DIE ORGANISATION DER IT-SICHERHEIT IN UNTERNEHMEN

Dr. Manfred Rack
Rechtsanwalt

Inhaltsverzeichnis

DIE ORGANISATION DER IT-SICHERHEIT IN UNTERNEHMEN

Die Funktionsfähigkeit von IT-Systemen wird immer wichtiger für Unternehmen und die Versorgung der Bevölkerung durch staatliche und kommunale Einrichtungen. Hackerangriffe machen das Risiko für die IT-Sicherheit deutlich. Bedroht sind vor allem die Einrichtungen der kritischen Infrastruktur, durch die die Allgemeinheit mit Energie, Wasser, Lebensmittel, medizinischer Versorgung, Transport- und Verkehrsleistungen versorgt wird. Mit dem IT-Sicherheitsrecht soll die Verfügbarkeit, die Unversehrtheit und die Vertraulichkeit von Informationen gesichert werden. Risiken ergeben sich vor allem aus der steigenden Cyberkriminalität. Die IT-Sicherheit muss organisiert werden. Die sechs Organisationspflichten eines Compliance-Management-Systems sind auch zum Schutz der IT-Sicherheit einzuhalten. Dazu müssen die Risiken für IT-Sicherheit erkannt, die Rechtspflichten zur Risikoabwehr ermittelt, auf Pflichtenträger delegiert, regelmäßig aktualisiert, erfüllt, kontrolliert und dokumentiert werden. Die IT-Sicherheit ist Teil eines Compliance-Management-Systems. Zu vermeiden ist der Vorwurf, durch Organisationsverschulden des Vorstands sei die IT-Sicherheit gefährdet worden.

(1) Das steigende Risiko der Cyberkriminalität

Die Presse berichtet regelmäßig über Angriffe auf die IT-Sicherheit von Supermärkten, Öl-Pipelinebetreibern, Kliniken und Stromversorgern. Das stetig steigende Risiko der Cyberkriminalität weist das Bundeskriminalamt in seinem Bundeslagebild *„Cybercrime 2020“* nach. Die wichtigsten Cyberangriffe in Deutschland im Jahr 2020 finden sich in einer zeitlichen Auflistung.[1] Angegriffen und mit Schadsoftware kompromittiert wurden Unternehmen von Automobilzulieferern, Pharmakonzernen, von kommunalen Versorgungsunternehmen, Forschungszentren, von Halbleiterherstellern, Universitätskliniken und börsennotierten Unternehmen der Lebensmittel- und Kosmetikbranche.

Nach dem Bundeslagebild 2020 steigt die Anzahl der Cyberstraftaten. Die Angriffe konzentrieren sich auf lukrative Opfer. Die Täter agieren global und professionell. Eine kriminelle Parallelwirtschaft wächst im Untergrund.[2] Im Kampf gegen die Cyberkriminalität meldet die Polizei inzwischen Erfolge. Betreiber des DarkMarket wurden festgenommen. Cybercrime im engeren Sinne richtet sich gegen das Internet und informationstechnische Systeme. Tatmittel ist das Internet, das mit forschreitender Digitalisierung an Bedeutung gewinnt. Die registrierten Straftaten im Cybercrimebereich betragen 82.649 im Jahr 2016, 108.474 Delikte im Jahr 2020 mit einer Steigerung von 7,9 % im Vergleich zum Vorjahr 2019. Davon aufgeklärt werden 31.000 bis circa 35.000. Die Aufklärungsquote stagniert. Die Ursachen der steigenden Cyberkriminalität werden in der zunehmenden Digitalisierung aller Lebensbereiche, der Professionalisierung der Täter, der wachsenden Fähigkeit der Schadsoftware sowie der zunehmenden Verschleierung von Sicherheitsmechanismen gesehen. Beschrieben werden im Bundeslagebild Cyberstraftaten als Dienstleistung einer arbeitsteilig

1 Bundeslagebild 2020, S. 5 u. 6.

2 Bundeslagebild Cybercrime 2020, S. 3.

organisierten Untergrundwirtschaft mit Preislisten.[3] Die Presse berichtet über Schwarz- und Graumärkte für digitale Angriffs- und Einbruchswerkzeuge und cybercrimetypische Schadprogramme (Malware). Das Geschäft mit den IT-Lücken ist enorm gewachsen. Unternehmen bieten Sicherheitsforschern Belohnung, wenn sie neu entdeckte Schwachstellen in ihren Produkten direkt an sie melden.[4] Berichtet wird über den Doppelkurs der Bundesregierung und des Bundesamtes für Sicherheit in der Informationstechnik. Die Behörden beschaffen die digitalen Einbruchswerkzeuge, um selbst Schwachstellen erkennen und schließen zu können.[5] Die Fallbeispiele für Schadsoftware sind auch für alle aufschlussreich, die als potenzielle Opfer sich vor Angriffen schützen müssen. Die Angriffe lassen Muster von der Programmierung über die Erpressung bis zum Lösegeldeingang erkennen.

(2) Cyberkriminalität gegen Unternehmen

Verdeutlicht wird die Bedrohungslage durch Cyberkriminalität in der Untersuchung *„Cyberangriffe gegen Unternehmen in Deutschland, Ergebnisse einer repräsentativen Unternehmensbefragung 2018/2019"*.[6] In der Studie werden IT-Sicherheitsstrukturen in Unternehmen erfasst[7], Einschätzungen zu IT-Risiken werden beschrieben[8], Cyberangriffe gegen die IT-Systeme von Unternehmen werden nach Angriffsart, nach Androhung einschließlich der Risikoeinschätzung analysiert. Die schwerwiegendsten Angriffe werden aufgezählt. Mögliche Schutzfaktoren, organisatorische Maßnahmen und die technischen Schutzmaßnahmen werden behandelt.[9] Im Bundeslagebild werden neun aktive Schadsoftware-Familien mit Fallbeispielen benannt.[10] Die Studie kann als Fundgrube für Angriffsbeispiele genutzt werden, auf deren Abwehr sich jedes Unternehmen einrichten muss.

Cyberkriminelle greifen dort an, wo es sich finanziell lohnt, insbesondere bei wirtschaftlich starken Unternehmen und bei Unternehmen der kritischen Infrastruktur in öffentlicher Einrichtungen. Die Täter nutzen die Notwendigkeit von Unternehmen aus, den reibungslosen Betrieb der öffentlicher Einrichtung zur Daseinsvorsorge gewährleisten zu müssen. Unternehmen der kritischen Infrastruktur bieten für die Gesellschaft besonders lebenswichtige Dienstleistungen an, auf die deren Kunden angewiesen sind und jeder Ausfall eine gesellschaftliche Notlage verursachen kann[11]. Als Fazit wird im Bundeslagebild 2020 festgestellt, dass Kriminalität sich zunehmend in den digitalen Raum verlagert. Das Internet wird als Tatmittel genutzt (Cybercrime im weiteren Sinne) und ist im Vergleich zum Vorjahr 2019 um 8,7 % gestiegen. Die Professionalität der Täter steigt und verschärft die Bedrohungslage. Die zunehmende Digitalisierung in allen Lebensbereichen vermehrt die Tatgelegenheiten. Das Phänomen des *„Cybercrime-as-a-Service"* erleichtert die Straftaten. Die kriminellen Hilfsmittel werden durch die digitalisierte Untergrundwirtschaft leichter zugänglich. Neue Schadsoftware für komplexe Angriffe werden durch die erbeuteten Lösegelder finanziert. Mangelnde Sicherheitsvorkehrungen in Unternehmen vergrößern das Risiko. Die Abhängigkeit der kritischen Infrastrukturen, der öffentlichen Verwaltung und der deutschen Unternehmen hängen immer mehr von funktionierenden IT-Einrichtungen ab.[12] 46 % aller befragten Unternehmen gaben an, schon einmal Opfer eines Cyberangriffs geworden zu sein.

3 Bundeslagebild Cybercrime 2020, S. 13.

4 Der Spiegel Nr. 27, vom 3.7.2021, S.43.

5 Der Spiegel Nr. 27, vom 3.7.2021, S.43.

6 Arne Dreißigacker, Benett von Skarczinski, Gina Rosa Wollinger, gefördert durch das Bundesministerium für Wirtschaft und Energie.

7 Cyberangriffe gegen Unternehmen in Deutschland, S. 69.

8 Cyberangriffe gegen Unternehmen in Deutschland, S. 89; Kipker/Wiegand, Cybersecurity

9 Cyberangriffe gegen Unternehmen in Deutschland, S. 155.

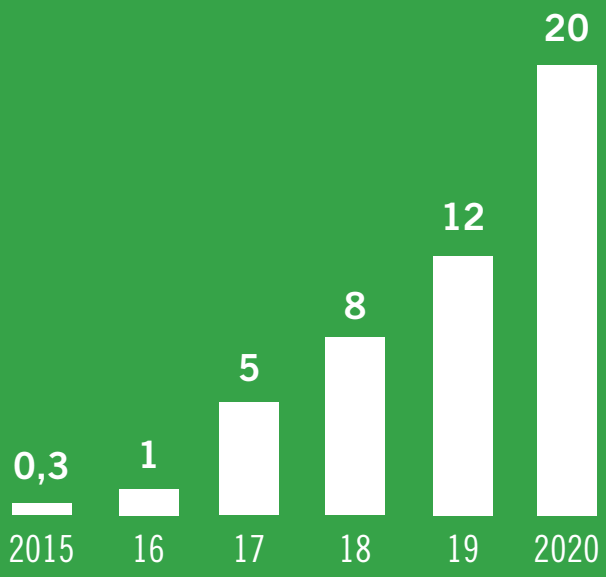
10 Bundeslagebild Cybercrime 2020, S. 25-26.

11 Bundeslagebild Cybercrime 2020, S. 29.

12 Bundeslagebild Cybercrime 2020, S. 38.

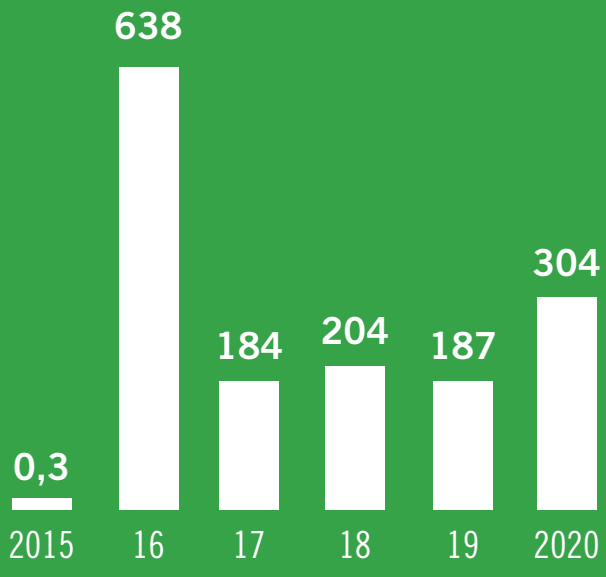
GLOBALER SCHADEN DURCH RANSOMWARE

in Milliarden Dollar



ZAHL DER ATTACKEN

Weltweit in Millionen



Quellen: Cyberreason; Statistik; Microsoft/Cybercrime Magazin/

alle 11 Sekunden
erfolgt global eine Ransomware-Attacke.

81 Prozent
aller Unternehmen sind besorgt über Ransomware-Attacken.

73 Prozent
der Unternehmen haben Abwehrpläne.

42 Prozent
sind überzeugt, Spezialisten zur rechten Zeit am rechten Ort zu haben.

178 000 Dollar
ist die Höhe der durchschnittlichen Lösegeldforderung.

80 Prozent
der Unternehmen, die Lösegeld zahlten, wurden von einer weiteren Attacke getroffen.

(3) Mit wachsendem Cybercrime-Risiko steigt der Bedarf an Schutzmaßnahmen

IT-Risiken sind präventiv durch Rechtspflichten abzuwenden. Rechtspflichten mit dem Zweck, IT-Systeme zu schützen, ergeben sich erstens aus gesetzlichen Regelungen und zweitens aus einer Vielzahl technisch geprägter Vorgaben, Standards, Sicherheitskonzepten und Leitlinien.[13]

(4) Die Entstehung gesetzlicher Regelungen des IT-Sicherheitsrechts in chronologischer Reihenfolge

Es existiert kein einheitlich kodifiziertes Rechtsgebiet. Das IT-Sicherheitsrecht hat sich in Etappen entwickelt. Ihm fehlt deswegen die systematische Grundstruktur, was die Vielzahl der Abgrenzungsfragen erklärt.

- **Erstens** wurde zunächst 1990 das Bundesamt für Sicherheit in der Informationstechnik (BSI) durch Gesetz errichtet.[14]
- **Zweitens** wurden weitere Regelungen auf bestimmte Branchen bezogen, insbesondere seit 1996 auf die Telekommunikationsbranche nach § 87 TKG (Telekommunikationsgesetz).
- **Drittens** wurde 2007 ein Notfallkonzept für IT-Systeme (IT-Compliance) für Banken in § 25a Abs. 1 S. 3 Nr. 3 KWG geregelt.
- **Viertens** folgte 2009 zum Risikomanagement in der Versicherungsbranche die Regelung nach § 26 VAG, durch die die Richtlinie 2009/138/EG umgesetzt wurde.
- **Fünftens** wurde 2009 in der Energiebranche eine Regelung der IT-Sicherheit bei Energieversorgungsnetzen in § 11 EnWG geregelt.
- **Sechstens** wurde das Gesetz über das Bundesamt für Sicherheit in der Informationstechnik 2009 BSIG neu gefasst. Dem Amt (BSI) wurden mehr Informationspflichten, aber keine neuen Kompetenzen übertragen.[15] Nach der Legaldefinition zur IT-Sicherheit nach § 2 Abs. 2 BSIG besteht der Gesetzeszweck aus drei Schutzzielen, erstens der Verfügbarkeit, zweitens der Unversehrtheit und drittens der Vertraulichkeit von Informationen. Sicherheitsstandards sind einzuhalten.

Vertraulichkeit

Informationen müssen oft geheim bleiben und dürfen nur von autorisierten Personen gelesen werden. Unter diesem Schutzziel wird die Vertraulichkeit verstanden. Es wird erreicht durch Verschlüsselungen[16] (kryptographische Methoden[17]), durch Zugriffskontrollen von der Beteiligung von Zugriffsberechtigungen.

Integrität

Das zweite Schutzziel ist die Integrität. Danach müssen Daten vor unautorisierten Änderungen geschützt werden. Sie dürfen nicht manipuliert werden.

Verfügbarkeit

Das dritte Schutzziel ist die Verfügbarkeit. IT-Systeme müssen immer verfügbar sein. Es muss jederzeit auf die Daten zugegriffen werden können.[18]

Durch informationstechnische Systeme, Komponenten oder Prozesse sollen Bedrohungen der Schutzziele erstens erkannt und zweitens durch geeignete Schutzmaßnahmen abgewendet werden. Die Mitarbeiter der bedrohten Unternehmen sind zu geeigneten Schutzmaßnahmen anzuhalten. Nach der Gesetzesbegründung ist das ausdrückliche Ziel der Regelungen, die IT-Sicherheit von Unternehmen zu gewährleisten, um den Schutz von Internet-Nutzern zu erhöhen.[19]

Die branchenspezifischen Regelungen dienten noch nicht dem Schutz der IT-Systeme als solche und dem Schutz der IT-Infrastruktur.[20]

13 Wimmer/Meschler, Rechtshandbuch Cyber-Security, S. 123, 128.

14 Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSIG) vom 17.12.1990 (BGBl. I 1990, S. 2234)

15 Gesetz zur Stärkung der Sicherheit in der Informationstechnik des Bundes vom 10. August 2009 (BGBl. I 2009 S. 2821).

16 Kipker, Cybersecurity: Rechtshandbuch, 2020, S. 31.

17 Kipker, Cybersecurity: Rechtshandbuch, 2020, S. 29.

18 Kipker, Cybersecurity: Rechtshandbuch, 2020, S. 26.

19 BT-Drs. 18/496 S. 1.

20 Roos, MMR 2014, S. 723, 724; Wimmer/Meschler, Rechtshandbuch Cyber-Security, S. 124.

- **Siebtens** trat das IT-SiG[21] (IT-Sicherheitsgesetz) am 25.07.2015 in Kraft. Das Bundesamt für Sicherheit in der Informationstechnik erhielt mit dem IT-SiG die Funktion einer Zentralstelle mit den neuen Aufgaben, Informationen über Sicherheitslücken und neue Angriffsmuster auf die Sicherheit der Informationstechnik zu sammeln und auszuwerten, ein Informationssystem aufzubauen, um die Sicherheitslage zu analysieren, die Bundesbehörden und Betreibern kritischer Infrastruktur zu unterrichten und um für IT-Sicherheitsvorfälle als zentrale Meldestelle zu fungieren. Es enthält Sicherheitsanforderungen für spezielle informationstechnische Systeme und Meldepflichten für IT-Sicherheitsvorfälle von Betreibern kritischer Infrastruktur und von Bundesbehörden.

Die Aufgaben des Bundesamtes nach § 3 BSIG sind,

- die Abwehr von Gefahren für die Sicherheit,
- die Sammlung und Auswertung von Informationen und das Bereithalten der gewonnen Erkenntnisse,
- die Untersuchung von Sicherheitsrisiken,
- die Prüfung, Bewertung und Zulassung von informationstechnischen Systemen,
- die Beratung bei organisatorischen und technischen Sicherheitsmaßnahmen,
- die Entwicklung sicherheitstechnischer Anforderungen an die einzusetzende Informationstechnik,
- die Bereitstellung von IT-Sicherheitsprodukten,
- die Amtshilfe für Behörden.

Das Bundesamt fungiert nach § 4 BSIG als zentrale Meldestelle für die Sicherheit in der Informationstechnik. Vor allem zählt nach § 8a BSIG die Sicherung der Informationstechnik kritischer Infrastrukturen in Form von Handlungspflichten und Nachweispflichten zu seinen Aufgaben. Nach § 8c BSIG sind die Anbieter digitaler Dienste zu präventiven Maßnahmen und zur Meldung verpflichtet.

Das IT-Sicherheitsgesetz (IT-SIG) ist kein Gesetz zur Gefahrenabwehr durch Sicherheitsbehörden, sondern dient dem Risikomanagement.[22] Es enthält keine einheitliche Regelung des Rechts der IT-Sicherheit, sondern ist ein Artikelgesetz, das dem Risikomanagement dient. Es enthält keine einheitliche Regelung des Rechts der IT-Sicherheit. Als Artikelgesetz enthält es punktuelle Änderungen in Spezialgesetzen. Es ändert Pflichten in sicherheitskritischen Sektoren, wie dem Atomrecht in § 4b AtG, im Energiewirtschaftsrecht in § 11 Abs. 1a, 1b, 1c, im Telekommunikationsrecht in § 109 und 109a und im Telemedienrecht in § 13 Abs. 7 TMG.

- **Achtens** wurde am **19.07.2016** ein Jahr nach Inkrafttreten des IT-Sicherheitsgesetzes die EU-Richtlinie 2016/1148/EU über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen (NIS-RL) EU-weit erlassen.[23]

- **Neuntens** hat der deutsche Gesetzgeber ein Jahr später am 24.06.2017 die Richtlinie mit dem NIS-Umsetzungsgesetz in nationales Recht übertragen.[24] Mit diesem Gesetz werden das BSIG, das AtG, das EnWG, das TKG, das SGB V geändert.

Im nächsten Umsetzungsgesetz ist der deutsche Gesetzgeber über die Anforderungen der NIS-RL hinausgegangen.[25] Der Adressatenkreis der in der NIS-RL geregelten kritischen Sektoren ist kleiner als der nach dem BSIG in Verbindung mit der BSI-KritisV. Die NIS-RL unterscheidet als Adressaten Betreiber wesentlicher Dienste nach Art. 14, 15 NIS-RL und richtet sich an die Betreiber kritischer Infrastruktur. Als geregelte Sektoren nach Anhang II benennt die Richtlinie als wesentliche Dienste die Trinkwasserlieferungsversorgung, während BSI-KritisV zusätzlich den Sektor der Ernährung einschließt. Der Sektor digitale Infrastruktur benennt als wesentliche Dienste nach der NIS-RL

21 Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme, BGBl. I 2015, S. 1324.

22 Wimmer/Meschler, Handbuch, S. 125; Schallbruch, CR 2016, 663, 667.

23 ABl. EU Nr. L 194, 6.07.2016 S. 1.

24 BT-Drs. 18/11242, S. 1.

25 Schallbruch, CR 2016, 663, 667; Wimmer/Meschler, Rechtshandbuch Cyber-Security , S. 125 Fn. 20. Siehe Anlage und Übersicht.

- Internetknoten,
- Domain-Namen-System-Dienste-Anbieter und
- Top-Level-Domain-Registres.

Darüber hinaus gehend erfasst die BSI-KritisV im Untersektor Informationstechnik die Telekommunikation, ortsgebundene Zugangsnetze, Übertragungsnetze, Rechenzentren, Serverfarmen, Content delivery Netzwerke und Anlagen zur Erbringung von Vertrauensdiensten.[26] Der nationale Gesetzgeber ist grundsätzlich berechtigt, die europäischen Regelungen in Richtlinien bei der Umsetzung zu überschreiten und damit die Sicherheitsregeln zu verschärfen. Dazu gehört auch die Ausweitung des Anwendungsbereichs. Mit der NIS-RL verpflichtet die EU die Betreiber kritischer Infrastrukturen und erstmalig vor allem auch die Anbieter digitaler Dienste außerhalb der kritischen Infrastrukturen zum Schutz der IT-Sicherheit.[27] Der Grund für die Regelung der Anbieter digitaler Dienste besteht darin, dass die Funktionsfähigkeit des Binnenmarktes von funktionsfähigen digitalen Diensten abhängt, auch wenn sie nicht als kritische Infrastruktur angesehen werden. Zu den digitalen Diensten werden beispielweise E-Mail-Dienste und DNS-Dienste gezählt.[28]

Zu den wesentlichen Diensten[29] nach Art. 14, 15 NIS-RL zählen zur digitalen Infrastruktur, Internet-Knoten (Internet exchange points-IXP), an denen verschiedene unabhängige Netze miteinander verbunden sind und die für den Austausch zwischen unterschiedlichen Providern sorgen. Internet-Knoten sind auch vom deutschen Gesetzgeber als kritisch angesehen worden.[30] DNS-Dienste-Anbieter, Top-Level-Domain-Namen-Registries. DNS-Dienste-Anbieter, leisten Dienste, mit deren Hilfe die im Internet verwendeten Domainnamen wie zum Beispiel www.cr-online.de in die für die technische Abwicklung nötigen IP-Adressen umgewandelt werden.[31] Im IT-BSIG und BSI-KritisV überschreitet der deutsche Gesetzgeber die EU-Definition digitaler Infrastruktur. Als kritische Dienstleistungen wird die Bereitstellung von Rechenzentrumsdienstleistungen (Housing) angesehen. Die Anforderungen an die Sicherheit digitaler Dienste im Vergleich zu den wesentlichen Diensten, die die Infrastruktur betreffen, sind gemäß Art. 49 NIS-RL der Richtlinie eingeschränkt. Weil sie regelmäßig grenzüberschreitende Wirkung haben, dürfen die Nationalstaaten keine zusätzlichen Sicherheits- oder Meldepflichten auferlegen, um die Wettbewerbsfähigkeit europaweit angebotener Dienste nicht zu gefährden. Zu den digitalen Diensten nach Art. 16 und 17 NIS-RL zählen Online-Marktplätze, soziale Netzwerke, Cloud-Computing-Dienste. Die digitalen Dienste sind enumerativ in Art. 4 Nr. 5 in Anhang III aufgezählt.[32]

Andere Internetdienste fallen nicht unter den Begriff der digitalen Dienste. Ausgenommen sind Art. 16 Abs. 11 NIS-RL, Angebote von Kleinst- und Kleinunternehmen mit weniger als 50 Mitarbeitern und einem Jahresumsatz unterhalb 10 Millionen Euro.[33]

Unter **Online-Marktplätze**[34] werden Internetdienste verstanden, die den Vertragsabschluss zwischen zwei Parteien ermöglichen, wobei der Betreiber nicht selbst Vertragspartei ist. Davon zu unterscheiden sind reine Vermittlerdienste, die nur den Vertragspartner zugänglich machen aber keine Vertragsschlüsse abwickeln.[35]

Zu **Online-Suchmaschinen**[36] werden nach der NIS-RL Dienste gezählt, die grundsätzlich Suchen in allen Websites ermöglichen.[37]

26 Wimmer/Meschler, Rechtshandbuch Cyber-Security, S, 125 Fn. 20.

27 Schallbruch, Die EU-RL über Netz- und Informationssicherheit: Anforderungen an digitale Dienste, CR 2016, S. 663.

28 Witt/Freudenberg, CR 2016.

29 ABl. EU Nr. L 194 Erwägungsgrund 19.

30 Anhang IV Teil III Nummer 1.3.1. BSI-KritisV.; Schallbruch, CR 2016, S. 665; ABl. EU Nr. L 194, Erwägungsgründe 48,49.

31 Artikel 4 Nr. 15 NIS-RL; ABl. EU Nr. L 194, Erwägungsgrund 18.

32 Schallbruch, CR 2016, S. 666.

33 Schallbruch, CR 2016, S. 666.

34 ABl. EU Nr. L 194, Erwägungsgrund 15.

35 Schallbruch, CR 2016, S. 666.

36 ABl. EU Nr. L 194, Erwägungsgrund 16.

37 EG 15, EG 16.

Unter **Cloud-Computing-Dienste**[38] als digitale Dienste im Sinne der NIS-RL werden diejenigen Dienste verstanden, die *„den Zugang zu einem skalierbaren und elastischen Pool gemeinsam nutzbarer Rechenressourcen"* möglich machen.[39] Darunter fallen nicht nur die klassischen Cloud-Anbieter, sondern auch Internetdienste wie etwa das Angebot virtueller Instanzen von Standardsoftware, Projektmanagementsystemen oder Fotosammlungen. Die stark erweiterte Cloud-Definition erfasst damit immer mehr Dienste, die im Ergebnis unter die NIS-RL fallen und damit Pflichten auslösen. Alle drei digitalen Dienste gelten grundsätzlich auch als Telemediendienste, die die Verpflichtung nach § 13 Abs. 7 TMG (Telemediengesetz) auslösen.

Cloud-Dienste wie Serverfarmen[40] sowie Content Delivery Networks gelten, sowohl nach der NIS-RL als auch nach der BSI-KritisV als kritische Infrastruktur.[41] Im deutschen Recht reicht umgekehrt der Anwendungsbereich des § 13 Abs. 7 TMG deutlich über die digitalen Dienste der NIS-RL hinaus, wodurch Webshops und soziale Netzwerke erfasst werden.[42] Nach deutschem Recht treffen diese Cloud-Dienste als Teil der kritischen Infrastruktur schärfere Vorgaben als nach der digitalen Dienste der NIS-RL. Cloud-Dienste müssen die Anforderungen des Art. 16 NIS-RL einhalten und zusätzlich die schärferen Anforderungen des IT-Sicherheitsgesetzes (IT-SIG) der kritischen Infrastruktur, sofern sie kritische Anlagen im Sinne des deutschen Rechts sind und unter den Anhang IV Teil III BSI-KritisV fallen. Für Cloud-Dienste gelten im Zweifel die strengeren Anforderungen nach deutschem Recht.

Zehntens wurde am 30.4.2021 das neue IT-Sicherheitsgesetz 2.0 verabschiedet und vom Bundesrat am 7.5.2021 gebilligt. In der Broschüre *„Das neue IT-Sicherheitsgesetz 2.0"* werden die Neuregelungen zusammengefasst.

38 ABl. EU Nr. L 194, Erwägungsgrund 17.

39 EG 17 NIS-RL.

40 EG 41, NIS-RL.

41 EG 58 der NIS-RL.

42 Schallbruch, CR 2016, S. 666.

(5) Die Pflicht zu IT-Sicherheitsmaßnahmen

Wer digitale Dienste anbietet, ist

- **erstens** zu technisch-organisatorischen IT-Sicherheitsmaßnahmen verpflichtet und hat
- **zweitens** Sicherheitsvorfälle zu melden und
- **drittens** Überwachungsmaßnahmen zu dulden (§ 8a BSIG).

Nach Art. 16 NIS-RL haben Anbieter digitaler Dienste IT-Sicherheitsmaßnahmen zu veranlassen. Die Schutzziele werden zwar in der NIS-RL nicht genannt, zu denen die Verfügbarkeit, die Vertraulichkeit, die Integrität und die Authentizität zählen. Sicherungspflichten sind nach § 13 Abs. 7 TMG definiert. Alle Maßnahmen müssen geeignet und verhältnismäßig sein und als Sorgfaltsmaßstab den Stand der Technik einhalten. Vorgeschrieben wird dieser Maßstab in der TK-Rahmenrichtlinie in Art. 13a Abs. 1, in dem IT-SiG, in § 8a Abs. 1 Satz 2 BISG, § 13 Abs. 7Satz 2 TMG, § 109 Abs. 3 Satz 3 TKG. Eine Auflistung der Maßnahmen nach dem Stand der Technik findet sich in Art. 16 Abs. 1 Satz 2 NIS-RL. Unter dem Stand der Technik ist der bekannte technische Entwicklungsstand und die darauf basierenden technischen Möglichkeiten zu Erreichung eines bestimmten praktischen Ziels zu verstehen. Zum Stand der Technik liefert das BSI mit dem *„IT-Grundschutzkompendium"* Hinweise.

(6) Der „Stand der Technik"

Erstmals wurde der Begriff *„Stand der Technik"* in der Kalkar-Entscheidung des Bundesverfassungsgerichts[43] von 1978 definiert. Das Bundesverfassungsgericht unterscheidet den Begriff Stand der Technik von ähnlich lautenden Technologiemaßstäben. Die allgemeinen anerkannten Regeln der Technik bilden die unterste Stufe. Die oberste und höchste Anforderung ist der Stand der Wissenschaft und Forschung. Dazwischen liegt der Stand der Technik. Die Abgrenzung wurde an den Anforderungen des § 7 AtomG vorgenommen und muss in das Cyber-Sicherheitsrecht übertragen werden, weil

43 BVerfG, Beschluss vom 8.8.1978 – 2 BvL 8/77 = BVerfGE 49, 89-147.

der Gesetzgeber diesen Begriff für die Cyber-Sicherheitsanforderungen ebenfalls nutzt.

Die Generalklausel der ***„allgemein anerkannten Regeln der Technik"*** wird für alle Fälle mit vergleichsweise geringem Gefährdungspotenzial verwendet, die aufgrund gesicherter Erfahrung technisch beherrschbar sind. Nach herrschender Ansicht der beteiligten Kreise, der Fachleute, Anwender und Verbraucher müssen die anerkannten Regeln der Technik geeignet sein, das gesetzlich vorgegebene Ziel zu erreichen und sich in der Praxis bewährt haben. Verwendung findet dieser Technologiestandard zum Beispiel in § 49 Abs. 1 EnWG.

Mehr wird dagegen vom ***„Stand der Technik"*** verlangt. Darunter ist der Entwicklungsstand fortschrittlicher Verfahren, Einrichtungen und Betriebsweisen zu verstehen, der nach herrschender Ansicht führender Fachleute das Erreichen des gesetzlich vorgegebenen Ziels gesichert erscheinen lässt. Die Technik sollte sich im Betrieb mit Erfolg erprobt haben, was bei durchgeführten Gefährdungsbeurteilungen zu ermitteln ist. Der Standard muss zwar mit Erfolg erprobt, aber er muss nicht anerkannt sein wie die anerkannten Regeln der Technik. Er muss über dem Durchschnitt liegen.

Der darüber hinausgehenden Anforderungen nach dem *„Stand von Wissenschaft und Technik"* beschreibt das höchste Anforderungsniveau und ist in Fällen mit sehr hohem Gefährdungspotenzial zu verwenden, wie zum Beispiel bei der friedlichen Nutzung der Kernenergie nach § 7 Abs. 2 Nr. 3 AtG. Nach herrschender Ansicht führender Fachleute aus Wissenschaft und Technik und auf der Grundlage neuester wissenschaftlich vertretbarer Erkenntnisse im Hinblick auf das gesetzlich vorgegebene Ziel muss das Erreichen dieses Ziel als gesichert erscheinen lassen.[44]

Der *„Stand der Technik"* im Bereich des Cyber-Sicherheitsrechts wird durch die schnellen Entwicklungszyklen der IT-Technik charakterisiert. Die Verwendung wird genutzt, um das erforderliche Sicherheitsniveau flexibel zu nutzen. Die Technik der IT-Sicherheit entwickelt sich ständig weiter. Sie wird vorgeschrieben, um die hohen Risiken abzuwenden und zu erkennen. Die Vorteile der Digitalisierung können nur genutzt werden, wenn in den für das Funktionieren des Gemeinwesens wichtigen Bereichen, der kritischen Infrastruktur, die Gewährleistung einer hohen Cybersicherheit erreicht wird. Das Sicherheitsbedürfnis erlaubt es nicht, auf die Anerkennung einer Technik zu warten. Vielmehr müssen beim Erkennen von Risiken für die IT-Sicherheit die erprobten Verfahren angewandt werden.[45] Auf eine allgemeine Anerkennung muss im Interesse der Sicherheit vor Angriffen und zur Abwendung von Angriffen verzichtet werden. Die Nutzung öffentlich bekannt gewordener Schwachstellen bedarf einer schnellen technischen Reaktion durch Patching auf dem jeweils neusten erprobten Stand, ohne dass eine allgemeine Anerkennung für die verwendete Technik erforderlich wäre. Die Schutz und Abwehrinteressen der Betreiber Kritischer Infrastruktur rechtfertigen es, die zuletzt erprobten überdurchschnittlichen Techniken der auf den Markt verfügbaren Soft- und Hardware vorzuschreiben.

Der jeweils aktuelle Entwicklungsstand der Technik beim Erkennen und beim Abwehren von Risiken für die IT-Sicherheit muss jeweils ermittelt werden. Inwieweit das IT-Grundschutz-Kompendium des BSI einen verbindlichen Maßstab zum Stand der Technik liefert ist umstritten. Der Gesetzgeber will offenbar die technischen Richtlinien des BSI als Wiedergabe des Standes Technik ansehen, was wörtlich dem Regierungsentwurf zu entnehmen ist. *„Authentifizierungsverfahren"* sind nach dem entsprechenden aktuellen und veröffentlicht technischen Richtlinien des BSI jedenfalls dem Stand der Technik gemäß als hinreichend sicher anzusehen.[46] Dagegen wird vertreten, mehr als Hinweise solle das IT-Grundschutzkompendium zum Stand der Technik nicht geben. Es fehle an einem förmlichen Verfahren und an der Beteiligung Dritter.[47]

Dagegen wiederum wird die Vermutung für den Stand der Technik durch das IT-Grundschutzkompendium durch die besondere Stellung des Bundesamtes (BSI) begründet, die ihm durch das Gesetz als zentrale Melde- und Sammelstelle für alle Vorfälle eingeräumt wird.

44 Kipker, Cybersecurity: Rechtshandbuch, 2020, S. 86.

45 Kipker, Cybersecurity: Rechtshandbuch, 2020, S. 91.

46 Begr. RegE, BT-Drs. 18/4096, 34.; Spindler, IT-Sicherheitsgesetz und zivilrechtliche Haftung, CR 2016, S. 303.

47 Spindler, IT-Sicherheitsgesetz und zivilrechtliche Haftung, CR 2016, S.

Das BSI soll nach der Gesetzeslage als Kompetenzzentrum für die IT-Sicherheit gelten. Inwieweit die Erstellung des Kompendiums auch von Dritten beeinflusst wird und ob ein förmliches Verfahren die Formulierung der Schutzmaßnahmen beeinflusst, ist nicht geregelt. Bei der Organisation der unternehmensinternen IT-Sicherheit kann auf keinen Fall auf die Berücksichtigung des IT-Kompendiums verzichtet werden.

(7) Stand der Technik: nur berücksichtigen oder zwingend einhalten?

Nach Art. 14 Abs. 1 Satz 2 NIS-RL ist der Stand der Technik als Maßstab für die zu ergreifende Maßnahmen auch bei wesentlichen Diensten im Sektor digitaler Infrastruktur zu **berücksichtigen**, was bedeutet, ihn nicht zwingend **einhalten** zu müssen. Die Berücksichtigung des Stands der Technik fordert der Gesetzgeber in § 13 Abs. 7 TMG von Telemediendiensten und in § 109 TKG von Telekommunikationsdiensten. Allerdings sollen dagegen die vom IT-SIG erfassten Betreiber kritischen Infrastrukturen nach § 8a Abs. 1 BSIG den Stand der Technik einhalten. Nur in begründeten und zu dokumentierenden Fällen darf abgewichen werden.[48] Der deutsche Gesetzgeber hat mit § 8a Abs. 1 BISG im Vergleich zum europäischen Recht einen schärferen Maßstab für kritische Infrastrukturen durchgesetzt, wozu er berechtigt ist, weil die Regelung zur kritischen Infrastruktur nur innerhalb der Grenzen der deutschen Rechtsordnung gelten. Deshalb besteht kein grenzüberschreitender Bedarf an Harmonisierung auf EU-Ebene.

Die Konkretisierung der Sicherungsmaßnahmen bleibt eine schwierige Aufgabe. Wenn einerseits offenbleibt, was unter dem *„Stand der Technik"* bei der Erkennung als auch bei der Abwehr von Risiken für die IT-Sicherheit gelten muss und ob und wo dieser nur schwer festzustellende Maßstab zu berücksichtigen oder verbindlich einzuhalten ist, erschwert dem Normadressaten die Einhaltung seiner Pflichten durch die Risikoabwehr für die IT-Sicherheit im Unternehmen. Diese Unsicherheit beim Normgeber sowohl auf europäischer als auch auf nationaler Ebene zwingt zur Selbsthilfe und zur Selbstregulierung. Das deutsche IT-SIG hat mit § 8a Abs. 2 BISG für die kritische Infrastruktur die Möglichkeit eingeräumt, branchenspezifische Sicherheitskataloge zu erarbeiten und dem Bundesamt vorzuschlagen, das wiederum auf Antrag feststellt, ob diese Anforderungen geeignet sind, um die Anforderungen nach § 8a Abs. 1 BSIG zu gewährleisten.[49]

(8) Dokumentations-, Mitteilungs- und Meldepflichten

Nach § 8a Abs. 3 BSIG haben Betreiber kritischer Infrastruktur alle 2 Jahre die Erfüllung der Anforderungen nach Abs. 1 in geeigneter Form dem BSI nachzuweisen, etwa durch Sicherheitsaudits, Prüfungen oder Zertifizierungen.[50]

Nach Art. 16 Abs. 3 NIS-RL haben die Anbieter digitaler Dienste Sicherheitsvorfälle mit erheblichen Auswirkungen auf die Bereitstellung ihrer Dienste, insbesondere Beeinträchtigungen der Verfügbarkeit, der Vertraulichkeit, der Integrität und der Authentizität unverzüglich zu melden, zum Beispiel den Ausfall des *„digitalen Dienstes"* oder den Diebstahl von Nutzerdaten. Meldepflichten für IT-Sicherheitsvorfälle bei digitalen Diensten außerhalb der kritischen Infrastruktur existieren im deutschen Recht nicht.

Den Meldepflichten vergleichbar ist die Befugnis des BSI nach § 7 Abs. 1 Nummer 1a BSIG zur Warnung der Öffentlichkeit vor Sicherheitslücken in informationstechnischen Produkten und Diensten. Bei *„wesentlichen Diensten"* besteht eine Meldepflicht nach Art. 14 Abs. 3 NIS-RL nur für Sicherheitsvorfälle mit erheblicher Beeinträchtigung der Verfügbarkeit. Das IT-SIG verpflichtet Betreiber kritischer Infrastrukturen in § 8b Abs. 4 Satz 1 BSIG zur Meldung bei Störung der Vertraulichkeit und der Authentizität oder Integrität

48 Spindler, CR 2016, S. 303.

49 Wimmer/Meschler, Rechtshandbuch Cyber-Security, S. 131.

50 Kipker, Cybersecurity: Rechtshandbuch, 2020, S. 378, 381; Wimmer/Meschler, Rechtshandbuch Cybersecurity S. 130.

(9) Die Legaldefinition Kritischer Infrastrukturen

Die Legaldefinition des § 2 Abs. 10 BSIG definiert kritische Infrastrukturen als Einrichtungen, Anlagen oder Teile davon, die

1. den Sektoren Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung, Finanz- und Versicherungswesen sowie Siedlungsabfallentsorgung angehören und
2. von hoher Bedeutung für das Funktionieren des Gemeinwesens sind, weil durch ihren Ausfall oder ihre Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit eintreten würden.[51]

Die kritischen Infrastrukturen im Sinne dieses Gesetzes werden durch Rechtsverordnung nach § 10 BSIG näher bestimmt. In der Fassung vom 18.5.2021 (BGBl. I . S. 1122) ist der Sektor *„Siedlungsabfallentsorgung"* dazu gekommen. In der BSI-KritisV nach § 10 Abs. 1 BSIG wird bestimmt, wann eine Anlage eine entsprechende Bedeutung für das Gemeinwesen hat und welche Dienstleistung und Anlagen in den jeweiligen Sektoren von der Regelung betroffen sein sollen. Der Adressatenkreis des BSIG wird in drei Schritten bestimmt:

- **Erstens** wird die Dienstleistung, die nach der BSI-KritisV für das Funktionieren des Gemeinwesens von besonderer Bedeutung ist bestimmt zum Beispiel die Versorgung der Allgemeinheit mit Elektrizität;
- **Zweitens** wird die Anlage oder Teile davon, die für die Erbringung der kritischen Dienstleistung erforderlich sind bestimmt zum Beispiel die Stromversorgung für die Erzeugungsanlage;
- **Drittens** wird der Schwellenwert für die Erzeugungsanlage nach der BIS-KritisV überprüft. Der Verordnungsgeber sieht eine Infrastruktur als kritisch regelmäßig dann, wenn mehr als 500.000 Menschen von der Anlage versorgt werden.[52]

(10) Die Pflichten in Unternehmen im IT-Sicherheitsrecht in drei Adressatenkreise

Alle Gesetze dienen der Abwehr von Gefahren für die IT-Sicherheit bei IT-Systemen. Nach dem BSIG lassen sich drei Adressatenkreise der Pflichten unterscheiden,

- **erstens** die Betreiber von kritischen Infrastrukturen nach § 8a, 8b BSIG sowie
- **zweitens** Betreiber kritischer Infrastrukturen, die nach § 8d Abs. 2 BISG nach speziellen Rechtsgebieten wie dem Atomrecht, dem Energiewirtschaftsrecht, dem Telekommunikationsrecht, dem Telemedienrecht geregelt sind.
- Die **dritte** Adressatengruppe sind die Anbieter digitaler Dienste außerhalb von kritischen Infrastrukturen, die aufgrund der europarechtlichen NIS-Richtlinie und nach dem NIS-Umsetzungsgesetz nach Art. 16 Abs. 1-2 NIS-RL eingeführt wurden.

Die NIS-RL verwendet für die *„Betreiber von kritischen Infrastrukturen"* nach Art. 4 Nr. 4 NIS-RL den Begriff Betreiber *„wesentlicher Dienste"*. Der Grund für die Verpflichtung der Betreiber von kritischen Infrastrukturen zum Schutz der IT-Sicherheit sind die drohenden gesamtgesellschaftlichen Folgen und Notlagen bei Störungen oder Ausfällen bei der Versorgung mit lebenswichtigen Gütern wie Strom, Wasser, Ernährung und medizinischer Versorgung.

Die BSI-KritisV bestimmt den Anwendungsbereich des Gesetzes und die anwendbaren Schutzstandards. Nach § 8d Abs. 1 BSIG sind die Pflichten nach den § 8a, 8b BSIG nicht auf Kleinstunternehmen mit weniger als 250 Mitarbeiter und einem Jahresumsatz unter 50 Millionen Euro anzuwenden.

51 Kipker, Cybersecurity: Rechtshandbuch, 2020, S. 356.

52 Wimmer/Meschler, Rechtshandbuch Cyber-Security, S. 130.

(11) Der Inhalt der Pflichten & die Bestimmung der IT-Sicherheitsstandards

Die Kritis-Betreiber haben nach § 8a Abs. 1 BSIG

„angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischer Systeme, Komponenten oder Prozesse zu treffen. Dazu zählen personelle Maßnahmen, infrastrukturelle Maßnahmen und die Abschottung besonders kritischer Prozesse."[53]

„Eingehalten werden soll" der *„Stand der Technik"*. Eingehalten bedeutet, dass eine Abweichung nur in begründeten Ausnahmefällen möglich ist.[54] Nach der Gesetzesbegründung ist der unbestimmte Rechtsbegriff *„Stand der Technik"* als *„der Entwicklungsstand fortschrittlicher Verfahren, Einrichtungen oder Betriebsweisen zu verstehen, der die praktische Eignung einer Maßnahme zum Schutz der Funktionsfähigkeit von informationstechnischen Systemen, Komponenten oder Prozessen gegen Beeinträchtigungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit gesichert erscheinen lässt."*[55] Damit werden Schutzmaßnahmen vorgeschrieben, die über dem Durchschnitt liegen. Jedenfalls wird mehr verlangt als die bloße Einhaltung der Regeln der Technik. Die auf ein *„Sollen"* beschränkte Pflicht ermöglicht Abweichungen vom Stand der Technik in begründeten Ausnahmefällen.[56]

(12) Die Konkretisierung des Stands der Technik durch Branchenstandards

Das BSIG räumt in § 8a Abs. 2 BSIG den Betreibern von Kritischer Infrastruktur und Branchenverbänden ein Vorschlagrechts ein, branchenspezifische Standards zur Konkretisierung gemäß § 8a Abs. 2 BSIG des Stands der Technik zu formulieren mit dem Nachweis, dass sie in der Praxis erfolgreich erprobte Verfahren darstellen. In einem feststellenden Verwaltungsakt befindet das BSI über die Eignung des branchenspezifischen Sicherheitsstandards. Mit diesem Verfahren gewinnt die jeweilige Branche einerseits Einfluss auf den Standard und andererseits Rechtssicherheit, die Pflicht zur Einhaltung des Stands der Technik erfüllt zu haben. Durch die Einschaltung der BSI wird vermieden, dass Branchen einen Standard praktizieren, der zu Gewährleistung der IT-Sicherheit nicht oder nur eingeschränkt geeignet ist und das Risiko von Notlagen durch Ausfälle von IT-Systemen nicht abwenden kann. Durch die Möglichkeit, den Standard selbst zu wählen, kann eine Branche den Aufwand und Kosten zur IT-Sicherheit steuern, und die jeweils kostengünstigste Variante wählen. Die Feststellung der Eignung von Branchenstandards folgt in der Regel für die Dauer von 2 Jahren. Abschließend festgestellt wurden

- Branchenstandards IT-Sicherheit für Wasser/Abwasser (Version 2.0),
- Sicherheitsstandards für die Ernährungsindustrie (Version 2.0)
- für den Lebensmittelhandel,
- die IT-Sicherheit für Anlagen oder Systeme zur Steuerung/Bündelung elektrischer Leistungen (B35 Aggregatoren, Version 1.1),
- branchenspezifische Sicherheitsstandards für Pharma,
- für die Laboratoriumsdiagnostik,
- die Gesundheitsversorgung im Krankenhaus, für die Verkehrssteuerung- und Leitsysteme im kommunalen Straßenverkehr,
- für gesetzliche Kranken- und Pflegeversicherer B35-GKV/PV (Ersatzkassen, Version 1.2).

Veröffentlicht finden sich die Sicherheitsstandards auf der Webseite des BSI.[57]

Kritisch hinterfragt wird die Lösung nach § 8a Abs. 2 BSIG zum Vorschlagsrecht von Branchenverbänden. Die technischen Regeln sind in der Praxis die durchschnittlichen Anforderungen. Mit dem Stand der Technik sind aber Anstrengungen über dem Durchschnitt zur Sicherung von IT-Syste-

53 BT-Drs. 18/4096, S. 26.

54 Spindler, CR 2016, 298, 299; Wimmer/Meschler, S. 131.

55 BT-Drs. 18/4096, S. 26; Siehe auf Seite 11 ff. zum Stand der Technik.

56 Spindler, CR 2016, S. 299.

57 https://www.bsi.bund.de

ABWEHR VON GEFAHREN FÜR IT-SYSTEME

nach NIS-RL vom 19.7.2016 und NIS, Umsetzungsgesetz von 2017
im Vergleich zum BSI-Gesetz und BSI-KritisV

ADRESSATENKREIS UND ANWENDUNGSBEREICH

NIS-RL

Wesentliche Dienste nach Art. 14, 15 NIS-RL

Nach Art. 4 Abs. 4, Anhang II Sektor Nr. 7 NIS-RL, digitale Infrastruktur

1. IXPs.
IXPs sind Internetknoten, deren Funktion in der Zusammenschaltung von technisch und organisatorisch getrennten Netzen besteht. Ein IXP ermöglicht keinen Netzzugang und fungiert weder als Transit-Anbieter noch als Carrier (Erwägungsgrund 18 der NIS-RL).

2. DNS-Diensteanbieter
Sind Domainnamen-Verwaltung

3. TLD-Register
Top-Level-Domain-Namen-Registries

In den folgenden Erwägungsgründen 19 f. gibt die NIS-RL vor, wie die Betreiber „wesentlicher Dienste“ zu ermitteln sind.

Entscheidend ist, welche Dienste für die Aufrechterhaltung kritischer gesellschaftlicher und wirtschaftlicher Tätigkeiten wesentlich sind. Die wesentlichen Dienste sind dadurch gekennzeichnet, dass sie von Netz- und Informationssystemen abhängen (Erwägungsgrund 20).

Nach Erwägungsgrund 26 gelten als Indikatoren für die Bedeutung der zu ermittelnden Betreiber die Anzahl und Größe, die Marktanteile, produzierte und transportierte Datenmengen.

Digitale Dienste nach Art. 16, 17 NIS-RL

Anbieter digitaler Dienste nach Art. 16 NIS-RL sind definiert und aufgelistet in Anhang III nach Art. 4 Nr. 5 NIS-RL

1. Online-Marktplätze
ermöglichen es Verbrauchern und Unternehmen, online Kaufverträge oder Dienstleistungsverträgen mit Unternehmen abzuschließen
(Erwägungsgrund 15)

2. Online-Suchmaschinen
ermöglichen die Suche auf allen Websites mit Abfragen zu beliebigen Themen
(Erwägungsgrund 16)

3. Coud-Computing-Dienste
Ermöglichen den Zugang zu einem skalierbaren und elastischem Pool gemeinsam nutzbarer Rechenressourcen, wie Netze, Server, Speicher
(Erwägungsgrund 17)

BSI-GESETZ / BSI-KRITISV VOM 22. APRIL 2016

Kritische Infrastruktur

Betreiber kritischer Infrastruktur oder nach Begrifflichkeit NIS-RL Betreiber „wesentlicher Dienste“ wie Art. 4 Nr. 4 NIS-RL. Die kritische Infrastruktur wird in § 2 Abs. 10 BSIG definiert. Der Anwendungsbereich ergibt sich aus § 2 Abs. 10 Nr. 1 BSIG iVm § 5 Abs. 4 BSI-KritisV, Anhang 4 Teil 3

1. Sprach- und Datenübertragung
1.1. Zugang
1.1.1. Ortsgebundene Zugangsnetze
1.2. Übertragung
1.2.1. Übertragungsnetze für öffentlich zugängliche Telefondienste und Datenübermittlungsdienste oder Internetzugangsdienste

1.3. Vermittlung
1.3.1. IXP für öffentlich zugänglich Telefondienste, Datenübermittlungsdienste oder Internetzugangsdienste
1.4. Steuerung

1.4.1. DNS-Resolver zur Nutzung öffentlich zugänglicher Telefondienste, Datenübermittlungsdienste und Interzugangsdienste
1.4.2. Autoritative DNS-Server

2. Datenspeicherung und Datenverarbeitung
2.1. Housing
2.1.1. Rechenzentrum
2.2. IT-Hosting
2.2.1. Serverfarm
2.2.2. Content Delivery Netzwerk
2.3. Vertrauensdienste
2.3.1. Anlage zur Erbringung von Vertrauensdiensten

§ 8 Abs. 1 BSIG
Stand der Technik einhalten

§ 8d BSIG
nicht anwendbar auf Kleinstunternehmen

§ 2 BISG
Das BSI-Gesetz ist nicht anwendbar auf die spezielleren Regeln im AtomG, Energiewirtschaftsgesetz, Telekommunikationsgesetz und Telemediengesetz.

Digitale Dienste

Nach § 2 Abs. 11 BSIG sind Dienste, im Aktionsverfahren auf dem Gebiet der technischen Vorschriften und der Vorschriften für die Dienste der Informationsgesellschaft,

- Online-Marktplätze
- Online-Suchmaschinen
- Cloud-Computing-Dienste

Nach § 2 Abs. 12 BSIG sind „Anbieter digitaler Dienste“ eine juristische Person, die einen digitalen Dienst anbietet.
(definiert in Art. 16 NIS-RL und Erwägungsgrund 15, 16 und 17)

ABWEHR VON GEFAHREN FÜR IT-SYSTEME

nach NIS-RL vom 19.7.2016 und NIS, Umsetzungsgesetz von 2017
im Vergleich zum BSI-Gesetz und BSI-KritisV

PFLICHTEN

NIS-RL

Wesentliche Dienste nach Art. 14, 15 NIS-RL

Art. 14 Abs. 1 – 2 NIS-RL

verpflichtet die Mitgliedstaaten, den Betreibern wesentlicher Dienste unter Berücksichtigung des Stands der Technik Sicherheitsanforderungen und die Meldung von Sicherheitsvorfällen zu verpflichten.

Digitale Dienste nach Art. 16, 17 NIS-RL

Nach Art. 16 Ziffer 3 sind die Mitgliedsstaaten verpflichtet, die Anbieter digitaler Dienste zu Sicherheitsanforderungen und zu Meldung von Sicherheitsvorfällen zu verpflichten.

§ 8a Abs. 2 BSIG
Konkretisierung des Stands der Technik durch branchenspezifische Sicherheitsstandards bestätigt durch feststellende Verwaltungsakte des BSI.

§ 8a Abs. 3 BSIG
Erfüllungsnachweis der Pflichten nach § 8a Abs. 1 BSIG durch Audits, Prüfungen und Zertifizierungen alle 2 Jahre.

§ 8a Abs. 4 BSIG
Zugangsgewährungspflicht
Herausgabepflicht von Unterlagen

BSI-GESETZ / BSI-KRITISV VOM 22. APRIL 2016

Kritische Infrastruktur

§ 8a Abs. 1 BSIG
Die Pflicht zur angemessenen organisatorischen und technischen Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit informationstechnischer Systeme, Komponenten und Prozesse zu treffen, die für die Funktionsfähigkeit der von ihnen betriebenen kritischen Infrastrukturen maßgeblich sind. Der Stand der Technik soll eingehalten werden.

§ 8a Abs. 2 BSIG
Konkretisierung des Stands der Technik durch branchenspezifische Sicherheitsstandards bestätigt durch feststellende Verwaltungsakte des BSI.

§ 8a Abs. 3 BSIG
Die Pflicht zum Nachweis alle 2 Jahre der Erfüllung der Anforderungen nach § 8a Abs. 1 BSIG.

§ 8d BSIG
Nicht anwendbar auf Kleinstunternehmen

Pflichten aus Spezialgesetzen zur IT-Sicherheit:
§ 44b AtG
§ 11 Abs. 1a, 1b, 1c EnWG
§§ 109 und 109a TKG
§ 13 Abs. 7 TMG

Verkehrssicherungspflichten
Pflichten ergeben sich aus der Definition des „Stands der Technik“ durch das Bundesamt für die IT-Sicherheit. Pflichten aus dem Grundschutzkompendium des BSI.

Digitale Dienste

§ 8c Abs. 1 BSIG
Anbieter digitaler Dienste haben technische und organisatorische Maßnahmen zu treffen, um Risiken für die Sicherheit der Netz- und Informationssysteme zu bewältigen, die sie zur Bereitstellung der digitalen Dienste innerhalb der EU nutzen, insbesondere um den Auswirkungen von Sicherheitsvorfällen auf digitale Dienste vorzubeugen oder die Auswirkungen so gering wie möglich zu halten.

§ 8c Abs. 2 BSIG
Bei allen Maßnahmen zur Bewältigung von Risiken für die Sicherheit der Netz- und Informationssysteme muss der Stand der Technik berücksichtigt werden, im Unterschied zu Einhaltung nach § 8a Abs. 1 BSIG:

§ 8c Abs. 3 BSIG
Jeder Sicherheitsvorfall ist vom Anbieter digitaler Dienste unverzüglich dem Bundesamt zu melden, insbesondere die Zahl der betroffenen Nutzer, die Dauer des Sicherheitsvorfalls, das vom Sicherheitsvorfall betroffene geographische Gebiet, das Ausmaß der Unterbrechung der Bereitstellung des Dienstes und die Auswirkungen auf wirtschaftliche und gesellschaftliche Tätigkeiten.

Art. 15 Abs. 1 NIS-RL
Nach § 15 BSIG gilt das BSI-Gesetz auch für Anbieter digitaler Dienste

men anzustreben. Fraglich ist auch, ob eine Branche sich freiwillig auf überdurchschnittliche Anstrengungen zur IT-Sicherheit verständigen kann.[58]

(13) Ungeregelte offene Fragen

Ungeregelt blieb im BSIG die Pflege und Aktualisierung der Branchenstandards, die Auswahl bei konkurrierenden Vorschlägen zu den Standards. Offen bleibt auch wie im Streitfall etwa durch Sachverständigengutachten der Stand der Technik zu ermitteln ist. Die Rechtswirkung von BSI-Feststellungen zu IT-Sicherheitsstandards besteht in der Selbstbindung der Verwaltung vergleichbar mit den Verwaltungsvorschriften mit Außenwirkung.[59] Die Selbstbindung des BSI muss Grund und Anreiz dafür sein, Branchenlösungen vorzuschlagen.

(14) Die Pflicht zum Nachweis der IT-Sicherheit nach § 8a Abs. 3 BSIG

Es ist mindestens alle 2 Jahre nachzuweisen, dass die Anforderungen nach § 8a Abs. 1 BSIG eingehalten werden. Diese Nachweispflicht dient der Überprüfung der Einhaltung eines angemessenen Sicherheitsniveaus durch den Betreiber.[60] Der Nachweis kann durch Audits und Zertifizierungen erbracht werden. Die Betreiber müssen nach § 8b Abs. 3 BSIG eine Kontaktstelle dauerhaft besetzen und dem BSI mitteilen oder nach § 8b Abs. 5 BSIG eine übergeordnete Ansprechstelle zur Verfügung stellen. Nicht geregelt sind Vorgaben für die Akkreditierung und Zugangsvoraussetzungen der Auditoren. Es fehlt im Übrigen eine Befugnis des BSI, ein Sicherheitsaudit anzuordnen.[61]

Als einzige Sanktion bleiben die Tatbestände des § 14 Abs. 1 Nr. 1, 2 BSIG. Um Sanktionen durch Bußgelder zu vermeiden, sind die Betreiber der kritischen Infrastruktur darauf angewiesen, konkrete Vorkehrungen zum Zwecke der IT-Sicherheit zu kennen.

(15) Mitwirkungspflichten

Betreiber von kritischer Infrastruktur sind verpflichtet, nach § 8a Abs. 4 Satz 2 BSIG Zugang zu Geschäfts- und Betriebsräumen zu gewähren und Unterlagen herauszugeben. Dem BSI steht das Recht zur Überprüfung gemäß § 8a Abs. 4 Satz 1 BSIG nach dem NIS-Umsetzungsgesetz gemäß Art. 15 Abs. 1 NIS-RL zu.

(16) Meldepflichten

„*Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit von informationstechnischen Systemen, Komponenten oder Prozessen*“ müssen nach § 8b Abs. 4 Satz 1 BSIG dem BSI gemeldet werden. Zu melden sind nur **erhebliche Störungen**, die zu einem Ausfall der kritischen Infrastruktur geführt haben oder dazu führen können. Eine Störung ist dann anzunehmen, wenn die eingesetzte Technik, die ihr zugedachte Funktion nicht mehr richtig oder nicht mehr vollständig erfüllen kann oder versucht wurde, entsprechend auf sie einzuwirken. Dazu zählen insbesondere Fälle von Sicherheitslücken, Schadprogrammen und Angriffen auf die Sicherheit in der Informationstechnik sowie außergewöhnliche und unerwartete technische Defekte mit IT-bezug.[62] Der Störungsbegriff ist weit auszulegen, um den Schutzzweck des BSIG zu gewährleisten.[63] **Erheblich** sind Störungen dann, wenn die Funktionsfähigkeit der erbrachten kritischen Dienstleistung bedroht ist und die IT-Störung nicht bereits automatisiert oder mit wenig Aufwand mithilfe der nach § 8a BSIG als Stand der Technik beschriebenen Maßnahmen abgewehrt werden kann.[64] Ob es auf den Aufwand der Abwehrmaßnahmen ankommen kann, wird bestritten. Es muss auf die Auswirkungen ankommen. Als erheblich angesehen werden nach der Gesetzesbegründung Fälle neuartiger Angriffe und unerwarteter Vorkommnisse.[65] An der Anonymisierung der Schadensfälle im Gesetzgebungsverfahren hatte die Wirtschaft aus Sorge um Reputationseinbußen ein starkes Interesse. Durch die

58 Spindler, CR 2016, S. 299.

59 Spindler, CR 2016, S. 299.

60 BT-Drs. 18/4096, S. 26.

61 Spindler, CR 2016, S. 300, Hornung, NJW 2016, S. 3336.

62 Begr. RegE, BT-Drs. 18/4096, S. 27.

63 Spindler, CR 2016, S. 300; Roos, MMR 2015, S. 636, 639.

64 Begr. RegE, BT-Drs. 18/4096, S. 28.

65 Begr. RegE. BT-Drs. 18/4096, S. 28.

Anonymisierung wird erreicht, dass die Meldung nicht direkt an das BSI, sondern über eine Kontaktstelle nach § 8b Abs. 3 BSIG erfolgen kann. Der Inhalt der Meldung muss *„zu der Störung sowie zu den technischen Rahmenbedingungen, insbesondere der vermuteten oder tatsächlichen Ursache der betroffenen Informationstechnik, der Art der betroffenen Einrichtung oder Anlage sowie zur Branche der Betreiber"* Angaben enthalten. Aus den Meldungen müssen sich genügende Informationen für Angriffsszenarien ergeben, um Erfahrungen für angemessene Schutzmaßnahmen treffen zu können. Die Meldepflicht enthält unbestimmte Rechtsbegriffe, sodass die Grenzen der Meldepflicht unklar bleiben. Jede Meldung kann Rückschlüsse über Versäumnisse der IT-Sicherheit im Unternehmen zulassen, sodass mit jeder Meldung die Gefahr der Selbstbelastung durch Hinweise auf Sicherheitslücken besteht. Untersuchungen durch das BSI vor Ort sieht das BSIG nicht vor.[66] Durch Meldungen können damit Anordnungen des BSI veranlasst werden, um von den Betreibern der Kritischen Infrastrukturen die Beseitigung von Sicherheitsmängeln nach § 8a Abs. 3 Satz 4 Nr. 2 BSIG zu verlangen.

(17) Anforderungen an Anbieter digitaler Diensten

Die bisher dargestellten Pflichten richteten sich an die Betreiber Kritischer Infrastrukturen. Nach § 8a BSIG haben die Betreiber Kritischer Infrastrukturen den Stand der Technik einzuhalten. Mit der NIS-RL vom 6.7.2016 hat die EU auch die Anbieter digitaler Dienste zu technischen und organisatorischen Maßnahmen verpflichtet, um die IT-Sicherheit einzuhalten. Umgesetzt ist die Pflicht in § 8c BSIG. Nach § 8c Abs. 1 BSIG sind die Anbieter digitaler Dienste zu Schutzmaßnahmen verpflichtet, den *„Stand der Technik"* zu berücksichtigen. Im Unterschied zu § 8a BSIG ist diese Pflicht schwächer, da die Betreiber Kritischer Infrastrukturen verpflichtet sind, den Stand der Technik einzuhalten. Die Pflicht, den Stand der Technik zu berücksichtigen bedeutet, dass er bei der Bestimmung der Schutzmaßnahmen einbezogen werden muss, aber davon abgewichen werden kann.[67] Die Betreiber kritischer Infrastrukturen können dagegen vom Stand der Technik nur in begründeten Ausnahmefällen abweichen.[68]

Diese Unterscheidung zwischen den Pflichten der Betreiber Kritischer Infrastruktur und den Anbieter digitaler Dienste begründet NIS-RL vom 6.7.2016 ausführlich in den Erwägungsgründen 48, 49 und 57.[69]

Anbieter digitaler Dienste gemäß § 2 Abs. 11 und 12 BSIG sind juristische Personen, die digitale Dienste, nämliche **Online-Marktplätze, Online-Suchmaschinen** und **Cloud-Computing-Dienste** anbieten. In Artikel 4 Nr. 5 und Anhang 3 NIS-RL sind diese digitalen Dienste enumerativ aufgezählt. Die Definition dazu findet sich in den Erwägungsgründen zur NIS-RL.[70] Online-Marktplätze bieten Vertragsabschlussgelegenheiten wie zum Beispiel ebay, Amazon, AppStores. Dazu zählen nicht die bloßen Vermittler. Online-Suchmaschinen bieten Recherchedienste in allen Websites an. Unter Cloud-Computing-Dienste sind Dienste zu verstehen, die den Zugang zu einem skalierbaren und elastischen Pool gemeinsam nutzbarer Rechenressourcen ermöglichen.

Im Ergebnis werden an die Anbieter digitaler Dienste geringere Anforderungen gestellt als an die Betreiber Kritischer Infrastruktur.

Die NIS-RL unterscheidet in Kapitel IV zwischen den Betreiber *„wesentlicher Dienste"* und Kapitel V den Anbietern digitaler Dienste. Die Betreiber *„wesentlicher Dienste"* werden in Artikel 14 und 15 NIS-RL geregelt, während die Anbieter digitaler Dienste in Artikel 16 und 17 NIS-RL geregelt sind. Entsprechend sind die Anbieter digitaler Dienste in der Umsetzung in § 8c BSIG geregelt. Das BSIG hat den Begriff der wesentlichen Dienste der NIS-RL nicht übernommen. Die wesentlichen Dienste nach NIS-RL sind geregelt in § 8a

66 Spindler, CR 2016, S. 301.

67 Wimmer/Meschler, S. 134.

68 Spindler, CR 2016, S. 298/299; Wimmer/Meschler, S. 131; Siehe auf Seite 12.

69 ABl. EU NR. L 194 Erwägungsgründe 48, 49 und 57.

70 ABl. EU Nr. L 194, Nr. 15 für Online-Marktplatz, Nr. 16 für Online-Suchmaschinen, Nr. 17 für Cloud-Computing-Dienste.

BSIG, nämlich als Betreiber Kritischer Infrastruktur. Nach der NIS-RL sollen die Mitgliedstaaten in ihrem Hoheitsgebiet erbrachte Dienste auflisten, die zu den Betreibern wesentlicher Dienste zählen.[71] Die Größe der Betreiber sollen dabei berücksichtigt werden, insbesondere der Marktanteil und die transportierten Datenmengen.[72] Die NIS-RL bezeichnet die Unterschiede zwischen wesentlichen Diensten und digitalen Diensten als grundlegend. Ein Hauptunterschied besteht darin, dass digitale Dienste grenzüberschreitend angeboten werden. Die Mitgliedstaaten sollen in die Lage versetzt sein, die Betreiber wesentlicher Dienste zu bestimmen und an sie strengere Anforderungen zu stellen als in der NIS-RL festgelegt ist. Damit ermächtigt die NIS-RL die Mitgliedstaaten zu strengeren Anforderungen an die Anbieter wesentlicher Dienste. Die grenzüberschreitenden digitalen Dienste sollten ein hohes Maß an Harmonisierung im Hinblick auf die Sicherheitsanforderungen und Meldepflichten für Anbieter digitaler Dienste gewährleisten. Das sollte zu einer einheitlichen Behandlung der Anbieter digitaler Dienste in der Union führen, die ihrer Art und der Höhe des Risikos, dem sie unterliegen könnten, angemessen ist.[73] Nach Artikel 16 Ziffer 10 der NIS-RL sollen die Mitgliedsstaaten den Anbietern digitaler Dienste keine weiteren Sicherheits- oder Meldepflichten auferlegen. Die NIS-RL will damit Anforderungen an die Anbieter digitaler Dienste europaweit harmonisieren und versperrt den Mitgliedsstaaten die Möglichkeit der nationalen schärferen Regelungen. Die Richtlinie überlässt es den Mitgliedsstaaten allerdings, den Betreibern Kritischer Infrastrukturen schärfere Regeln zu setzen, weil bei der örtlich gebundenen Kritischen Infrastruktur kein Harmonisierungsbedarf auf EU-Ebene besteht.

Problematisch sind die Dienste, die sowohl Teil der Kritischen Infrastruktur sind, als auch digitale Dienste angesehen werden können. Im Zweifel sind für solche digitalen Dienste die schärferen präventiven Pflichten anzuwenden, weil sie ein höheres Risiko auslösen können.[74]

Die Abgrenzung zwischen wesentlichen Diensten für Betreiber Kritischer Infrastrukturen und den Anbietern digitaler Dienste dürfte dann keine Probleme machen, weil das Ausfallrisiko beim Betreiben Kritischer Infrastruktur auch bei den Anbietern digitaler Dienste berücksichtigt werden muss. Das Risiko von Anbietern digitaler Dienste würde mit dem Risiko der Betreiber Kritischer Infrastruktur zusammenfallen und sich schon dadurch erhöhen.

Betreiber *„wesentlicher Dienste“* gemäß Art. 4 Nr. 4 NIS-RL finden sich im Anhang II der NIS-RL, aufgeteilt nach sieben Sektoren, Energie, Verkehr, Bankwesen, Finanzmarkt, Infrastrukturen, Gesundheitswesen, Trinkwasserlieferung und –versorgung und digitale Infrastruktur. Die NIS-RL nennt im Untersektor digitale Infrastruktur nur drei Dienste,

- **erstens** Internetknoten (IXPs),
- **zweitens** DNS-Dienstanbieter (Domain-Name-System-Dienstanbieter) und
- **drittens** TLD-Name-Registries (Top-Level-Domain-Registrees).

Die BSI-KritisV führt dagegen im Untersektor Informationstechnik und Telekommunikation darüber hinaus auch ortsgebundene Zugangsnetze, Übertragungsnetze, Rechenzentren, Serverfarmen, Content-Delivery-Netzwerke und Anlagen zur Erbringung von Vertrauensdiensten auf.[75]

(18) Die Befugnisse des BSI gegenüber Betreibern Kritischer Infrastruktur und Anbietern digitaler Dienste

Nach § 1 BSIG und nach § 3 Abs. 1 Satz 2 Nr. 17 BSIG ist das BSI die zentrale Stelle für IT-Sicherheit bei digitalen Diensten und damit ist das BSI zuständig für die Informationssicherheit auf nationaler Ebene. Damit das BSI die Beratungsfunktionen ausüben kann, werden alle Informationen zur IT-Sicherheit beim BSI

71 Abl. EU Nr. L 194 Erwägungsgrund 23, 25.

72 Abl. EU Nr. L 194 Erwägungsgrund 26.

73 Abl. EU Nr. L 194 Erwägungsgrund 57.

74 Wimmer/Meschler, S. 131; Schallbruch, CR 2016, S. 663, 664.

75 Wimmer/Meschler, S. 125.

zentriert. Nach § 3 Abs. 3 BSIG berät das BSI die Kritis-Betreiber zur IT-Sicherheit. Es kann nach § 3 Abs. 1 Satz 2 Nr. 14 BSIG und nach § 7 BSIG Warnungen vor Sicherheitslücken in Produkten und Diensten, vor Schadprogrammen und im Fall eines Verlustes von Daten, Warnungen aussprechen vor Sicherheitslücken in Produkten und den Einsatz von Sicherheitsprodukten empfehlen.

Das BSI hat die Kompetenz, konkretisierende Sicherheitsstandards für einzelne Branchen festzustellen. Nach § 8a Abs. 5 BSIG kann das BSI Anforderungen an die Sicherheitsaudits und die Zertifizierung festlegen und Dokumentationen von Kritis-Betreibern nach § 8a Abs. 3 Satz 3 BSIG anfordern (Artikel 15 Abs. 3 NIS-RL). Die Einhaltung der Sicherheitsanforderungen kann das BSI gemäß § 8a Abs. 4 BSIG selbst durch Dritte überprüfen (Artikel 15 Abs. 2 NIS-RL).

Das BSI sammelt Informationen und wertet sie aus. Nach § 8b Abs. 2 BSIG hat es die Auswirkungen zu analysieren, ein Lagebild zu erstellen und unverzüglich die Kritis-Betreiber und Behörden zu unterrichten. Eine generelle Unterrichtung der Öffentlichkeit sieht das Gesetz nicht vor.

Durch diese Informationen der Kritis-Betreiber können zivilrechtliche **Verkehrssicherungspflichten** durch das BSI ausgelöst werden, weil Betreiber *„quasi bösgläubig“* werden und dadurch unverzüglich ihre technische und organisatorische Vorkehrungen überprüfen und Schutzmaßnahmen veranlassen müssen.[76] Die Anbieter von digitalen Diensten, die Anbieter von Software, haben dann Verkehrssicherungspflichten, wenn sich IT-Sicherheitslücken zeigen, die sie durch Update-Pflichten beseitigen müssen. Trotz dem Ende der Gewährleistungshaftung treffen den Anbieter Verkehrssicherungspflichten für die von ihm in den Verkehr gebrachte Software auch außerhalb der vertraglichen Pflichten. Dem Anbieter digitaler Dienste in Form einer Software sind Vorkehrungen zum Schutz der Rechtsgüter Dritter zumutbar. Der Anbieter muss die Software, die er in Verkehr gebracht hat, auch danach noch auf Sicherheitslücken und Risiken hin beobachten. Die deliktische Verkehrssicherungspflichten schützen das Integritätsinteresse. Der Anbieter muss den Nutzer vor Schäden bewahren, was auch durch eine Warnung möglich ist, durch die der Nutzer in die Lage versetzt wird, die Nutzung einzustellen.[77] Nach § 8c Abs. 4 BSIG kann das BSI von dem Anbieter digitaler Dienste verlangen, erforderliche Informationen zur Beurteilung der Sicherheit seiner Netz-Informationssysteme einschließlich der Nachweise über ergriffene Maßnahmen zu erbringen.

(19) Präventive Befugnisse des BSI gegenüber Herstellern von IT-Diensten und IT-Produkten

Nach § 7a BSIG hat das BSI das Recht auf dem Markt angebotene IT-Dienste und IT-Produkte zu untersuchen, und zwar auch gegen den Willen des jeweiligen Herstellers. Das gilt insbesondere, wenn Bedenken gegen Produkte bestehen, die in der kritischen Infrastruktur eingesetzt werden.[78]

Nach § 8b Abs. 6 BSIG kann das BSI Hersteller und IT-Dienste dazu verpflichten, bei der Vermeidung von Störungen der kritischen Infrastruktur mitzuwirken. Zu den Befugnissen des BSI gehört nach § 9 Abs. 2 BSIG auch Produkte und Dienste von BSI zertifizieren zu lassen.

(20) Die Organisation der IT-Sicherheit im Unternehmen

Die IT-Sicherheit muss nach den BSIG in Unternehmen organisiert werden. Die sechs Organisationspflichten eines Compliance-Management-Systems sind auch auf die Organisation der IT-Sicherheit anzuwenden. Das BSI hat sich zur Organisation konkret geäußert und sogenannte Bausteine *„ORP.1“* zur Organisation herausgegeben. Die sechs Organisationspflichten nämlich das Ermitteln der Risiken und der Pflichten zur Risikoabwehr, die Delegation der Pflichten auf Mitarbeiter des Unternehmens und die Festlegung der jeweiligen Funktionen als Geschäftsleiter,

76 Spindler, CR 2016, S. 308.

77 Kipker/Wiegand, S. 217.

78 Schallbruch, CR 2018, S. 215, 218; Wimmer/Meschler, S. 136.

Beauftragte und Erfüller, die Kontrollen und die Dokumentation finden sich in den vom BSI veröffentlichten Bausteinen wieder.

Zur allgemeinen Organisationspflicht äußert sich das BSI im Baustein *„ORP.1"* mit dem Titel *„Organisation"*. Allgemeine Anforderungen im Bereich der Organisation werden formuliert, um das Niveau der Informationssicherheit zu erhöhen und zu erhalten. Unter 2.1 wird in dem Baustein *„Organisation"* verlangt, mit organisatorischen Regelungen Sicherheitslücken zu vermeiden. Nach 2.2 sind die geltenden Regelungen allen Mitarbeitern bekannt zu machen und zur Verfügung zu stellen, sodass sie von allen Betroffenen im Arbeitsalltag gelebt werden können. Diese Vorgaben entsprechen der Organisationspflicht der Delegation von Pflichten auf Mitarbeiter im Unternehmen. Unter Ziffer 3 wird die Erfüllung der Anforderungen, das heißt der Pflichten zur IT-Sicherheit, als Organisationspflicht vorgeschrieben. Dem Informationssicherheitsbeauftragten wird die Rolle zugeschrieben, die Erfüllung aller Pflichten zur IT-Sicherheit zu überwachen. Unter ORP.1.1a wird die Festlegung von Verantwortlichkeiten und Regelungen verlangt. Dies entspricht der allgemeinen Organisationspflicht der Delegation nach ORP.1.1a.4. Vorgegeben wird die Trennung von unvereinbaren Aufgaben und Funktionen in der Organisation. Dies entspricht der Trennung zwischen Mitarbeitern mit Linienfunktion zur Entscheidung und Stabsfunktion zur Kontrolle. Diese Funktionstrennung ist zu dokumentieren. Auch dieser Hinweis entspricht der allgemeinen Organisationspflicht zur Delegation unterschiedlicher Pflichten auf unterschiedliche Mitarbeiter, damit im Ergebnis Mitarbeiter mit Linienfunktion die Erfüllung ihrer Pflichten nicht selbst kontrollieren.

(21) Die digitale Kreuzreferenztabelle

Gefordert wird von der Organisation die Anlage einer *„Kreuzreferenztabelle zu elementaren Gefährdungen"*. In ihr sollen elementare Gefährdungen den Anforderungen zugeordnet werden, damit ermittelt werden kann, welche der elementaren Gefährdungen durch welche Anforderungen, d.h. durch welche Sicherheitsmaßnahmen abgewendet werden können. Das BSI trennt erkennbar zwischen der Ermittlung von Risiken und den Pflichten zur Abwendung dieser Risiken und verlangt, ein Zusammenhang zwischen Risiko und Pflicht zur Risikoabwendung herzustellen. Die Forderung nach der *„Kreuzreferenztabelle zur elementaren Gefährdungen"* findet sich ebenfalls in Baustein ORP.5 Compliance-Management (oder Anforderungsmanagement) unter Ziffer 5 als auch in Baustein DER.1.: *„Detektion von sicherheitsrelevanten Ereignissen"* ebenfalls unter Ziffer 5. Zur Veranschaulichung ist als Anlage eine Matrix beigefügt, die in der horizontalen oberen Leiste die Gefährdungen auflistet und in der vertikalen Leiste die Anforderungen zur Abwendung der jeweiligen Gefährdung. Eine derartige Matrix ist in ihrer Funktionsweise begrenzt und kaum praktikabel, weil sie nur eine bestimmte Anzahl von Risiken und Pflichten zur Abwehr aufnehmen kann. Es empfiehlt sich eine digitale Kreuzreferenztabelle, in der konkrete Risiken mit konkreten Pflichten digital so verlinkt werden, dass für jedes IT-Sicherheitsrisiko die entsprechenden Schutzmaßnahmen zur Risikoabwehr jederzeit abgerufen werden kann. Eine digitalisierte Kreuzwerttabelle ist geeignet, Risiken in unbegrenzter Anzahl zu erfassen und mit den jeweils geeigneten Schutzpflichten so zu verlinken, dass alle in einem Unternehmen beteiligten Mitarbeiter jederzeit Zugriff auf diese Datenbank haben. Im Unternehmen lässt sich von jedem Mitarbeiter jederzeit ermitteln, erstens welcher IT-Sachverhalt ein Risiko darstellt und zweitens mit welcher Schutzpflicht dieses Risiko abzuwenden ist. Entsprechend der Rechtsprechung des BGH zur Wissensaufspaltung[79] sind alle Mitarbeiter eines Unternehmens dadurch in der Lage, sich das erforderliche Wissen zu Risiken über die IT-Sicherheit und die jeweilige Schutzmaßnahme abzurufen.[80]

79 GHZ 132, 30 - BGH, 2.2.1996 – V ZR 239/94, NJW 1996, 1339 (Wissensaufspaltungsentscheidung); BGHZ vom 15.04.1997, BGHZ 135, 202, XI ZR 105/96 (Scheckinkasso).

80 Eine digitale Kreuzreferenztabelle bietet das Compliance-Management-System „Recht im Betrieb".

(22) Die Vorgaben des BSI zum Compliance-Management (Anforderungsmanagement) nach ORP.5.

Die Einhaltung aller rechtlichen Vorgaben zur Informationssicherheit ist durch die Unternehmensleitung sicherzustellen (1.1). Aus gesetzlichen Vorgaben sind die Sicherheitsanforderungen abzuleiten. Unter 3 (*„Anforderungen"*) wird im Baustein festgestellt, dass Compliance-Manager für die Erfüllung der Anforderung zuständig ist und der Informationssicherheitsbeauftragte bei Entscheidungen stets einzubeziehen ist.

Nach ORP.5.A1 sind alle relevanten gesetzlichen, vertraglichen und sonstige Vorgaben zu identifizieren, die Auswirkungen auf die Informationssicherheit haben können. Nach ORP.5.A2 haben die Leiter der Organisationen für die Einhaltung der rechtlichen Vorgaben zu sorgen. Alle Mitarbeiter müssen in die einschlägigen Gesetze eingewiesen und verpflichtet werden, diese einzuhalten. Den Mitarbeitern muss bekannt sein, welcher *„rechtliche Rahmen ihre Tätigkeit bestimmt"*. Nach ORP.5.A8 ist das Compliance-Management regelmäßig auf Angemessenheit zu überprüfen. In Ziffer 5 wird ebenfalls eine Kreuzreferenztabelle vorgeschrieben. Die digitale Kreuzreferenztabelle lässt sich insofern erweitern, als mit jeder Pflicht auch die Mitarbeiter namentlich verlinkt werden können, die die jeweilige Pflicht zur Gewährleistung der IT-Sicherheit erfüllen, welcher Mitarbeiter die Erfüllung unabhängig kontrollieren muss und welcher Geschäftsleiter die Oberaufsicht über die Erfüllung und deren Kontrolle zu verantworten hat.

(23) Die Detektion von sicherheitsrelevanten Ereignissen

Das BSI hat in seinem Bausteinen DER.1 als organisatorische Maßnahmen das rechtzeitige Erfassen sicherheitsrelevanter Ereignisse vorgeschrieben. Dabei handelt es sich um ein Ereignis, dass sich auf die Informationssicherheit auswirkt und die Vertraulichkeit, Integrität und Verfügbarkeit beeinträchtigen kann. Typische Folgen solcher Ereignisse sind ausgespähte, manipulierte oder zerstörte Informationen. Die Ursachen sind vielfältig. Um die IT-Systeme schützen zu können, fordert das BSI sie rechtzeitig zu erkennen.

Im Rahmen des Compliance-Management-Systems handelt es sich hierbei um die Ermittlung aller riskanten Sachverhalte. Zu bedenken ist dabei, dass es sich um Risiken handeln, die erst dann zu erkennen sind, wenn sie sich zum Schaden entwickelt haben. Risiken sind keine Fakten, sondern Fiktionen, die nicht zu erkennen sind, die man sich denken muss. Das Erfassen von Risiken setzt Erfahrungen mit IT-Arbeitsverläufen voraus. Vor dem Schadenseintritt können Risiken allenfalls anhand von Indizien erfasst werden, von denen aufgrund eines Erfahrungssatzes auf ein Risiko geschlossen werden kann, weil schon einmal die Erfahrung über den Eintritt eines Schadens gemacht werden konnte. Im IT-Sicherheitsrecht ist der Schaden an den drei Schutzgütern der Vertraulichkeit, der Integrität und der Verfügbarkeit der Informationen abzuwenden. Die ständige BGH-Rechtsprechung legt strenge Maßstäbe bei der Risikoanalyse an. Sogar Risiken ohne erkennbare Indizien sind zu erfassen.[81]

Zielgerichtete Cyberangriffe nutzen die Überraschung mit dem Einsatz neuer unbekannter Angriffstechniken. Die erfolgreiche Detektion sicherheitsrelevanter Ereignisse setzt die Simulation von Angriffstechniken im Rahmen der Cyberkriminalität voraus. Für eine erfolgreiche Abwehrstrategie muss gefordert werden, sämtliche Erfahrungen über Angriffe und Störungen der IT-Sicherheit systematisch zu sammeln und für jedermann zugänglich und verfügbar bereitzustellen. Diese Zielsetzung wird unter Ziffer 1.2 des Bausteins DER.1. formuliert. Von großer Bedeutung ist deshalb das Protokollieren aller Angriffe und Störungen, womit sich der Baustein OPS.1.1.5 *„Protokollierungen"* befasst.

81 RG v. 14.12.1911 (VI 75/11), in: RGZ 78 S. 107 [Kutscher-Urteil]; RG v. 25.02.1915 (VI 526/14), in: RGZ 87 (1916) S. 1 [Heilsalz-Urteil]; BGH v. 25.10.1951 (III ZR 95/50), in: BGHZ 4 S. 1 [Benzinfahrt-Urteil]; BGH v. 04.11.1953 (VI ZR 64/52), in: BGHZ 11 S. 151 [Zinkdach-Urteil]; BGH v. 13.05.1955 (I ZR 137/53), in: BGHZ 17 (1955) S. 214 [Bleiwaggon-Urteil]; BGH v. 09.02.1960 (VIII ZR 51/59), in: BGHZ 32 (1960) S. 53 [Besitzdiener-Urteil]; BGH v. 08.11.1963 (VI ZR 257/62), in: VersR 1964, S. 297 [LKW-Unfall-Urteil]; BGH v. 17.10.1967 (VI ZR 70/66), in: NJW (1968) S. 247 ff. [Schubstreben-Fall]; BGH v. 20.04.1971 (VI ZR 232/69), in: NJW 1971 (1971) S. 1313 [Tiefbau-Unternehmer-Urteil]; BGH JZ 1978 (1978) S. 475 [Kfz-Werkstatt-Urteil].

Zur Abwehr sicherheitsrelevanter Ereignisse sind Programme zum Beispiel Antivirenprogramme, Firewalls oder Intrusions-Detections-Systems (IDS/IPS) erforderlich, um Anomalien im Datenverkehr aufzudecken. Die Mitarbeiter sind ausreichend zu sensibilisieren und zu schulen, um sicherheitsrelevante Ereignisse als solche zu identifizieren, um denkbare Angriffe möglichst frühzeitig zu erkennen und von Indizien auf die drohenden Angriffe zu schließen. Die Informationssicherheitsbeauftragten haben die Aufgabe, wichtige Auffälligkeiten zu sammeln, darauf hinzuweisen und sie als Indizien für drohende Angriffe zu beschreiben. Alle Abweichungen vom Normalbetrieb der IT-Systeme müssen einen Verdacht auf Angriffe und Störungen begründen. Wird ein IT-System im Ablauf langsamer, kann dies ein Indiz für ein im Hintergrund aktives Schadprogramm sein. Eine Abweichung vom Normalbetrieb sind auch die Anzeigen von ungewöhnlichen Werten bei der Steuerungen von Produktionsanlagen. Sie sind Indizien, die einen Verdacht begründen. Die im BSI gesammelten Meldungen und Erfahrungen sind zugänglich zu machen und von einem Informationssicherheitsbeauftragten zu nutzen.

Neben dem Erfassen der IT-Risiken und den Pflichten zur Abwendung dieser Risiken wird in DER.1.A2 die Einhaltung aller relevanten gesetzlichen Bestimmungen gefordert. Die IT-Sicherheit als Gesetzeszweck enthalten 324 Gesetze, die insgesamt etwa 500 Pflichten vorgeben. Mit erfasst sind dabei die Regelungen in Spezialgesetzen wie dem Atomgesetz, dem Energiewirtschaftsgesetz, dem Telekommunikationsgesetz und dem Telemediengesetz.

(24) Das System zur Meldung von sicherheitsrelevanten Ereignissen

Gefordert wird unter DER.1.A3 (Detektion von sicherheitsrelevanten Ereignissen) die Festlegung von Meldewegen für sicherheitsrelevante Ereignisse.

Das Compliance-Management-System *„Recht im Betrieb“* enthält ein Meldesystem, mit dem Informationen von der Arbeitsebene zentral an eine dafür vorbestimmte Stelle gemeldet werden können. Dabei können vordefinierte Meldetypen bestimmt werden, mit denen die sicherheitsrelevanten Ereignisse unternehmensintern gesammelt und gemeldet werden können. Alle Mitarbeiter sind zu verpflichten, jeden individuell erkannten Sicherheitsvorfall und –verdacht unverzüglich dem Incident-Management zu melden. Hervorzuheben ist außerdem die im Baustein DER.1.1A11 enthaltene Anforderung, eine zentrale Protokollierungsinfrastruktur für die Auswertung sicherheitsrelevanter Ereignisse zu unterhalten. Die Ereignismeldungen sind zentral zu speichern und auszuwerten, um abgerufen werden zu können. Die gesamten Ereignisse von Auffälligkeiten müssen nachträglich erkannt werden können, immer aktuell und auf dem gleichen Stand sein. Unter DER.1.1A12 wird die Pflicht formuliert, Informationen aus externen Quellen zu sammeln und auszuwerten. Diese entspricht der BGH-Rechtsprechung im IKB-Urteil, alle verfügbaren Informationsquellen bei der Risikoanalyse zu erschöpfen.[82] Unter Ziffer 5 wird wiederum eine Kreuzreferenztabelle gefordert, in die Risikosachverhalte zu speichern und mit Pflichten zur Risikoabwehr zu verlinken sind. In digitaler Form kann so der gesamten Erfahrungsschatz zu sicherheitsrelevanten Ereignissen zentral sammelt und für alle einsehbar verfügbar gehalten werden. Diese organisatorische Pflicht entspricht den Vorgaben der Rechtsprechung des BGH in der Wissensaufspaltungsentscheidung.[83]

Die Sammlung aller Erfahrungen zu IT-Risiken und deren Abwehr durch Schutzmaßnahmen lässt sich auf einer Plattform organisieren. Je mehr Nutzer das gleiche Compliance-Management-System mit der von allen gespeisten Datenbank über typische Risiken in der IT-Sicherheit nutzen, umso erfolgreicher lässt sich die Cyberrisiko-Abwehr organisieren. Die Erfahrung über IT-Risiken müssen gesammelt, gespeichert und abrufbar verfügbar gehalten werden, und zwar nicht nur im eigenen Unternehmen sondern im Verbund aller potenziell betroffenen Cyberangriffsopfer. Um dieses Ziel zu erreichen, empfiehlt es sich, die Kreuzreferenztabelle ständig um aktuelle Erfahrungen über Angriffs- und Abwehrtechniken zu erweitern und allen betroffenen Nutzern zugänglich zu machen.

Wenn das IT-Grundschutzkompendium des BSI nur

82 BGH, Urteil v. 13.12.2011 - XI ZR 51/10 (IKB-Urteil).

83 GHZ 132, 30 - BGH, 2.2.1996 – V ZR 239/94, NJW 1996, 1339 (Wissensaufspaltungsentscheidung); BGHZ vom 15.04.1997, BGHZ 135, 202, XI ZR 105/96 (Scheckinkasso).

einmal pro Jahr aktualisiert wird, dürfte dieser zeitliche Abstand zu groß sein und die Gefahr erhöhen, dass Cyberkriminelle ihren technischen Vorsprung beim Angriff ausbauen und die Abwehrtechnik nachhängt.

(25) Die Vorteile einer ständig aktualisierten Kreuzreferenztabelle als digitales Gedächtnis

Für die Organisation der IT-Sicherheit im Unternehmen ist der Einsatz digitaler Instrumente unverzichtbar. Die Sammlung aller sicherheitsrelevanten Sachverhalte eines Unternehmens in einer Datenbank ermöglicht den schnellen Zugriff auf alle Indizien, von denen schon einmal ein Risiko für die IT-Sicherheit des Unternehmens ausgegangen ist. Die gespeicherten Erfahrungen erlauben als Indizien Schlüsse auf drohende Angriffe und Störfälle. Es sind die aus Erfahrung gesammelten Abweichungen vom Normalbetrieb der IT-Praxis. Eine Sammlung kann als digitales Gedächtnis für alle Mitarbeiter eines Unternehmens dienen, die schon arbeitsrechtlich verpflichtet sind, auf alle Auffälligkeiten und Risiken hinzuweisen, die einen Schaden im Unternehmen auslösen können. Die Unternehmensleitung ist darauf angewiesen, dass sämtliche Mitarbeiter zum Schutz der IT-Sicherheit Unregelmäßigkeiten nicht nur erfassen, sondern auch unverzüglich melden. Die digitale Kreuzreferenztabelle erlaubt außerdem den schnellen Zugriff auf die Schutzmaßnahmen, die in der Datenbank gespeichert sind und mit dem jeweiligen IT-Risiko verlinkt sind.

Die Datenbank ist für alle Mitarbeiter verfügbar und kann als zentrales Frühwarninstrument eingesetzt werden. Nicht allein der IT-Sicherheitsbeauftragte kann die IT-Sicherheit garantieren. Er ist auf die Aufmerksamkeit aller Mitarbeiter angewiesen und vor allem auf deren Meldebereitschaft bei potenziellen Gefahren für die IT-Sicherheit.

Die Kreuzreferenztabelle ist zu ergänzen um alle Pflichten zur Abwehr der erfassten Risiken. Die Pflichten ergeben sich aus dem Grundschutzkompendium des BSI als Mindestanforderung.

(26) IT-Compliance und IT-Sicherheit als Organisationspflicht der Unternehmensleitung

Zur Organisation verpflichtet sind Geschäftsführer und Vorstände. Sie haften für Fehler und verletzte Organisationspflichten. Der durch das KontraG eingeführte § 91 Abs. 2 AktG schreibt vor, dass der Vorstand, als Teil seiner Verpflichtung zur ordentlichen und gewissenhaften Geschäftsführung geeignete Maßnahmen zur rechtzeitigen Erkennung von Sicherheitsrisiken zu treffen hat. Vorstände haben die Pflicht, ein angemessenes Risiko-Management zu implementieren. Alle Mitglieder des Vorstands sind dazu verpflichtet. Zur üblichen Sorgfalt gehört bei der Unternehmensleitung auch das Ermitteln und Abwehren von IT-Risiken. Die IT-Sicherheit ist ein bedeutender Bestandteil des Ressourcenschutzes und der betrieblichen Vermögensgegenstände und zählt als wichtiger Teil zur allgemeinen Organisationspflicht.[84]

Zu Recht wird empfohlen, einen IT-Sicherheitsbeauftragten als Stabsstelle zu etablieren und nicht als Teil der IT-Abteilung, da deren Interessen und Ziele sich nicht immer mit den Aufgaben des IT-Sicherheitsbeauftragten decken. Der IT-Sicherheitsbeauftragte hat vergleichbar mit den gesetzlichen Beauftragten im Umweltschutz und Arbeitsschutz die Aufgabe, den Betreiber zu beraten, die Mitarbeiter über Pflichten zur IT-Risikoabwehr zu informieren und deren Einhaltung zu kontrollieren. Wäre der IT-Sicherheitsbeauftragte innerhalb der IT-Abteilung angesiedelt, würde er sich selbst kontrollieren. Auch im IT-Sicherheitsrecht empfiehlt es sich deshalb, Stabs- und Linienfunktionen zu trennen und den IT-Sicherheitsbeauftragten von der Pflicht, Entscheidungen zur IT-Sicherheit zu treffen, zu entbinden und ihn auf die Berater-, Informations- und Kontrollfunktion zu beschränken.[85]

84 Schmidt/Tannen, in: Kipker, Cybersecurity, 2020, S. 181.

85 Schmidt/Tannen, in: Kipker, Cybersecurity, 2020, S. 192.

RACK
RECHTSANWÄLTE

Lurgiallee 12 (Mertonviertel) - 60439 Frankfurt am Main - Fon 0 69/95 78 31 0 - Fax 0 69/95 78 31 40
Email anwaltsbuero@rack-rechtsanwaelte.de - www.rack-rechtsanwaelte.de

RACK
RECHTSANWÄLTE • NOTARE

ALLES AUS EINER HAND

Rechtsinhalte, Software & präventive Rechtsberatung

Nutzen Sie unsere gespeicherten **Erfahrungen aus 29 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 wir den 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: 19.000 Rechtsvorschriften von EU, Bund, Ländern und Berufsgenossenschaften, 8.200 Gerichtsurteile, standardisierte Pflichtenkataloge für 45 Branchen und 62.000 vorformulierte Betriebspflichten. **46.000 Unternehmensrisiken sind mit 62.000 Rechtspflichten 3,3 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