen durch illoyale Mitarbeiter kann Hackerangriffe begünstigen.
Dem Cybervorstand ist zu raten, sich am BSI Grundschutzkompendium zu orientieren. Es umfasst Hinweise zur Umsetzung eines Managementsystems für Informationssicherheit. Benannt werden die unterschiedlichen Risiken und die Handlungsempfehlungen zur Abwendung dieser Risiken. Ebenfalls ergeben sich Handlungsempfehlungen aus der ISO-Norm 27001, nach der auch Zertifizierungen möglich sind.

Zum ISMS gehören - ohne Anspruch auf Vollständigkeit - folgende Maßnahmen:

- Erstens gehört zum ISMS ein Überwachungssystem, mit dem Angriffe zu erkennen sind, was von externen Dienstleistern angeboten wird.

- Zweitens zählt zum ISMS ein Notfallplan für den Fall des Cyberangriffs mit Ablaufdiagramm. Für den Ernstfall ist ein Maßnahmenkatalog zu erstellen, aus

[9] Standard 200-2 zur IT Grundschutz-Methodik

dem sich ergibt, wer, was und wann zu tun hat. Pflichten müssen für den Hackerangriffsfall klar delegiert sein. Zunächst ist die Wiederherstellung der IT-Systeme zu sichern. Die Delegation der Pflichten gehört als zweite von sechs Organisationspflichten nach der Rechtsprechung des BGH zum Organisationsverschulden zum unverzichtbaren Teil eines Compliance-Management-System. Zum Notfallplan zählen auch das Sichern der Daten und der schnelle Shut-Down aller Systeme.

- Drittens sind die Behörden und die Betroffenen zu informieren. Diese Meldungen ist die Grundlage für eventuelle Bußgeld- und Schadensersatzrisken.

- Viertens hat der Cybervorstand durch Schulungen und fachliche Unterstützungen Grundkenntnisse und Kompetenz zur Cybersicherheit zu erwerben, was sich aus § 38 BSIG und § 14 KRITIS-DachG ergibt.

- Fünftens ist die Cybersicherheit als Dauerpflicht zu verstehen, die eine ständige Verbesserung und Nachbesserung des Cyberschutzes verlangt. Die Cybersicherheit ist ständig zu aktualisieren und zwar nicht nur zur Rechtslage sondern auch zur technischen Sachlage im Rahmen eines Schwachstellenmanagements. Neue Techniken zum Erkennen von Risiken und zu ihrer Abwehr sind in das ISMS aufzunehmen.[10]

4. Der Cybervorstand mit eigener IT-Kompetenz

Geschäftsleitern fehlt in der Regel die fachliche IT- Kompetenz, Cyberrisiken und die Möglichkeiten der Abwehr einzuschätzen. Der IT- Laie erkennt seine IT-technische Inkompetenz nicht, weil ihm dazu schon die Kompetenz fehlt. Dies hat zur Folge, dass er nicht in der Lage ist, Cyberrisiken und IT-Schwachstellen zur erkennen und zu erfragen. Diesen Zusammenhang erklärt die Verhaltensökonomie und Psychologie mit

[10] Deutscher Anwaltsspiegel, CyberSecurity ist C-Level Aufgabe, Verschärfte Haftung für Leitungsorgane in Unternehmen: Kommt der Cybervorstand, 24. Mai 2023, von Dr. Kristina Schreiber und Dr. Eren Basar.

dem Dunning-Kruger-Effekt.[11] Geschäftsleiter müssen sich dieser Lage bewusst sein, und deshalb routinemäßig sich in allen IT-Sicherheitsfragen beraten lassen. Die sicherste Organisation der Cybersicherheit wäre die Schaffung eines Cybervorstands mit ausgewiesener eigener IT-Kompetenz.[12]

5. Die Billigungs-, Überwachungs- und Schulungspflichten für Geschäftsleiter besonders wichtiger und wichtiger Einrichtungen

Die Risikomaßnahmen, die von den Geschäftsleitern zu billigen und zu überwachen sind, ergeben sich aus § 30 BSIG, mit dem Art.21 der europäischen Cybersicherheits- und Resilienzrichtlinie NIS2 umgesetzt wird.

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,

4. Sicherheit der Lieferkette einschließlich sicherheitsbezogener Aspekte der Beziehungen zwischen den einzelnen Einrichtungen und ihren unmittelbaren Anbietern oder Diensteanbietern,

5. Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von informationstechnischen Systemen, Komponenten und Prozessen, einschließlich Management und Offenlegung von Schwachstellen,

6. Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen im Bereich der Sicherheit in der Informationstechnik,

7. grundlegende Verfahren im Bereich der Cyberhygiene und Schulungen im Bereich der Sicherheit in der Informationstechnik,

8. Konzepte und Verfahren für den Einsatz von Kryptografie und Verschlüsselung,

9. Sicherheit des Personals, Konzepte für die Zugriffskontrolle und für das Management von Anlagen,

10. Verwendung von Lösungen zur Multi-Faktor-Authentifizierung oder kontinuierlichen Authentifizierung, gesicherte Sprach-, Video- und Textkommunikation sowie gegebenenfalls gesicherte Notfallkommunikationssysteme innerhalb der Einrichtung.

---

[11] Rack, Compliance Berater 6/2027 S. 206 Das Rechtsrisiko des Dunning-Kruger-Effekts-eine psychologische Erklärung für Rechtsverstöße wegen unterlassener präventiver Rechtsprüfung.

[12] Siehe Fn. 10

6. Besondere Anforderungen an das Risikomanagement

Von Betreibern kritischer Anlagen nach § 31 BSIG sind Systeme zur Angriffserkennung einzusetzen, Bedrohungen sind zu identifizieren und zu vermeiden sowie Beseitigungsmaßnahmen vorzusehen. Der Stand der Technik ist zu beachten.
Das Risiko ist als eine Beziehung zwischen der Schadensursache und dem Schaden als Wirkung sowie einen Erfahrungssatz zu verstehen, nachdem auf eine Schadensursache mit Wahrscheinlichkeit ein Schaden eintritt, wenn er nicht durch ein Schutzmaßnehme verhindert wird, wobei die Schutzmaßnahme eine Rechtspflicht darstellt, Diese Dreiteilung eines Risikos in erstens die Ursache, zweitens die Wirkung und drittens den Erfahrungssatz, wonach auf eine bestimmte Ursache nach geltenden Erfahrungssätzen mit hoher Wahrscheinlichkeit eine Schaden als Wirkung folgt, ergibt sich vor allem aus der Rechtsprechung des IKB Urteils des BGH.[13]
Auf dem Risikogebiet der Cybersicherheit sind die Schwachstellen der IT im Unternehmen von Betreibern kritischer Anlagen ohne Schutzmaßnahmen als Schadensursachen und die Cyberangriffe mit Vorfällen als Wirkung zu verstehen. Die Erfahrungen über das Verhalten von Hackern beim Ausnutzen von Schwachstellen ohne ausreichendes Schwachstellenmanagement mit effektiven Schutzmaßnahmen begründen die Wahrscheinlichkeit eines Vorfalls nach einem drohenden Angriff.
Der Stand der Technik dient dem Erfassen der jeweils aktuellen Erfahrungen beim Erkennen und Vermeiden von Cyberattacken und deren Folgen.

7. Schwachstellenmanagement als Cyber-Risikovorsorge

Schwachstellen in IT-Systemen ermöglichen das Eindringen von Hackern zur Erpressung, Datenklau, Sabotage, Spionage, Störung der Produktionsabläufe und zum Ausfall von Informationssystemen. Die wichtigste Quelle für Schwachstelleninformationen ist **die National Vulnerability Database (NVD), die vom US National Institute of Standards an Technology (NIST) betrieben wird.** Sie veröffentlicht fortlaufend neue Schwachstellen. Bis 2016 wurden jeden Monat etwa 10 Jahre lang etwa 500 neue Schwachstellen in Softwareprodukten gefunden. Ab 2017 wurden dreimal mehr Schwachstellen gefunden, in den drei Quartalen 2023 waren es mehr neue als in 2014 bis 2016 zusammen. Aktuell liegt die Anzahl neuer

[13] IKB Urteil BGH, 2.2.1996 – V ZR 239/94, BGHZ 132,30, BB 1996, 924 .

Schwachstellen im Durchschnitt beim fünffachen von 2016 also bei 2.500 im Monat. [14] Der Anspruch, sie alle zu beheben, ist unrealistisch. Zu prüfen ist bei dieser Einschätzung die rechtliche Unmöglichkeit einer solchen Pflicht nach § 275 BGB. Der Gesetzgeber hat jedoch die Pflichten der Geschäftsleiter im Gesetz unter den Vorbehalt der Verhältnismäßigkeit gestellt.

Das Gesetz verlangt deshalb in § 30 Abs.1 BSIG v**erhältnismäßige** technische und organisatorische Maßnahmen, um Störungen der Verfügbarkeit, Integrität und Vertraulichkeit der informationstechnischen Systeme, die sie für die Erbringung ihrer Dienste nutzen, zu vermeiden und Auswirkungen von Sicherheitsvorfällen möglichst gering zu halten. In § 10 KRITIS-DachG werden die Betreiber kritischer Anlagen verpflichtet, geeignete **und verhältnismäßige**, technische, sicherheitsbezogene und organisatorische Maßnahmen zur Gewährleistung ihrer Resilienz zu ergreifen. Nach § 31 Abs.2 BSIG soll der erforderliche Aufwand zum Identifizieren von Bedrohungen den geeigneten Beseitigungsmaßnahmen nicht außer Verhältnis zu den Folgen des Ausfalls oder einer Beeinträchtigung der betroffenen kritischen Anlage stehen. Der Umgang mit Schwachstellen besteht darin, Schwachstellen regelmäßig und kontinuierlich zu identifizieren, sie für die Umgebung im Unternehmen zu bewerten, um sie zu priorisieren, d.h. zu entscheiden, was zuerst und vorrangig zu veranlassen ist, mit angemessenen Maßnahmen zu behandeln und um schließlich damit Schäden zu verhindern oder zu verringern. Die drei Kernaufgaben sind das Identifizieren, das Priorisieren und das Behandeln. Die wichtigste Aufgabe ist das Priorisieren.[15] Rechtlich wird damit das Verhältnismäßigkeitsprinzip angewandt. Wenn nicht alle Schwachstellen wegen der großen Zahl verhindert werden können, müssen sie soweit wie möglich behandelt werden. Zur Bewertung von Schwachstellen wird auf den offenen Standard verwiesen, den Common Vulnerability Scoring System (CVSS), der von der US National Infrastructure Advisory Council (NIAC) erstellt und veröffentlicht wird. Aktuell betrieben wird dieser Standard von dem Forum of Incident Response und Security Teams (FIRST). Der CVSS-Score repräsentiert die Relevanz von Schwachstellen und setzt sich aus verschiedenen Eigenschaften der Schwachstelle, aus Metriken, zusammen. Er berechnet sich aus komplexen Formeln und gibt einen

[14] Frank und Casper, iX 12/2023, Schwachstellenmanagement: mehr als Scannen und Finden, Seite 50 mit aufschlussreicher Abbildung 2 zum Stand von 19.10.2023.

[15] Frank und Casper, iX, 12/2023 Schwachstellenmanagement: mehr als Scannen und Finden, S. 50 f. Abbildung 1.

Maßstab darüber ab, wie die Schutzziele der Vertraulichkeit, der Integrität und der Verfügbarkeit betroffen sind. Vor allem kann er eine Entscheidungshilfe den verantwortlichen Geschäftsleitern bieten, welche der vielen Schwachstellen vorrangig zu behandeln sind. [16] Zu berücksichtigen sind außerdem, der Schutzbedarf der bedrohten Systeme, die Verfügbarkeit von Patchs als Gegenmaßnahmen, die Wahrscheinlichkeit der Ausnutzung der Schwachstelle, die das Exploit Prediction Scoring System (EPSS) von FIRST bietet, der für alle veröffentlichten Schwachstellen tagesaktuell und kostenfrei zur Verfügung gestellt wird.[17] Die Schutzbedürftigkeit kann vom jeweiligen Unternehmen abhängen. Forschungsergebnisse, Medizindaten oder Produktionsdaten können unterschiedlich bewertet werden. Dringend zu empfehlen ist die Dokumentation des Schwachstellenmanagements, um die Beweise für die Entlastung des Geschäftsleiters zu sichern, da dieser die Beweislast für die Erfüllung seiner Pflichten nach § 38 i.V.m.§ 30 BSIG trägt. Die Beweislastumkehr ergibt sich aus den BGH Rspr. zum Organisationsverschulden.

Eine Marktübersicht zu Anbietern von Werkzeugen für die Behandlung von Schwachstellen bietet der zitierte Aufsatz.[18]

8. Die Organisation der Cybersicherheit mit dem Compliance-Management-System RECHT IM BETRIEB

Wie jedes Risiko eines Rechtsverstoßes ist auch das Risiko des Verstoßes gegen Rechtsvorschriften zu Vermeidung und Verringerung des Cyberrisikos zu organisieren, was mit dem CMS RECHT IM BETRIEB zu leisten ist. Zu unterscheiden sind die sechs Organisationspflichten und die zu organisierenden Pflichten zur Abwehr von Cyber- und IT-Risiken.

Die sechs Organisationspflichten ergeben sich aus der nach DIN ISO 373001 und aus der einschlägigen Rspr. des BGH zum Organisationsverschulden. Die zu organisierenden Rechtspflichten ergeben sich aus den Entwürfen zum KRITIS-DachG und dem NIS-2-UmsuCG. In RECHT IM BETRIEB sind die einzuhaltenden

[16] Frank und Casper, iX, 12/2923 Schwachstellenmanagement: mehr als Scannen und Finden, S. 50 f. Abbildung 4.

[17] Frank und Casper, iX, 12/2023 Schwachstellenmanagement: mehr als Scannen und Finden, S. 50 f. Abbildung4.

[18] Frank und Casper, iX,12/2023, Werkzeuge für das Schwachstellenmanagement, s.58 f

Rechtspflichten ermittelt und markiert und sind an Mitarbeiter zu delegieren, zu aktualisieren, einzuhalten, auf ihre Einhaltung zu kontrollieren und zur Beweissicherung und zum Nachweis gegenüber Aufsichtsbehörden zu dokumentieren. Im Folgenden werden die Rechtsgrundlagen benannt.

- Erstens sind die Risikosachverhalte und die Rechtspflichten zur präventiven Abwehr der Risiken zu **ermitteln**[19] **und zu identifizieren.** Die Organisationspflicht zur Ermittlung von Cyberrisiken und von Schutzmaßnahmen ergeben sich aus §§ 30 Abs.1,2 und 31 Abs.2 BSIG. Umgesetzt wird Art.21 der NIS2 Richtlinie. Die Ermittlung, Analyse und Bewertung der Risiken der Betreiber kritischer Anlagen ist in § 9 KRITIS-DachG und die Ermittlung der Pflichten zur Risikoabwehr ist in § 10 KRITIS-DachG geregelt.

- Zweitens sind die einschlägigen Rechtspflichten zu **delegieren**.[20] In 21 Einzelentscheidungen haben RG und BGH die Pflicht zu Delegation konkretisiert. Neu gesetzlich und erstmalig geregelt ist die Geschäftsleiterverantwortung nahezu wortgleich in § 38 BSIG sowie in § 14 KRITIS-DachG. Die Verantwortung der Cyber- und IT-Sicherheit wird an den jeweiligen Geschäftsleiter, an das Organ des Unternehmens delegiert.

- Drittens sind die Pflichten zu **aktualisieren.** [21] Vor allem sind auch die Verkehrssicherungspflichten zu aktualisieren, was sich aus dem Kupolofen Urteil des BGH ergibt. Der Gesetzgeber und die Verwaltung können nicht sämtliche Schadensrisiken eines Unternehmens erfassen. Deshalb sind Unternehmen zur Selbstregulierung in Form von Verkehrssicherungspflichten dazu verpflichtet, Risiken zu ermitteln und im Unternehmen abzuwenden. [22] Diese Rechtslage gilt ganz besonders für die Cybersicherheit und die IT-Sicherheit für Betreiber kritischer Anlagen, da sich die Schwachstellen und

[19] Rack, Compliance Berater, 5/2013, S. 191, Die Organisationspflicht nach der höchstrichterlichen Rechtsprechung mit Einzelnachweisen zur Risikoanalyse;

[20] Rack, Compliance Berater, 6/2013, S.231, Die Organisationspflicht zur Delegation;

[21] Rack, Compliance Berater 7/2013, Die Aktualisierung von Unternehmenspflichten, S. 275

[22] Kupolofen Urteil BGHZ 92, S. 143

damit die Risikolage täglich ändern kann und die Schutzmaßnahmen im gleich schnellen Rhythmus wie die Verkehrssicherungspflichten aktualisiert werden müssen. Die gleiche Aktualisierungspflicht zur Anpassung an den technischen Fortschritt ergibt sich aus dem Hühnerpest Urteil des BGH .[23]

- Viertens sind die Pflichten zu erfüllen[24]. Gesetzlich geregelt ist die Erfüllung in § 39 BSIG sowie in §§ 10 und 11 KRITIS-DachG.

- Fünftens ist die Einhaltung der Pflichten zu kontrollieren. Gesetzlich geregelt ist die Kontrollpflicht in § 14 Abs.1 KRITIS-DachG und § 38 Abs.1 BSIG.

- Sechstens ist die Einhaltung der Rechtspflichten eines Unternehmens zu dokumentieren.[25] Gesetzlich geregelt ist die Pflicht zur Dokumentation in § 39 BSIG. Vor allem lässt sich der Nachweis von den Geschäftsleitern mit der **Organoberaufsichtsmaske** führen. Ob und welche Rechtspflichten ermittelt, delegiert, eingehalten, kontrolliert und schließlich zur Beweissicherung auch dokumentiert sind, erschließt sich für die Geschäftsleiter und allen Dritten auf einen Blick. Mit der Oberaufsichtsmaske wird im Compliance-Management-System RECHT IM BETRIEB dokumentiert, dass der jeweilige Geschäftsleiter seine Pflicht nach § 14 KRITIS-DachG und nach § 38 BSIG eingehalten hat, die Umsetzung der Schutzmaßnahmen zu überwachen. Das Bundesamt kann nach § 39 BSIG und die Aufsichtsbehörden nach § 14 Abs.2 und § 11 Abs.1 und Abs. 5 KRITIS-DachG geeignete Nachweise verlangen. Die Oberaufsichtsmaske eignet sich als Nachweis über die Einhaltung aller Rechtspflichten zur IT- und Cybersicherheit.

[23] BGH, 26.11.1989 – VI ZR 212/66; BGHZ 51, 91 – Hühnerpestentscheidung.

[24] Rack, Compliance Berater 8/2014 S. 110,115, Die rechtlichen Voraussetzungen eines Compliance-Management-Systems, mit Einzelnachweisen aus Urteilen zu jeder Organisationspflicht.

[25] Rack, Compliance Berater, 8/2024, S.288;

9. Die weiterentwickelte IT-Sicherheits- Regelung in zwei Richtlinien nach EU-Recht

Der Schutz der IT-Sicherheit Kritischer Infrastrukturen ist bisher im Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSIG) vom 14.8.2009 geregelt.
Seit 16.Januar 2023 sind zwei Richtlinien der EU in Kraft, die Cybersicherheits- und Resilienzrichtlinien **NIS2** (Network an Information Security) und **CER** (Critical Entities Resilience Directive).
Die CER regelt den physischen Schutz vor Sabotagen und Angriffen. Die NIS2 regelt die Sicherheit der Informations- und Kommunikationstechnik.
Beide Richtlinien sollen sicherstellen, dass die Bevölkerung der EU mit lebenswichtigen Gütern und Diensten von den als kritisch eingestuften Einrichtungen versorgt werden können.

10. Der erweiterte Anwendungsbereich der Richtlinien

Anzuwenden sind die Richtlinien auf **achtzehn Industriesektoren** mit Vorgaben an das Risikomanagement und die Cyber-sicherheit. Mit der Richtlinie 2022/2557 wurde ein einheitlicher europäischer Rechtsrahmen für die Stärkung der Resilienz kritischer Einrichtungen in mindestens elf Sektoren gegen Gefahren auch außerhalb des Schutzes der IT-Sicherheit im Binnenmarkt geschaffen .[26] Die Richtlinie schafft einen übergreifenden Rahmen, der als „DACH“ illustriert wird, einen All-Gefahren-Ansatz verfolgt, und damit auch Naturkatastrophen oder vom Menschen verursachte, unbeabsichtigt oder sogar vorsätzliche Gefährdungen berücksichtigt. Zur Abgrenzung von der IT-Sicherheit wird das Ziel als „physischer Schutz“ bezeichnet. Mit dem KRITIS-DachG werden erstmals eigenständige sektorenübergreifende abstrakte Regelungen getroffen. Das KRITIS-DachG soll einen Prozess aufsetzen, der nationale und betreiberseitige Risikobewertungen in allen Sektoren, das Erstellen von Resilienzplänen durch die Betreiber, und branchenspezifische Schutzstandards fördert. [27]
Nach **Schätzungen des statistischen Bundesamtes werden zehnmal** mehr Unternehmen als bisher gesetzlich zur Einhaltung der Rechtsvorschriften aus den

[26] Referentenentwurf vom 21.12.2023, S. 1
[27] Referentenentwurf vom 21.12.2023, S. 1 und 2 unter Problem und Ziel.

Richtlinien verpflichtet sein.[28] Bisher sind beim BSI 800 Betreiber kritischer Infrastrukturen registriert. Dazu kommen noch etwa zwei- bis dreitausend Unternehmen im besonderen öffentlichen Interesse aus dem Chemie- und Rüstungssektor. Nach der Umsetzung von NIS2 und CER in Deutschland betrifft die Regulierung rund 30 000 Einrichtungen. Doppelt so viele Sektoren als bisher werden als kritisch eingestuft. Die Klassifizierung als kritische Einrichtung richtet sich gemäß der Neuregelung nach Unternehmensgröße und Umsatz. Erstens müssen Unternehmen zu den achtzehn Sektoren und zweitens mehr als 50 Mitarbeiter oder 10 Millionen Euro Jahresumsatz haben, um als “wichtige Einrichtungen“ zu gelten. „Besonders wichtige Einrichtungen – essential entities“ gelten Unternehmen mit mehr als 250 Mitarbeitern oder 50 Millionen Euro Jahresumsatz. Die besonders wichtigen Einrichtungen sind zum aktiven Nachweis des Einhaltens der vorgegebenen Regeln verpflichtet. Dies gilt schon bisher für die KRITIS Betreiber.[29] Bisher wurden Unternehmen als kritisch danach eingestuft, ob sie mit dem Ausfall ihrer Leistung 500.000 zu versorgende Personen betreffen.

Die im Folgenden aufgelisteten achtzehn Sektoren zählen zu dem Anwendungsbereich der Richtlinien CER und NIS2, da aus diesen Wirtschaftsbranchen die EU-Bürger mit lebenswichtigen und existentiellen Gütern und Dienstleistungen versorgt werden.

(1) Energie
(2) Finanzmarktinfrastruktur
(3) Trinkwasser
(4) Digitale Infrastruktur
(5) Forschung
(6) Banken
(7) Weltraum
(8) Verwaltung
(9) Abfall
(10) Anbieter digitaler Dienste
(11) Gesundheit
(12) Transport
(13) Ernährung
(14) Post
(15) Abwasser
(16) Verwaltung von IKT-Diensten
(17) Gefährliche Chemikalien
(18) Industrie

[28] Plate, NIS2 – und jetzt?, in iX 2024 S. 53

[29] Plate, NIS2 – und jetzt? in iX 2024 S. 53

11. Die Begründung der neuen Regelungen für kritische Anlagen

In der Begründung des Referentenentwurfs wird die bisherige Rechtslage vor und nach dem Entwurf beschrieben. Grundsätzlich sind in einer Marktwirtschaft die Betreiber kritischer Anlagen aus eigenem Interesse an der Funktionsfähigkeit ihrer Anlagen interessiert. Kommt es allerdings zu Störungen der Versorgung mit Strom, Wasser, Lebensmitteln, kann es zu Kettenreaktionen und Kaskadeneffekte über die gesamte Wertschöpfungskette kommen. Nachteile drohen nicht nur dem einzelnen Versorgungsunternehmen, sondern allen Unternehmen, die von den kritischen Dienstleistungen wie Wasser, Strom, Verkehr, Lebensmitteln abhängig sind, und zwar europaweit.[30] Bisherige Regelungen sind sektorenspezifisch. Sektorenübergreifend und bundeseinheitlich sind dagegen die folgenden neuen Regelungen nach dem KRITIS-DachG zur allgemeinen Verbesserung der Resilienz

- Gleiche Resilienz Maßnahmen,
- Zur Identifizierung kritischen Anlagen,
- Zu gleichen Maßnahmen und Mindeststandards zur Resilienz,
- Zur Aufrechterhaltung des Betriebs kritischer Anlagen,
- Zur zügigen Wiederherstellung gestörter und ausgefallener Anlagen,
- Zu einheitlichen Analyse und Bewertung gleiche Risiken,
- Zu einem gleichen Störungsmonitoring,
- Zum fortlaufenden Überblick über gleiche Risiken,
- Zum Austausch von Erfahrungen über gleiche Risiken und gleiche Indizien, die Rückschlüsse auf drohende Risiken zulassen,
- Durch vereinheitlichte Begriffsbestimmungen,
- Durch Mindestvorgaben für Resilienz Maßnahmen,
- Durch die Einführung eines Meldewesens für Sicherheitsvorfälle,
- Durch Berichtspflichten gegenüber der EU Kommission.

Der Anspruch auf die Sicherung störungsfreier Versorgung mit lebenswichtigen Leistungen und der Anspruch auf die Resilienz der Daseinsvorsorge lässt sich aus

[30] Begründung Referentenentwurf S.30

dem Sozialstaatsprinzip herleiten und umfasst auch die Infrastruktur, auf die jeder angewiesen ist. Das Sozialstaatsprinzip ist als Staatszielbestimmung in Art. 20 I GG und Art. 28 I S.1 GG. begründet. Subjektive Rechte und Ansprüche lassen sich jedoch nicht herleiten. [31] Die rechtspolitische Akzeptanz der verpflichtenden Regelungen zur Stärkung der Resilienz der Daseinsvorsorge in Form der Cybersicherheit ergibt sich aus der Bedrohungslage durch die Cyberangriffe und der unternehmensinternen Einsicht, dass dringende Investitionen leichter zu entscheiden und durchzusetzen sind, wenn eine gesetzliche Pflicht dazu besteht. Das Gesetz liefert den IT-Abteilungen die Argumente für das Aufstocken ihrer Budgets.[32] Hinzu kommt die neu geregelte Geschäftsleiterverantwortung, für die Vorstände und Geschäftsführer persönlich haften, die sie nicht an Angestellte unterhalb der Organebene delegieren und ausdrücklich auch nicht abbedingen können. Beim Genehmigen von finanziellen und personellen Mitteln für die Cybersicherheit im Unternehmen schützen sich in Zukunft die Geschäftsleiter selbst persönlich. Die neue Geschäftsleiterverantwortung für Cybersicherheit begründet Motive zu erhöhter Aufmerksamkeit und Investitionsbereitschaft.

Die Daseinsvorsorge ist zwar grundsätzlich die Aufgabe der öffentlichen Hand. Nachdem jedoch Krankenhäuser, Wasser-, Energieanbieter und Telekommunikationsnetzbetreiber zunehmend privatisiert wurden, erscheint es als konsequent, auch private Versorgungunternehmen zur Resilienz der von ihnen angebotenen Daseinsvorsorge in Form der Sicherheit vor Cyberangriffen zu verpflichten.

12. Die Ziele und Maßnahmen zur Resilienz nach § 10 KRITIS-DachG und Art.21 NIS-2

Die Anforderungen der NIS2 Richtlinie ist in Art.21 geregelt und enthält zehn Risikomanagementmaßnahmen zur Cybersicherheit. Sie sind abstrakt formuliert und als Grundvoraussetzungen von allen Einrichtungen einzuhalten. In deutsches Recht übernimmt das KRITIS-Dachgesetz die Vorgaben in § 10. Die Vorschrift nennt in § 10 Abs.1 Nr. 1 bis 6 die Ziele und dazu in Abs.3 Nr.1 bis 6 die Schutzmaßnahmen.

[31] Sachs, Michael, in: Sachs, Grundgesetz Kommentar, 8. Auflage 2018, Art. 20, Rn. 47 ff. Karl-Peter, in: von Mangoldt/Klein/Starck, Kommentar zum Grundgesetz, Band II, 7. Auflage 2018, Art. 20 Rn. 103

[32] Plate, NIS2 – und jetzt?, in iX 2024 S. 53

Konkret regelt die Vorschrift in Abs.3

- Nr. 1 das Verhindern der Vorfälle durch Notfallvorsorge
- Nr. 2 den physischen Schutz durch Zäune, Umgebungsüberwachung, Detektionsgeräte,
- Nr. 3 die Reaktion auf Vorfälle, durch Alarmfallpläne, Krisenmanagement,
- Nr. 4 die Wiederherstellung des Betriebs durch Notstromversorgung und Ermittlung alternativer Lieferketten zur Wiederaufnahme des Dienstes,
- Nr. 5 das Personal- und Sicherheitsmanagement,
- Nr.6 das Informieren, Schulen und Üben.

13. Stand des Gesetzgebungsverfahrens zur Umsetzung in deutsches Recht

Die neue **NIS-2-Richtlinie** vom 16.1.2023 EU 2022/2557 ist nunmehr in deutsches Recht umzusetzen, gemäß Art. 26 I bis zum 17.Oktober 2024.

Ein offizieller Entwurf mit dem Titel (NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz- BSIG) **liegt seit dem 7.5.2024 vor.** .[33]

Der zweite Referentenentwurf ist unter den Ressorts schon abgestimmt. Die Länder und Verbände sind angehört. Das KRITIS-Dachgesetz normiert erstmals und einheitlich bundesgesetzliche sektorenübergreifende Mindeststandards. Das KRITIS-Dachgesetz wird neben dem BSIG und dem BSIG gelten. Eine größtmögliche Kohärenz wird angestrebt. Ziel und Zweck ist die Stärkung der Resilienz von Betreibern kritischer Anlagen durch physische Maßnahmen.

FAZIT

Besonders Geschäftsleitern und ganz speziell den Geschäftsleitern kritischer Anlagen, wie allen Versorgern von Energie, Wasser und sonstigen Leistungen der Daseinsvorsorge, ist zu empfehlen, sich mit der neuen Rechtslage zur Abwendung von Cyber- und IT-Risiken durch die hochaktuellen Referentenentwürfe zum BSIG mit dem neuen BSI-Gesetz- sowie dem KRITIS-DachG vertraut zu machen. Der Anwendungsbereich der kritischen Infrastruktur ist auf etwa 30 000 Unternehmen ausgeweitet. Den Geschäftsleitern ist die Verantwortung und die persönliche Haftung

[33] Das KRITIS – DachG ist als Art.1 des BSIG geregelt. Art. 2 ist die Änderung, Art. 3 die Regelung zum Inkrafttreten am 18.10.2024.

erstmalig und neu gesetzlich ausdrücklich übertragen worden, die sie nicht delegieren oder abbedingen können. Die fehlende IT-Kompetenz sollen sie sich durch Schulungen aneignen und nachweisen. Das Schwachstellen Management ist wegen einer täglich neuen Risikolage eine erhebliche Herausforderung für die Organisation eines Unternehmens kritischer Infrastruktur. Monatlich werden aktuell 2500 neue Schwachstellen erfasst. Schließlich drohen existentielle Schäden durch die unberechenbaren Angriffe mit Vorfällen und nicht kalkulierbaren Schadensfolgen. Das Compliance-Management-System RECHT IM BETRIEB bietet die Einhaltung aller sechs Organisationspflichten und vor allem die Nachweismöglichkeiten. Geschäftsleiter vermeiden damit präventiv den eventuellen Vorwurf des Verschuldens bei der Organisation der Rechtspflichten zum Schutz vor IT- und Cyberrisiken, sollte es nämlich trotz aller Compliance Bemühungen zu einem Rechtsverstoß kommen.

RACK
RECHTSANWÄLTE

ALLES AUS EINER HAND

Rechtsinhalte, Software & präventive Rechtsberatung

Nutzen Sie unsere gespeicherten Erfahrungen aus 28 Jahren Complianceberatung. Wir vermeiden die Haftung für Organisationsverschulden von Führungskräften. Sie müssen organisatorisch dafür sorgen, dass sie sich selbst und dass sich alle Mitarbeiter des Unternehmens legal verhalten. Dazu lassen sich alle Risiken und Pflichten eines Unternehmens mit unserem System ermitteln, delegieren, monatlich aktualisieren, erfüllen, kontrollieren, digital speichern und für alle jederzeit verfügbar halten. Die Verantwortlichen können digital abfragen, wer, welche Pflicht, an welchem Betriebsteil, wie zu erfüllen hat. Führungskräfte können auf einer Oberaufsichtsmaske mit einem Blick kontrollieren, ob alle Pflichten im Unternehmen erfüllt sind. Systematisch senken wirden Complianceaufwand durch Standardisierung um 60 %. Sachverhalte im Unternehmen wiederholen sich, verursachen gleiche Risiken und lösen gleiche Rechtspflichten zur Risikoabwehr aus. Rechtspflichten werden nur einmal geprüft, verlinkt, gespeichert und immer wieder mehrfach genutzt.

Wir sind Rechtsanwälte mit eigenen Informatikern und bieten eine Softwarelösung mit Inhalten und präventiver Rechtsberatung aus einer Hand. Auf Anregungen aus den Unternehmen passen unsere EDV-Spezialisten die Software unseres Compliance-Management-Systems an. Der aktuelle Inhalt unserer Datenbank: 21.519 Rechtsvorschriften von EU, Bund, Ländern und Berufsgenossenschaften, 8.772 Gerichtsurteile, standardisierte Pflichtenkataloge für 45 Branchen und 73.000 vorformulierte Betriebspflichten. 57.000 Unternehmensrisiken sind mit 72.000 Rechtspflichten 4,5 Millionen Mal verlinkt und gespeichert. Auf die Inhalte kommt es an. Je umfangreicher die Datenbank umso geringer ist das Risiko, eine Unternehmenspflicht zu übersehen.

Weitere Informationen unter:
www.rack-rechtsanwälte.de