medien und recht

Zeitschrift für Medien- und Kommunikationsrecht

4/23

41. Jahrgang/August 2023

MUR

von **Christoph Reiter / Roman Heidinger / Philipp Gstrein**

Die NIS2-Richtlinie: Von Cybersicherheit und Haftung

Die NIS2-Richtlinie „über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union", Richtlinie (EU) 2022/2555, die bis Oktober 2024 in nationales Recht umgesetzt werden muss, bringt nicht nur verschärfte Regelungen für Unternehmen im Bereich der Cybersicherheit, sondern auch deutlich höhere Strafrahmen. Neben einem Überblick soll der vorliegende Artikel auch schon erste Handlungsempfehlungen für die Anpassung an die neuen Vorschriften bieten.

1. Einleitung

Aktuelle Entwicklungen, wie insbesondere der Konflikt in der Ukraine und damit verbundene Störungen der Lieferketten, haben das Augenmerk nationaler und europäischer politischer Akteure wieder verstärkt auf die Bedeutung widerstandsfähiger und zuverlässiger Netz- und Informationssysteme gelenkt.[1]) Die Relevanz diesbezüglicher Gesetzgebungsvorhaben zeigt sich für Österreich etwa plakativ anhand der Tatsache, dass laut einer Studie 32 % der befragten Unternehmen schon Opfer von Cyberangriffen waren.[2]) Angesichts der zunehmenden Komplexität und Häufigkeit derartiger Bedrohungen reagiert der europäische Gesetzgeber mit der NIS2-Richtlinie[3]) auf die sich wandelnde Risikolage und erkennt die dringende Notwendigkeit an, die Cybersicherheit in Europa durch ergänzende Regulierung weiter zu stärken. Mit der Umsetzung der Richtlinie, welche am 16. Jänner 2023 in Kraft getreten ist, muss in Österreich bis spätestens 17. Oktober 2024 gerechnet werden.

2. NIS1-Richtlinie und deren Umsetzung in Österreich

Die NIS1-Richtlinie[4]) konstituierte im Jahr 2016 erstmalig einen rechtsverbindlichen Rahmen für die Etablierung eines vereinheitlichten Sicherheitsniveaus für Netz- und Informationssysteme von Betreibern sog wesentlicher Dienste innerhalb der EU und präzisierte essenzielle Maßnahmen zur Verstärkung der Cyberabwehrkapazitäten der Mitgliedstaaten sowie zur Förderung der kooperativen Zusammenarbeit auf europäischer Ebene.

In den Anwendungsbereich der NIS1-Richtlinie fallende Unternehmen (insbesondere in den Sektoren Energie, Verkehr, Bankwesen, Finanzmarktinfrastrukturen, Gesundheitswesen, Trinkwasserversorgung und Digitale Infrastruktur) haben die Pflicht zur Implementierung von IT-bezogenen Sicherheitsmanagementsystemen sowie zur Erstellung, Umsetzung und Kontrolle der Einhaltung von Sicherheitsrichtlinien für betriebsnotwendige Teile der durch sie betriebenen, kritischen Infrastruktur.

Das Regelungskonzept der NIS1-Richtlinie stieß in der Vergangenheit immer wieder auf umfangreiche kritische Resonanz, insbesondere im Hinblick auf das bisweilen weiterhin nur unzureichende Niveau der Cybersicherheit in gesellschaftlich bedeutsamen Wirtschaftszweigen sowie die oftmals erheblich divergierende Implementierung der Richtlinie in den Mitgliedstaaten.[5]) In einer Evaluation der NIS1-Richtlinie führt die Europäische Kommission[6]) etwa das Gesundheitswesen als konkretes Beispiel für wesentlich unterschiedliche Standards der Cybersicherheit in der Europäischen Union (EU) an: So fallen beispielsweise in einem Mitgliedstaat bestimmte große Krankenhäuser nicht unter die Umsetzung der NIS1-Richtlinie und müssen folglich die entsprechenden Sicherheitsmaßnahmen nicht ergreifen, während die NIS-Sicherheitsanforderungen in einem anderen Mitgliedstaat für nahezu alle Krankenhäuser gelten.

Die NIS1-Richtlinie wurde in Österreich im Jahr 2018 durch das NISG implementiert. Dieses kodifizierte die nationalen Regelungen zur Operationalisierung der NIS1-Richtlinie und etablierte auf diesem Wege einen richtlinienkonformen, rechtlichen Rahmen für den Schutz kritischer Netz- und Informationssysteme in Österreich. Ergänzende, sektorspezifische Regeln zur IT-Sicherheit sind in diversen Materiengesetzen wie dem Telekommunikationsgesetz (TKG),[7]) der Datenschutz-Grundverordnung (DSGVO)[8]) und dem Sicherheitspoli-

Mag. Christoph Reiter ist Rechtsanwalt und Partner, **Dr. Roman Heidinger, M.A.** ist Rechtsanwalt bei der CERHA HEMPEL Rechtsanwälte GmbH in Wien. **Philipp Gstrein** ist juristischer Mitarbeiter in genannter Kanzlei.

1) *Voigt/Bastians*, Neue europarechtliche Anforderungen an die IT-Sicherheit, CR 2022, 768.

2) *Steinbrenner*, „Die Presse am Sonntag", 2.7.2023.

3) Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS-2-Richtlinie), ABl L 333 vom 27.12.22, 80.

4) Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union, ABl L 194 vom 19.7.2016, 1.

5) *Wegmann*, Too much of a good thing? Erweiterung und Verschärfung von Cybersicherheitspflichten durch die NIS2 – Richtlinie, BB 2023, 835.

6) Folgenabschätzung zur Überprüfung der Richtlinie (EU) 2016/1148 vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union, SWD (2020) 344 final vom 16.12.2020.

7) Vgl § 44, § 45, § 46, § 47 sowie § 163 TKG.

8) Vgl Art 5 iVm Art 32 sowie Art 33 DSGVO.

zeigesetz (SPG) zu finden.[9]) Alle diese Rechtsinstrumente enthalten mehr oder minder detaillierte Vorgaben zu Detailfragen des Schutzes von Netz- und Informationssystemen sowie zur Meldung und dem konkreten Vorgehen bei Bezug habenden Sicherheitsvorfällen.

3. Die NIS2-Richtlinie

3.1. Einführung

Im Rahmen der neu aktualisierten EU-Cybersicherheitsstrategie wurde am 16. Dezember 2020 ein Entwurf der NIS2-Richtlinie von der Europäischen Kommission[10]) vorgelegt, welche ihrerseits die bislang geltende NIS1-Richtlinie ablösen soll. Die NIS2-Richtlinie ist bis zum 17. Oktober 2024 in nationales Recht umzusetzen. Generell kann folglich davon ausgegangen werden, dass auch in Österreich das seinerzeit eigens hierfür geschaffene NISG bis zum genannten Datum entsprechend den Anforderungen der neuen NIS2-Richtlinie adaptiert werden wird.

Die NIS2-Richtlinie bringt eine Vielzahl von Neuerungen mit sich, welche unter anderem erweiterte Anforderungen an den Schutz von Netz- und Informationssystemen – gepaart mit einer deutlichen Ausdehnung des Umfangs der konkret als kritisch eingestuften IT-Infrastruktur –, klare Vorgaben hinsichtlich der Meldung von etwaigen Sicherheitsvorfällen sowie eine besser strukturierte Zusammenarbeit zwischen den Behörden und zuständigen Stellen der Mitgliedstaaten untereinander umfassen. Darüber hinaus werden auf einheitlichen Sicherheitsstandards basierende Zertifizierungen und Sicherheitsaudits eingeführt.

Im Vergleich zur NIS1-Richtlinie, welche seinerzeit noch eine Unterscheidung zwischen Betreibern wesentlicher Dienste und Anbietern digitaler Dienste vorgenommen hat, differenziert die NIS2-Richtlinie nun zwischen wesentlichen und wichtigen Einrichtungen.[11])

3.1.1. Verhältnis zu anderen EU-Rechtsnormen

Die NIS2-Richtlinie ist ihrerseits integraler Bestandteil einer größeren politischen Initiative zur Verbesserung der Cybersicherheit und zum Schutz kritischer IT-Infrastrukturen in der EU[12]). Relevant sind allen voran folgende Rechtsakte:

a. Der Digital Operational Resilience Act (DORA)[13]), welcher zum Ziel hat, den Finanzsektor vor Bedrohungen durch Angriffe auf digitale Infrastruktur zu schützen und die operative Widerstandsfähigkeit der betroffenen Marktteilnehmer zu stärken. In diesem Sinne stellt DORA eine *lex specialis* zur NIS2-Richtlinie dar.[14])
b. Der Cyber Resilience Act (CRA)[15]), welcher darauf abzielt, das Sicherheitsniveau bei Produkten mit digitalen Elementen zu steigern. Solche Produkte weisen nämlich häufig ein zu geringes Maß an Cybersicherheit auf, insbesondere weil sie keinen regelmäßigen Updates unterzogen werden.[16]) Unter die Regelung fallen beispielsweise Password-Manager, Router und industrielle Geräte für das Internet of Things (IoT).[17]) Der CRA unterwirft sog „economic operators" – also insbesondere Hersteller, Importeure sowie Händler von Produkten mit digitalen Elementen – umfangreichen Update-, Melde- und korrespondierenden Vorsorge- und Schutzpflichten, wie zum Beispiel auf Durchführung eines Konformitätsbewertungsverfahrens.[18])
c. Die DSGVO, konkret deren Art 32, welcher Bestimmungen zur Datensicherheit durch geeignete technische und organisatorische Maßnahmen enthält. Der Anwendungsbereich dieser Bestimmung ist aber auf Datensicherheitsmaßnahmen zum Schutz personenbezogener Daten iSd Art 4 Z 1 DSGVO beschränkt. Damit ist der Anwendungsbereich wesentlich enger als jener der NIS2-Richtlinie. Datenlecks oder Zerstörung bloßer Steuerungsdaten sowie unbefugter Zugriff auf Computersysteme, auf denen keine personenbezogenen Daten gespeichert sind, unterliegen etwa keiner Regelung durch die DSGVO. Einen Beitrag zur allgemeinen Cybersicherheit und zum Schutz gesamtgesellschaftlicher Interessen leistet die DSGVO somit allenfalls nur als Reflex.[19])

3.2. Erweiterung des Anwendungsbereichs der NIS2-Richtlinie

In den Anwendungsbereich der NIS2-Richtlinie fallen nach Art 2 Abs 1 öffentliche und private Einrichtungen mit Tätigkeit in einem der im Anhang I bzw II der Richtlinie genannten Sektoren und Sitz in der EU, soweit sie

9) Vgl § 22 Abs 1 Z 6 SPG.
10) Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union und zur Aufhebung der Richtlinie (EU) 2016/1148 vom 16.12.2020, COM (2020) 823 final.
11) *Voigt/Bastians* (FN 1), 769. Zu den Unterscheidungsmerkmalen wesentlicher und wichtiger Einrichtungen siehe sogleich weiter unten, Punkt 3.3.
12) *Kipker*, Chefsache Cybersicherheit: NIS-2 ist da, EuZW 2023, 249-250.
13) Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über die digitale operationale Resilienz im Finanzsektor und zur Änderung der Verordnungen (EG) 1060/2009, (EU) 648/2012, (EU) 600/2014, (EU) 909/2014 und (EU) 2016/1011, OJ L 333 vom 27.12.2022.
14) *Dittrich/Heinelt*, Der Europäische DORA – neue Sicherheitsvorgaben für den Finanzsektor, RDi 2023, 164, 165; *Voigt/Ritter-Döring*, Der Digital Operational Resilience Act – Sektorspezifische Anforderungen an die digitale Resilienz von Finanzunternehmen, CR 2023, 82, 89.
15) Vorschlag für eine VO über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen und zur Änderung der Verordnung (EU) 2019/1020, COM (2022) 454 final vom 15.9.2022.
16) *Voigt/Falk*, Der Cyber Resilience Act, MMR 2023, 88.
17) Die erfassten Produktkategorien sind Anhang III des Vorschlags (FN 15) zu entnehmen.
18) *Voigt/Falk* (FN 16), 91 mwN.
19) *Wegmann* (FN 5), 836.

zumindest als mittlere Unternehmen[20]) gelten. Die Größenschwelle eines mittleren Unternehmens unterschreiten Einrichtungen, die weniger als 50 Mitarbeiter beschäftigen und deren Jahresumsatz oder Jahresbilanzsumme 10 Mio. EUR nicht übersteigt.

In bestimmten Ausnahmefällen, welche in Art 2 Abs 2 bis 5 festgelegt sind, gilt die NIS2-Richtlinie allerdings unabhängig von der Unternehmensgröße. Diese Ausnahmen sind detailliert geregelt (allein Abs 2 enthält sechs *literae* zuzüglich diverser Untergliederungen) und betreffen beispielsweise Dienste in den Bereichen der öffentlichen elektronischen Kommunikation oder monopolartige Anbieter von Diensten in gesellschaftlich oder ökonomisch kritischen Tätigkeitsbereichen.

Im Hinblick auf die erfassten Netzwerk- und Informationssysteme ist der Anwendungsbereich der NIS2-Richtlinie deutlich weiter als jener der NIS1-Richtlinie:

So wird in Erwägungsgrund 22 der NIS1-Richtlinie noch explizit darauf verwiesen und anerkannt, dass von der NIS1-Richtlinie erfasste Einrichtungen neben wesentlichen auch nicht wesentliche Dienste erbringen können. Dementsprechend normiert § 17 Abs 1 NISG, dass Betreiber wesentlicher Dienste Sicherheitsvorkehrungen nur in Hinblick auf jene Netz- und Informationssysteme zu treffen haben, die sie für die Bereitstellung des wesentlichen Dienstes nutzen. Die Verpflichtung eines Flughafens beschränkt sich daher beispielsweise auf Bereiche wie etwa das Start- und Landebahn-Management, nicht jedoch auf IT-Systeme in Einkaufsbereichen.[21]) Eine vergleichbare Einschränkung fehlt in der NIS2-Richtlinie. Dies wird dahingehend interpretiert, dass nach der neuen Rechtslage keine Unterscheidung zwischen wesentlicher und nicht-wesentlicher IT-Infrastruktur mehr möglich sein soll, sondern vielmehr sämtliche Netz- und Informationssysteme richtlinienunterworfener Einrichtungen gesamtheitlich in den Anwendungsbereich von NIS2 einbezogen sind.

Im Hinblick auf Art und Ausmaß der erforderlichen Maßnahmen zur Risikominimierung[22]) wird die Wichtigkeit des betroffenen Teils eines Netz- und Informationssystems für die vom jeweiligen Unternehmen betriebenen Dienste aber sehr wohl eine Rolle spielen. Wenngleich nunmehr etwa auch das Abrechnungssystem eines Energieversorgers grundsätzlich in den Anwendungsbereich der NIS2-Richtlinie fällt, können die Schutzmaßnahmen für diesen Teilbereich unter Umständen geringer ausfallen als bei Teilen der IT-Infrastruktur, die unmittelbar für die Lieferung von Strom notwendig sind; dies wird aber vor allem davon abhängen, inwieweit das Abrechnungssystem auch als Einfallstor für Bedrohungen „kritischerer" Teile der IT-Infrastruktur der betroffenen Einrichtung missbraucht werden könnte.

20) Für die Einstufung maßgeblich ist Art 2 des Anhangs der Empfehlung 2003/361/EG der Kommission vom 6. Mai 2003 betreffend die Definition der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen, ABl. L 124 vom 20.5.2003, 39.

21) So das Beispiel in Erwägungsgrund 22 der NIS1-Richtlinie.

22) Vgl dazu unten Punkt 3.5.2.

Erfasste Wirtschaftssektoren (Auswahl)

SEKTOREN MIT HOHER KRITIKALITÄT
(Anhang I)

1. **Energie** (Strom inkl. Fernwärme, Öl, Gas, Wasserstoff)
2. **Verkehr** (Luft, Schiene, Wasser, Straßen)
3. **Bankwesen**
4. **Finanzmarktinfrastrukturen**
5. **Gesundheit** (Gesundheitsdienstleister, EU-Referenzlaboratorien, Arzneimittelforschung und -entwicklung, pharmazeutische Grundstoffe und Präparate & medizinische Notfallgeräte)
6. **Trinkwasserversorgung**
7. **Abwässer**
8. **Digitale Infrastruktur**
9. **IKT Dienstleistungsmanagement**
10. **Öffentliche Verwaltung**
11. **Raumfahrt**

SONSTIGE KRITISCHE SEKTOREN
(Anhang II)

1. **Post-** und **Kurierdienste**
2. **Abfallwirtschaft**
3. Herstellung, Produktion und Vertrieb von **Chemikalien**
4. Herstellung, Verarbeitung und Vertrieb von **Lebensmitteln**
5. Herstellung von medizinischen **Geräten**, Computern, elektronischen und optischen Erzeugnissen, elektrischen Ausrüstungen, Maschinen und Ausrüstungen, Kraftfahrzeugen, Anhängern und Sattelanhängern, sonstigen Transportmitteln
6. **Digitale Anbieter** (Online-Marktplätze, Online-Suchmaschinen & Plattformen für soziale Netzwerkdienste)
7. **Forschung**

3.3. Wesentliche und wichtige Einrichtungen

Generell unterscheidet die NIS2-Richtlinie zwischen wesentlichen und wichtigen Einrichtungen, die beide in den Anwendungsbereich der Richtlinie fallen.

Die dargestellte Unterscheidung hat zunächst hinsichtlich der regelmäßigen Kontrolle und Überwachung betroffener Unternehmen durch die zuständigen Behörden und Einrichtungen iSd der NIS2-Richtlinie Bedeutung. So unterliegen wesentliche Einrichtungen aufgrund der potenziell höheren Auswirkungen von Störungen ihrer Dienste strengeren Überwachungs- und Meldepflichten. Überdies ist die Differenzierung auch hinsichtlich der bei Verstößen gegen die Richtlinienvorgaben minimal zu verhängenden Geldbußen bzw Sanktionen von Bedeutung.[23])

Zentrale Pflichten, wie insbesondere die Umsetzung von Maßnahmen zur Schaffung eines wirksamen Cybersicherheitsmanagements samt Planung, Dokumentation und Umsetzung angemessener Sicherheitsmaßnahmen,[24]) gelten demgegenüber für wesentliche und wichtige Einrichtungen gleichermaßen.

Art 3 Abs 1 NIS2-Richtlinie liefert eine einheitliche – und im Detail durchaus komplexe – Definition des Begriffs der „wesentlichen" Einrichtung. Darunter sind zum Beispiel Vertrauensdiensteanbieter, ausgewählte Telekommunikationsanbieter, bestimmte staatliche Institutionen und bereits bisher nach besonderen Rechtsvorschriften als kritisch eingestufte Einrichtungen zu subsumieren, ebenso aber auch sämtliche Unternehmen (ab mittlerer Größe) in den in Anhang I angeführten Wirtschaftssektoren mit hoher Kritikalität. Dazu zählen ua Energie, Verkehr, Bankwesen, Finanzmarktinfrastruktur, Gesundheitswesen, Trinkwasser, Abwasser, digitale Infrastruktur, Verwaltung von Diensten der Informations- und Kommunikationstechnologie, öffentliche Verwaltung und Raumfahrt.

Alle Unternehmen, welche die Anforderungen des Art 2 der NIS2-Richtlinie erfüllen und eine Tätigkeit in einem der in Anhang I bzw II der NIS2-Richtlinie genannten Sektoren entfalten, nicht aber als wesentliche Einrichtungen einzustufen sind, gelten gemäß Art 3 Abs 2 der NIS2-Richtlinie als wichtige Einrichtungen. Hierzu zählen insbesondere Unternehmen in den Bereichen Post- und Kurierdienst, Abfallbewirtschaftung, Herstellung, Produktion und Handel mit chemischen Stoffen, Produktion, Verarbeitung und Vertrieb von Lebensmitteln, Betriebe im Bereich des verarbeitenden Gewerbes und der Herstellung von Waren, Anbieter digitaler Dienste sowie Forschungseinrichtungen. Die weite Definition der wichtigen Einrichtungen bewirkt, dass sich viele Unternehmen mit Inkrafttreten der NIS2-Regeln erstmals umfassend mit Cybersicherheits-Compliance auseinandersetzen müssen.[25])

3.4. All hazards approach

Die NIS2-Richtlinie erfordert, dass richtlinienunterworfene Einrichtungen Vorkehrungen gegen alle Gefahren treffen, welche die Sicherheit und Integrität ihrer Netz- und Informationssysteme tatsächlich oder potentiell bedrohen, unabhängig von deren Art oder Herkunft. Dieser sog „all-hazards approach" bedeutet, dass IT-Systeme nicht nur gegen typische IT-bezogene Gefahren wie Hackerangriffe oder Computerviren geschützt werden müssen. Vielmehr sind auch ausreichende Vorkehrungen zum Schutz vor anderen Ereignissen wie zB Diebstahl, Feuer, Überschwemmungen und Telekommunikations- oder Stromausfällen[26]) zu treffen. Erfasst sind sowohl unternehmensinterne als auch externe Faktoren, bis hin – wie soeben gezeigt – zu Bedrohungen durch Ereignisse höherer Gewalt, etwa Naturkatastrophen.

Die NIS2-Richtlinie verpflichtet betroffene Unternehmen sohin zu einem holistischen Denk- und Handlungsansatz in der Planung und Umsetzung der von der Richtlinie geforderten Sicherungsmaßnahmen; dies mit dem Ziel, wesentliche und wichtige IT-Infrastruktur umfassend und lückenlos vor Angriffen und Kompromittierung zu schützen.

3.5. Governance und Risikomanagement

Zur Erreichung eines hohen Sicherheitsniveaus der Netz- und Informationssysteme wesentlicher und wichtiger Einrichtungen verpflichtet die NIS2-Richtlinie die betroffenen Unternehmen zur Umsetzung diverser Maßnahmen, die im Folgenden überblicksmäßig dargestellt werden.

3.5.1. Governance

Gemäß Art 20 der NIS2-Richtlinie sind Leitungsorgane wesentlicher und wichtiger Einrichtungen – bei sonstiger, persönlicher (!) Haftung – dafür verantwortlich, die getroffenen Risikomanagementmaßnahmen zu genehmigen und zu überwachen.[27]) Darüber hinaus müssen die Mitgliedstaaten sicherstellen, dass die Mitglieder der Leitungsorgane betroffener Einrichtungen Schulungen im Bereich der Cybersicherheit absolvieren, um die notwendigen Kenntnisse und Fähigkeiten zu erlangen, welche zur Einhaltung der Richtlinienvorgaben notwendig sind. Gemäß Art 20 Abs 2 der NIS2-Richtlinie ist gleichermaßen vorgesehen, dass Mitarbeitern wesentlicher und wichtiger Einrichtungen derartige Schulungen regelmäßig angeboten werden müssen.[28])

3.5.2. Risikomanagement

Das von richtlinienunterworfenen Einrichtungen einzuführende Risikomanagement muss folgende Voraussetzungen erfüllen und Prämissen beachten:

a. Angemessene Maßnahmen in wesentlichen und wichtigen Einrichtungen: Die NIS2-Richtlinie

23) *Kipker* (FN 12), 250.
24) *Voigt/Bastians* (FN 1), 770.
25) *Wegmann* (FN 5), 838.
26) Vgl dazu Erwägungsgrund 79 NIS2-Richtlinie.
27) Zur Haftung bei Verstößen gegen die Pflichten der Leitungsorgane vgl unten Punkt 4.
28) *Voigt/Bastians* (FN 1), 771.

verpflichtet die Mitgliedstaaten dazu, sicherzustellen, dass wesentliche und wichtige Einrichtungen angemessene und verhältnismäßige technische, organisatorische und operative Maßnahmen ergreifen, um die Risiken für die Sicherheit der Netz- und Informationssysteme, die diese Einrichtungen für ihren Betrieb oder für die Erbringung ihrer Dienste nutzen, zu beherrschen. Damit sollen die Auswirkungen von Sicherheitsvorfällen auf die Empfänger ihrer Dienste und auf andere Dienste verhindert oder möglichst gering gehalten werden.

b. Berücksichtigung des Standes der Technik und der Kosten: Bei der Umsetzung sind der Stand der Technik und europäische sowie internationale Standards, aber auch die durch die betroffenen Einrichtungen aufzuwenden Implementierungskosten angemessen zu berücksichtigen.

c. Risikobasierter Ansatz: Gemäß Art 21 Abs 1 der NIS2-Richtlinie ist auf Basis eines risikobasierten Denk- und Implementierungsansatzes vorzugehen und daher jeweils das Ausmaß potentieller Bedrohungen der Cybersicherheit des betroffenen Unternehmens, dessen Größe, die Wahrscheinlichkeit von Sicherheitsvorfällen und die Schwere der gesellschaftlichen und wirtschaftlichen Auswirkungen denkbarer Sicherheitsvorfälle zu berücksichtigen.

d. Konkretisierung des erforderlichen Mindestmaßes an das Risikomanagement: Art 21 Abs 2 der NIS2-Richtlinie konkretisiert die in der Richtlinie zunächst abstrakt beschriebenen Maßnahmen und legt fest, welche Aspekte das geforderte Risikomanagement zumindest umfassen muss. Dazu gehören Konzepte und Maßnahmen zur Risikoanalyse und Informationssicherheit, zur Bewältigung von Sicherheitsvorfällen, zur Aufrechterhaltung des Betriebs (zB Backup- und Krisenmanagementpläne und -mechanismen) und betreffend die Sicherheit der Lieferkette[29]); weiters Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von Informationssystemen, Konzepte zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen, grundlegende Verfahren im Bereich der Cyberhygiene und Schulungen zur Cybersicherheit, der Einsatz von Kryptographie und Verschlüsselungsmechanismen sowie von gesicherter Kommunikation und von Notfallkommunikationssystemen innerhalb der jeweils betroffenen Einrichtung.

e. Durchführungsrechtsakte der EU-Kommission: Gemäß Art 21 Abs 5 Unterabsatz 2 der NIS2-Richtlinie kann die EU-Kommission Durchführungsrechtsakte erlassen, um technische und methodische Spezifikationen für die geforderten Maßnahmen festzulegen. Sie ist verpflichtet, dies innerhalb von 21 Monaten nach Inkrafttreten der Richtlinie für bestimmte Einrichtungen zu tun (Art 21 Abs 5 Unterabsatz 1 NIS2-Richtlinie). Bei der Ausarbeitung dieser Rechtsakte hat sich die EU-Kommission an internationalen und europäischen Normen sowie relevanten technischen Spezifikationen zu orientieren (Art 21 Abs 5 Unterabsatz 3 NIS2- Richtlinie).[30])

3.6. Absicherung der Supply Chain (Lieferkettensicherheit)

Auch hinsichtlich des Supply-Chain-Managements besteht angesichts der vielfältigen Akteure und Schnittstellen eine zunehmende Anfälligkeit für cyberbedingte Gefährdungen. Durch die digitale Vernetzung globaler Märkte stellt jeder einzelne Teilnehmer der Lieferkette eine potenzielle Schwachstelle dar, welche das reibungslose Funktionieren der Supply-Chain in ihrer Gesamtheit gefährden kann. Konkrete Bedrohungen treten dabei in unterschiedlichsten Formen auf, etwa als Ransomware-Angriffe, Datendiebstahl, Sabotageakte oder Industriespionage. Die NIS2-Richtlinie erfasst derartige inhärente Verwundbarkeiten von Lieferketten und versucht, diesen durch die Etablierung angemessener Sicherheitsmaßnahmen präventiv entgegenzuwirken.

Art 21 Abs 1 NIS2-Richtlinie bestimmt, dass wesentliche und wichtige Einrichtungen geeignete und verhältnismäßige technische, operative und organisatorische Maßnahmen zu ergreifen haben, um die Risiken für die Sicherheit der Netz- und Informationssysteme, welche die betroffenen Einrichtungen für ihren Betrieb oder für die Erbringung ihrer Dienste nutzen, zu beherrschen und die Auswirkungen von Sicherheitsvorfällen auf die Empfänger ihrer Dienste und auf andere Dienste zu verhindern oder möglichst gering zu halten. Derartige Maßnahmen müssen gemäß Art 21 Abs 2 lit d NIS2-Richtlinie insbesondere auch die Sicherheit der Lieferkette einschließlich sicherheitsbezogener Aspekte der Beziehungen zwischen den wesentlichen und wichtigen Einrichtungen und ihren unmittelbaren Anbietern oder Diensteanbietern umfassen.

Aus Erwägungsgrund 85 der NIS2-Richtlinie geht hervor, dass Art 21 in Hinblick auf die Absicherung der Lieferkette dem Umstand sich häufender Vorfälle entgegenzuwirken versucht, bei denen wesentliche und wichtige Einrichtungen Opfer von Cyberangriffen werden, welche daraus resultieren, dass es böswilligen Akteuren gelingt, die Sicherheit der von den betroffenen Einrichtungen betriebenen Netz- und Informationssysteme zu beeinträchtigen, indem Schwachstellen im Zusammenhang mit den Produkten und Diensten Dritter ausgenutzt werden. Exemplarisch werden Anbieter von Datenspeicherungs- und -verarbeitungsdiensten, Anbieter verwalteter Sicherheitsdienste und Softwarehersteller als potentielle Einfallstore für Sicherheitsrisiken in der Supply Chain erwähnt.

Wesentlichen und wichtigen Einrichtungen wird im gegebenen Kontext die Pflicht auferlegt, die Gesamtqualität und Widerstandsfähigkeit der Produkte und

29) Siehe hierzu auch nochmals sogleich unter Punkt 3.6.

30) *Voigt/Bastians* (FN 1), 770-771.

Dienste ihrer Lieferanten unter Berücksichtigung der darin enthaltenen Risikomanagementmaßnahmen im Bereich der Cybersicherheit zu bewerten und auf dieser Basis geeignete Abwehrmechanismen in die vertraglichen Vereinbarungen mit den betroffenen Lieferanten einzubeziehen. Unklar ist insoweit allerdings die für die Praxis bedeutsame Frage, ob die Absicherungspflicht für alle Stufen der gesamten Lieferkette gilt:

Während der Wortlaut des Art 21 Abs 2 lit d NIS2-Richtlinie nur Absicherungen gegenüber *unmittelbaren* Lieferanten und Diensteanbietern erfasst und sohin weiter vorgelagerte Ebenen der Supply Chain *de lege lata* nicht explizit miteinschließt, verdeutlichen die Erwägungsgründe der Richtlinie zunächst, dass wesentliche und wichtige Einrichtungen insbesondere dazu angehalten werden sollen, Risikomanagementmaßnahmen im Bereich der Cybersicherheit in die vertraglichen Vereinbarungen mit ihren *direkten* Lieferanten und Diensteanbietern einzubeziehen. Der letzte Satz des Erwägungsgrundes 85 der deutschen Fassung der Richtlinie trifft dann allerdings weiters – uE einigermaßen kryptisch – folgende Aussage: „*Diese Einrichtungen könnten auch die Risiken berücksichtigen, die von Lieferanten und Dienstleistern anderer Ebenen ausgehen.*“

Unklar ist, worauf sich das Wort „diese“ im zitierten, letzten Satz des Erwägungsgrundes 85 genau bezieht: Damit könnten dem grammatikalischen Sinn nach sowohl die (jeweils im Vorsatz des betreffenden Erwägungsgrundes erwähnten) von der Richtlinie betroffenen wesentlichen und wichtigen Einrichtungen, als auch die jeweiligen unmittelbaren Lieferanten und Diensteanbieter gemeint sein. Im systematischen Zusammenhang und unter Berücksichtigung des Wortlauts des Art 21 Abs 2 lit d NIS2-Richtlinie naheliegender erscheint uE eine Auslegung in letzterem Sinne und sohin die Interpretation des Wortes „diese“ im Sinne einer Referenz auf die unmittelbaren Lieferanten und Diensteanbieter der betroffenen wesentlichen und wichtigen Einrichtungen. Auch ein Blick in die englische Fassung des Erwägungsgrundes 85 spricht zumindest nicht gegen diese Auffassung. Im Sinne einer rechtlichen Absicherung wird es uE dennoch ratsam sein, unmittelbare Lieferanten nach Möglichkeit im vertraglichen Wege auch dahingehend zu verpflichten, ihrerseits die Sicherheit der ihnen vorgelagerten Supply-Chain sicherzustellen.

Inwieweit wesentliche und wichtige Einrichtungen ihren unmittelbaren Lieferanten entsprechende vertragliche Pflichten auferlegen können, sofern sie nicht bereits in der Vergangenheit Vorkehrungen hierfür in Form der Ausverhandlung geeigneter (und ausreichend umfangreicher) Vertragsanpassungsklauseln getroffen haben, lässt die Richtlinie offen. Es bleibt abzuwarten, ob und inwieweit der österreichische Gesetzgeber hierfür spezifische Instrumentarien im Rahmen der Umsetzung der NIS2-Richtlinie in nationales Recht vorsehen wird. Wünschenswert und wichtig wäre *de lege ferenda* uE zumindest die gesetzlich explizit verankerte Möglichkeit, betroffene Vertragsverhältnisse mit unmittelbaren Lieferanten aus wichtigem Grund beenden zu können, sofern diese sich weigern, die von der Richtlinie geforderten Maßnahmen auf ihrer Ebene zu implementieren. Auf diese Weise könnten wesentliche und wichtige Einrichtungen wenigstens rechtssicher davon ausgehen, nicht in für sie unter der NIS2-Gesetzgebung potentiell haftungsbegründenden Lieferantenbeziehungen längerfristig verharren zu müssen.

Andernfalls[31]) drohen uE in Hinblick auf die Fortsetz- und Beendbarkeit bestehender Vereinbarungen, die den Anforderungen von NIS2 nicht (mehr) entsprechen, erhebliche rechtliche Unsicherheiten für alle Beteiligten. Die strengen Vorgaben der NIS2-Richtlinie könnten in diesem Lichte schlimmstenfalls sogar in „Erpressbarkeit“ wesentlicher und wichtiger Einrichtungen durch Supplier kulminieren. Dies umso mehr, wenn man bedenkt, dass die Fortführung von (insbesondere bereits länger andauernden) Geschäftsbeziehungen zu wichtigen Lieferanten – wenngleich zu gegebenenfalls angepassten Bedingungen – wirtschaftlich im Regelfall die sinnvollere Lösung darstellen wird, als eine Vertragsbeendigung. Supplier könnten diesen Umstand und die nach aktuellem Regelungsstand zu befürchtende Rechtsunsicherheit dazu nutzen, Preiserhöhungen oder sonstige Verbesserungen ihrer vertraglichen Position im Austausch für ihre Kooperation iSd NIS2-Regeln einzufordern. De *lege lata* erscheinen potentiell zahllose Rechtsstreitigkeiten in diesem Zusammenhang aus derzeitiger Sicht geradezu vorprogrammiert.

Den betroffenen Einrichtungen iSd NIS2-Richtline ist jedenfalls dringend anzuraten, zumindest *pro futuro* besonders sorgsam auf die Ausgestaltung ihrer vertraglichen Beziehungen zu Lieferanten aus der Perspektive der einschlägigen Cybersicherheitsvorschriften zu achten und in den jeweiligen Vereinbarungen ausreichend Vorsorge dafür zu treffen, dass eine effektive und lückenlose Umsetzung der einschlägigen Richtlinienvorgaben gewährleistet werden kann. *In praxi* werden betroffene Unternehmen die für ihren Betrieb ausgearbeiteten Risikomanagementmaßnahmen auf unmittelbare Supplier anpassen und an diese überbinden müssen, um sich verlässlich absichern zu können. Inwieweit derartige Maßnahmen von Lieferanten akzeptiert und mitgetragen werden, bleibt freilich fraglich und abzuwarten. Auch insoweit wäre daher eine nochmalige kritische Hinterfragung der Treffsicherheit und praktischen Umsetzbarkeit der aktuellen Richtlinienziele wünschenswert.

3.7. Berichtspflichten bei Sicherheitsvorfällen

Gemäß Art 23 Abs 1 in Verbindung mit Abs 3 und 4 der NIS2-Richtlinie haben die Mitgliedstaaten sicherzustel-

31) Das heißt, sofern der Gesetzgeber in Hinblick auf die (Neu-) Gestaltbarkeit bestehender Vertragsbeziehungen wesentlicher und wichtiger Einrichtungen zu deren Lieferanten keine weiteren Vorkehrungen treffen, sondern betroffene Unternehmen stattdessen auf allgemeine zivilrechtliche Grundsätze verweisen sollte. Zu denken wäre in diesem Zusammenhang insbesondere an die generelle, zwingende Kündbarkeit von Dauerschuldverhältnissen bei Unzumutbarkeit deren Fortführung für einen Vertragsteil; aber auch Vertragsanfechtung bzw -anpassung, Sittenwidrigkeit und ähnliche Denkansätze erscheinen, abhängig vom Einzelfall, überlegenswert.

len, dass wesentliche und wichtige Einrichtungen umgehend das zuständige CSIRT (Computer Security Incident Response Team)[32]) oder, wo relevant, die zuständige Behörde über Sicherheitsvorfälle informieren, die einen erheblichen Einfluss auf ihre Dienste haben. Ein Sicherheitsvorfall wird als jedes Ereignis definiert, das die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit von Daten oder Diensten, die über Netz- und Informationssysteme angeboten werden, beeinträchtigt. Ein Vorfall gilt als erheblich, wenn er schwerwiegende Betriebsstörungen oder finanzielle Verluste für die betroffene Einrichtung verursacht oder andere Personen erheblich materiell oder immateriell schädigt.

Die dargestellten Berichtspflichten werden durch Art 23 Abs 4 der NIS2-Richtlinie weiter konkretisiert:

a. Wesentliche und wichtige Einrichtungen müssen zunächst innerhalb von 24 Stunden nach Kenntnisnahme eines erheblichen Sicherheitsvorfalls eine Frühwarnung an das CSIRT oder die zuständige Behörde senden, falls der Verdacht besteht, dass der Vorfall wahrscheinlich auf rechtswidriges und böswilliges Handeln zurückzuführen ist oder grenzüberschreitende Auswirkungen haben könnte.
b. Innerhalb von 72 Stunden muss eine weitere Meldung erfolgen, die die vorherigen Informationen aktualisiert, eine erste Bewertung des Vorfalls enthält und auf seine Schwere, Auswirkungen sowie mögliche Kompromittierungsindikatoren eingeht. Betroffene Vertrauensdiensteanbieter müssen die Folgemeldung spätestens innerhalb von 24 Stunden abgeben.
c. Auf Anfrage des CSIRT oder der zuständigen Behörde müssen betroffene wesentliche und wichtige Einrichtungen zudem jederzeit einen Zwischenbericht mit relevanten Status-Updates vorlegen. Die NIS2-Richtlinie enthält insoweit keine genauen Angaben zur Frist für die Beantwortung des jeweiligen Verlangens, sodass insoweit – sollte der nationale Gesetzgeber hier keine Klarstellung vornehmen – vom grundlegenden Prinzip der Unverzüglichkeit auszugehen sein wird.

Schließlich müssen die betroffenen Einrichtungen einen Abschlussbericht vorlegen, der in der Regel spätestens einen Monat nach der Folgemeldung (vgl lit b oben) zu übermitteln ist. Dieser Bericht muss eine ausführliche Beschreibung des Vorfalls einschließlich seiner Schwere und Auswirkungen, Angaben zur Art der Bedrohung bzw zugrundeliegenden Ursache, Informationen über ergriffene und laufende Abhilfemaßnahmen sowie gegebenenfalls über grenzüberschreitende Auswirkungen des Vorfalls enthalten. Wenn der Vorfall zum Zeitpunkt der Berichterstattung noch andauert, ist stattdessen ein weiterer Fortschrittsbericht zu erstatten.

32) CSIRTs sind gem Art 10 Abs 1 NIS2-Richtlinie von jedem Mitgliedsstaat einzurichten oder zu benennen.

3.8. Sonderpflichten für Domänennamen-Registrierungs-Datenbanken

TLD-Namensregister und Einrichtungen, die Domänennamen-Registrierungsdienste anbieten, werden gemäß Art 28 Abs 1 der NIS2-Richtlinie mit zusätzlichen Pflichten belegt. Die Mitgliedstaaten sollen derartige Einrichtungen dazu verpflichten können, genaue und vollständige Domänennamen-Registrierungsdaten in einer eigenen Datenbank zu sammeln und zu pflegen, wobei unter anderem auch die Vorgaben der DSGVO zu beachten sind. Gemäß Art 28 Abs 2 Buchstabe c der NIS2-Richtlinie müssen Informationen wie der Name des Domäneninhabers, seine E-Mail-Adresse und seine Telefonnummer in der Datenbank enthalten sein. Die Notwendigkeit und Verhältnismäßigkeit dieser Verpflichtungen im Hinblick auf das Ziel der Stärkung der IT-Sicherheit auf EU-Ebene sind jedoch sicherlich diskussionswürdig.[33])

3.9. Sanktionen

Gem Art 34 Abs 4 und 5 NIS2-Richtlinie drohen wesentlichen Einrichtungen bei Verstößen Bußgelder in einem Höchstbetrag von mindestens 10 Mio. Euro oder 2 % des weltweiten Jahresumsatzes (je nachdem, welcher Betrag höher ist). Wichtigen Einrichtungen drohen Bußgelder in einem Höchstbetrag von mindestens 7 Mio. Euro oder 1,4 % des weltweiten Jahresumsatzes. Abzustellen ist dabei nach dem Wortlaut der Richtlinie jeweils auf den *Umsatz des Unternehmens, dem die wesentliche oder wichtige Einrichtung angehört*. Dies erscheint vor allem in jenen – praktisch weit überwiegenden – Fällen undeutlich, in denen sich bereits aus der Definition der wesentlichen/wichtigen Einrichtung ergibt, dass es sich dabei um ein Unternehmen handelt.[34]) Fraglich bleibt, wie die Formulierung des Art 34 Abs 4 und 5 in diesem Zusammenhang zu verstehen sein soll. Denkbar wäre uE, dass der europäische Gesetzgeber Konzernstrukturen vor Augen hatte und insoweit den gesamten Umsatz einer Unternehmensgruppe als Rahmen für die jeweils zu verhängende Strafe heranziehen möchte. Eindeutig und zwingend indes erscheint diese Lesart *de lege lata* keineswegs. Eine Klarstellung – zumindest durch den nationalen Gesetzgeber im Rahmen der Umsetzung der Richtlinie – wäre insoweit einmal mehr wünschenswert und geboten.

Im Vergleich zum für Österreich geltenden NISG in dessen bisheriger Fassung, in welcher der Höchstbetrag für Verstöße im Erstfall bei EUR 50.000 und im Falle eines wiederholten Verstoßes bei EUR 100.000 liegt, führt die NIS2-Richtlinie jedenfalls zu einer deutlichen Erhöhung der drohenden Bußgeldsanktionen. Besonders bedeutsam ist in diesem Zusammenhang auch Art 20 Abs 1 der NIS2-Richtlinie, nach welchem die Mitgliedstaaten ihrerseits sicherstellen müssen, dass Leitungsorgane wesentlicher und wichtiger Einrichtungen

33) *Voigt/Bastians* (FN 1), 771.

34) Zur Klarstellung: Auch Einrichtungen der öffentlichen Verwaltung können wesentliche oder wichtige Einrichtungen iSd NIS2-Richtlinie sein, es muss sich bei einer Einrichtung also nicht stets und geradezu zwangsweise um ein Unternehmen handeln (vgl Art 2 Abs 2 lit f).

über die Implementierung von Maßnahmen zur Cybersicherheit zu entscheiden und deren Umsetzung zu überwachen haben, wobei sie bei Nichteinhaltung dieser Pflichten persönlich haftbar gemacht werden können.[35]) Details zur Konkretisierung des Haftungsumfangs der Leitungsorgane enthält die NIS2-Richtlinie insoweit indes leider nicht. Insbesondere legt die NIS2-Richtlinie keinen konkreten Sorgfaltsmaßstab fest, sodass es hier im besonderen Maße auf die konkrete nationale Umsetzungsgesetzgebung ankommen wird.[36])

4. Haftung von Leitungsorganen von Kapitalgesellschaften bei mangelnder IT-Sicherheit

4.1. NIS2-Richtlinie und IT-Compliance

In Zukunft wird die Pflicht zur Einhaltung jener Bestimmungen, mit denen die NIS2-Richtlinie in Österreich umgesetzt wird, wesentlicher Bestandteil der IT-Compliance (*i.e.* der Summe aller Maßnahmen zur Einhaltung von sämtlichen gesetzlichen und vertraglichen Regelungen betreffend die Sicherheit der IT-Systeme eines Unternehmens)[37]) sein.

Gesetzlich[38]) festgelegt ist, dass Leitungsorgane von Kapitalgesellschaften ein Kontrollsystem einzurichten haben. Aus dieser Pflicht wird auch das Erfordernis der Einrichtung eines Compliance-Management-Systems als organisatorische Pflicht abgeleitet.[39]) Die juristische Diskussion – auch in Österreich – ist hier maßgeblich vom *Siemens/Neubürger*-Urteil[40]) geprägt. Darin hat das LG München I ausgesprochen, dass der Vorstand einer Aktiengesellschaft seine Organisationspflicht nur erfüllt, wenn er bei entsprechender Gefährdungslage eine auf Schadensprävention und Risikokontrolle angelegte Compliance-Organisation einrichtet.[41]) Auch der OGH[42]) hat sich in einer jüngeren Entscheidung ausführlich mit den Anforderungen an ein internes Kontrollsystem auseinandergesetzt, und zwar im Zusammenhang mit einem CEO-Fraud.[43]) IT-Compliance ist folglich keine Aufgabe, die allein von der IT-Abteilung eines Unternehmens zu bewältigen ist.[44]) Vielmehr ist die Unternehmensleitung direkt davon betroffen, da sie persönlich für die Einhaltung der Vorgaben – im Sinn der zuvor angeführten Prinzipien – zu sorgen hat. [45])

In Zukunft werden Leitungsorgane von Unternehmen daher darauf zu achten haben, eine Compliance-Organisation zu schaffen, die die Einhaltung eines IT-Sicherheitsniveaus sicherstellt, das den Bestimmungen der NIS2-Richtlinie entspricht. Im Bedarfsfall sind dabei Fachleute oder Sachverständige[46]) als Berater beizuziehen. Da – gerade im Bereich der IT-Sicherheit – absolute Schadensprävention nicht möglich ist, ist bei der Errichtung einer Compliance-Organisation allerdings jeweils eine Kosten-Nutzen-Abwägung zulässig und letztendlich auch geboten.[47])

4.2. Im Besonderen: Haftung der Leitungsorgane

Leitungsorgane von Kapitalgesellschaften sind gesetzlich[48]) verpflichtet, bei ihrer Geschäftsführung die Sorgfalt eines ordentlichen Geschäftsmannes anzuwenden. Dazu zählt auch die Einhaltung öffentlich-rechtlicher Verpflichtungen,[49]) wie jener, die in der NIS2-Richtlinie normiert sind.

Kommt es aufgrund von Missachtung der Verpflichtungen zur IT-Sicherheit, die sich aus der NIS2-Richtlinie ergeben, zu einem Schaden für die Gesellschaft, so kann dieser ein Anspruch auf Schadenersatz zustehen.[50]) Voraussetzung ist ein fahrlässiges Handeln des Leitungsorgans, wobei sich der entsprechende Verschuldensvorwurf auch aus der fehlenden Errichtung eines Kontrollsystems zur Einhaltung der Bestimmungen der NIS2-Richtlinie ergeben kann. Im Übrigen trifft das Leitungsorgan nach der Rechtsprechung auch die Beweislast dafür, dass es die ihm obliegende Sorgfalt angewendet hat.[51]) Im einzelnen bestehen Sondervorschriften,[52]) die Vergleiche oder Verzichte betreffend Schadenersatzansprüche gegenüber Leitungsorgangen erschweren. Somit ist eine tatsächliche Inanspruchnahme des Managements bei Schäden durch mangelnde Einhaltung der NIS2-Vorschriften auch durchwegs praxis-

35) Vgl dazu unten Punkt 4.2.

36) *Wegmann* (FN 5), 840; Zum Inhalt des diesbezüglichen deutschen Referentenentwurfs vgl *Kipker/Dittrich*, Rolle der Kritischen Infrastrukturen nach dem neuen NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz, MMR 2023, 481, 485 f.

37) *Petsche/Larcher* in Petsche/Mair (Hrsg), Handbuch Compliance[3] (2019), Interpretation von Compliance in verschiedenen Branchen, Pkt 2.3.

38) Vgl § 22 Abs 1 GmbHG, § 82 AktG.

39) *J. Reich-Rohrwig/Zimmermann* in *Artmann/Karollus*, AktG II[6] § 82 Rz 34 (Stand 1.10.2018, rdb.at).

40) LG München I, Urteil vom 10.12.2013 – 5HK O 1387/10, abrufbar unter: *https://openjur.de/u/682814.html.*

41) *J. Reich-Rohrwig/Zimmermann* in *Artmann/Karollus*, AktG II[6] § 82 Rz 35 (Stand 1.10.2018, rdb.at). Konkret wurde dabei ausgeführt, dass das Unternehmen so organisiert und beaufsichtigt werden muss, dass keine Gesetzesverstöße wie Schmiergeldzahlungen erfolgen. Wenngleich es sich nur um ein erstinstanzliches Urteil handelte, so hat dieses die juristische und Compliance-Diskussion ganz maßgeblich geprägt.

42) OGH 8 Ob A 109/20t, GesRZ 2022, 132 (*Gerlach*).

43) CEO-Fraud liegt vor, wenn sich Kriminelle als Leitungsorgane von Firmen ausgeben und sich mit gefälschten E-Mails in deren Namen an Mitarbeiter wenden, oftmals zu dem Zweck, Geldüberweisungen anzuordnen.

44) *Petsche/Larcher* FN37.

45) *Petsche/Larcher* FN37.

46) *J. Reich-Rohrwig* in Straube/Ratka/Rauter, WK GmbHG § 25 Rz 53 (Stand 1.9.2022, rdb.at) im Zusammenhang mit der Haftung der Geschäftsführer.

47) *J. Reich-Rohrwig/Zimmermann* in *Artmann/Karollus*, AktG II[6] § 82 Rz 38 (Stand 1.10.2018, rdb.at).

48) Vgl § 25 Abs 1 GmbHG und § 84 Abs 1 AktG.

49) *J. Reich-Rohrwig* in Straube/Ratka/Rauter, WK GmbHG § 25 Rz 30 (Stand 1.9.2022, rdb.at).

50) Anspruchsgrundlage ist § 25 Abs 1 GmbHG bzw § 84 Abs 1 AktG.

51) *J. Reich-Rohrwig* in Straube/Ratka/Rauter, WK GmbHG § 25 Rz 330 (Stand 1.9.2022, rdb.at); *Nowotny* in Doralt/Nowotny/Kalss, AktG[3] § 84 Rz 27 (Stand 1.6.2021, rdb.at); vgl auch OGH 8 Ob A 109/20t, GesRZ 2022, 132 (*Gerlach*).

52) Vgl § 84 Abs 4 AktG; § 35 GmbHG; vgl auch *J. Reich-Rohrwig* in Straube/Ratka/Rauter, WK GmbHG § 25 Rz 350f (Stand 1.9.2022, rdb.at).

nah. Darüber hinaus ist zu bedenken, dass die Leitungsorgane nach Cyberangriffen oftmals die einzigen Personen sind, die faktisch und wirtschaftlich erfolgreich zur Verantwortung gezogen werden können.[53])

Wie schon oben in Pkt 3.9 dargestellt, legt Art 21 Abs 1 NIS2-Richtlinie auch eine persönliche Verantwortlichkeit der Leitungsorgane fest. Ob dies nur im Zusammenhang mit der Verhängung von Geldbußen gilt, ist der NIS2-Richtlinie nicht deutlich zu entnehmen. Die Bestimmung könnte uE durchaus auch im Sinne einer eigenständigen Grundlage für die zivilrechtliche Haftung der Leitungsorgane verstanden werden. Für die endgültige Klärung dieser Frage wird insbesondere die Umsetzung der Richtlinie maßgeblich sein.

5. Zusammenfassung

Die NIS2-Richtlinie ist mit 16. Jänner 2023 in Kraft getreten und muss bis 17. Oktober 2024 in nationales Recht umgesetzt werden. Mit dem Inkrafttreten der Umsetzungsbestimmungen der NIS2-Richtlinie werden die Anforderungen an Unternehmen im Bereich der Cybersicherheit sprunghaft ansteigen. Zahlreiche Einrichtungen, insbesondere im verarbeitenden und herstellenden Gewerbe, werden überdies erstmals einem umfassenden Cybersicherheitsregime unterworfen.

Für die Einhaltung der Richtlinienvorschriften müssen betroffene Unternehmen umfassende Maßnahmen ergreifen. An erster Stelle steht hierbei die Planung und Implementierung eines holistischen, unternehmensinternen Risikomanagementsystems für Cybersicherheitsbedrohungen, das auch eine umfassende Absicherung der Lieferkette miteinschließt. Aufgrund des zu erwartenden hohen zeitlichen und administrativen Aufwandes bei der Anpassung an die Anforderungen der NIS2-Richtline sollten betroffene Unternehmen nunmehr rasch entsprechende Planungs- und Umsetzungsschritte einleiten, um Haftungen zu vermeiden.

Bei sämtlichen künftigen Vertragsabschlüssen mit unmittelbaren Lieferanten sollten betroffene Einrichtungen sorgsam darauf achten, die Erfüllbarkeit der sie treffenden Pflichten zur Absicherung der Lieferkette durch geeignete vertragliche Regeln umfassend abzusichern. Hinsichtlich bestehender Lieferantenbeziehungen ist dringend zu empfehlen, bereits jetzt zumindest jene Supplier zu identifizieren, deren Leistungen mit einem erhöhten Cybersicherheitsrisiko für das eigene Unternehmen verbunden sind und die sohin als besonders gefährdend eingestuft werden müssen; auf dieser Grundlage können frühzeitig Verhandlungen über notwendige Anpassungen der bestehenden Vertragsverhältnisse eingeleitet werden, um sich auf das Inkrafttreten der strengen NIS2-Vorgaben bestmöglich vorbereiten zu können.

Verstöße gegen die Bestimmungen der NIS2-Richtlinie bzw der diese in nationales Recht transponierenden Gesetzgebungsakte können zu umfangreichen Geldbußen und persönlicher Haftung der Leitungsorgane betroffener Unternehmen führen. Aufgrund der dargestellten Haftungsszenarien sollte mit der NIS2-Richtlinie das Thema IT-Sicherheit in den betroffenen Unternehmen nun endgültig zur Chefsache erklärt werden.

53) *Schmidt-Versteyl*, Cyber Risks – neuer Brennpunkt Managerhaftung?, NJW 2019, 1637, 1642.

Symposion: „Generative K.I. und das Urheberrecht – Eine komplizierte Beziehung“

Das Institut für Urheber- und Medienrecht in München (urheberrecht.org) veranstaltet am 10. November 2023 ein Symposium zu dem aktuellen Thema der Spannungslage zwischen generativer Künstlicher Intelligenz und Urheberrecht.

Generative Künstliche Intelligenz (KI) hält Einzug in alle Lebensbereiche: Die bekanntesten Beispiele sind Sprachmodelle für die Texterzeugung wie ChatGPT von OpenAI, eine KI-basierte Chatbot-Lösung zur erleichterten Generierung von Texten sowie Bildgeneratoren wie DALL·E, Midjourney oder Stable Diffusion. Die Produktivität dieser Systeme basiert darauf, dass sie auf der Grundlage von sehr großen Mengen von Trainingsdaten unter dem Einsatz von fortgeschrittenen Verfahren maschinellen Lernens Muster, Korrelationen und Wahrscheinlichkeiten erkennen, die es dem System ermöglichen, neue, in dieser Form bislang nichtexistierende Inhalte zu erzeugen.

Ziel der Veranstaltung ist es, die spezifisch rechtswissenschaftlichen Aspekte der mit dem Einsatz von generativer KI verbundenen urheberrechtlichen Probleme herauszuarbeiten.

Wer partizipiert an der Wertschöpfung durch generative KI? Vieles, was zunächst plausibel und einleuchtend erscheint – und zwar sowohl für die Kreativbranche als auch für die KI-Unternehmen –, stellt sich bei genauer rechtsdogmatischer und regulatorischer Analyse als weniger gesichert heraus, als ursprünglich angenommen. Gemeinsam mit ausgewählten Expert*innen soll dazu am 10.11.2023 von 10.00 – 15.00 Uhr auf der Präsenztagung diskutiert werden.

Ort: Literaturhaus München, Salvatorplatz 1, 80333 München. Eine Anmeldung ist erforderlich und wird voraussichtlich im September freigeschaltet (https://www.urheberrecht.org/events/20231110.php). Die Veranstaltung ist kostenlos.