universität wien

MASTER THESIS

Titel der Master Thesis / Title of the Master‘s Thesis

„Der Austausch von Cyber Threat Intelligence im Lichte der Umsetzung der NIS-Richtlinie“

verfasst von / submitted by

Mag.iur. Vinzenz Heußler

angestrebter akademischer Grad / in partial fulfilment of the requirements for the degree of

Master of Laws (LL.M.)

Wien, 2018 / Vienna 2018

Studienkennzahl lt. Studienblatt / Postgraduate programme code as it appears on the student record sheet:	A 992 942
Universitätslehrgang lt. Studienblatt / Postgraduate programme as it appears on the student record sheet:	Informations- und Medienrecht
Betreut von / Supervisor:	ao. Univ.-Prof. Dr. Dietmar Jahnel

Gewidmet meinen Eltern, Schwestern und IP

Vorwort

Infolge der Digitalisierung ist die Gesellschaft in ihren alltäglichen Abläufen einem ständigen Wandel unterworfen. Heutzutage sind Staat, Wirtschaft und die Gesellschaft als solche in weiten Teilen auf Netzwerk- und Informationssysteme angewiesen und in vielen Bereichen von diesen abhängig. Als Folge davon ist der „Cyberraum" ein Schlüsselelement in wirtschaftlichen und gesellschaftlichen Aktivitäten sowie im täglichen Leben geworden. Der rasante Prozess der Digitalisierung führt dabei zu Chancen wie auch zu Herausforderungen auf internationaler und nationaler Ebene. Eine zentrale Herausforderung stellt dabei die Gewährleistung der Sicherheit im digitalen Raum dar. Denn unbestrittenermaßen geht eine tendenziell steigende Gefahr von Cyberangriffen aller Art aus, seien sie nachrichtendienstlicher, wirtschaftsspionagetechnischer, kriegerischer oder krimineller Natur. Zur Stärkung der Cybersicherheit bedarf es effizienter Strukturen, um auf Cyberangriffe angemessen zu reagieren und die Gefahr, die von ihnen ausgeht, eindämmen zu können. Aufgrund der engen Verzahnung von Staat, Wirtschaft und Gesellschaft im Cyberraum ist es erforderlich, einen umfassenden Ansatz zu entwickeln. Die Europäische Kommission hat die Brisanz dieser Thematik erkannt und im Jahr 2013 eine Cybersicherheitsstrategie sowie eine weitere Strategie im Jahr 2017 mit umfassenden Vorhaben veröffentlicht. Als wichtigster Bestandteil der Strategie aus dem Jahr 2013 ging mit der NIS-Richtlinie die erste EU-weite Rechtsetzung zur Cybersicherheit hervor. In diesem großen und komplexen Umfeld widmet sich diese Arbeit der Frage, ob der österreichische Rechtsrahmen aus datenschutzrechtlicher Sicht geeignete Instrumentarien vorsieht, um vor dem Hintergrund der Umsetzung der NIS-Richtlinie Cybersicherheit gesamtstaatlich sicherstellen zu können. Obgleich die Gewährleistung der Cybersicherheit ein gemeinsames Ziel der Akteure ist und ein Kooperationsbedürfnis zweifelsohne vorliegt, stellt dieses Thema die in der Praxis Beteiligten vor diverse Herausforderungen, die sich zum einen aus der schwierigen Verknüpfung von technischen mit rechtlichen Erfordernissen und zum anderen daraus ergibt, dass hierbei Akteure sowohl aus dem öffentlichen als auch aus dem privaten Bereich kooperieren müssen. Im Hinblick auf die wenige Literatur, die sich dieses Themas konkret annimmt, soll mit dieser Arbeit ein Beitrag zum besseren Verständnis der rechtlichen Gegebenheiten zur Verfügung gestellt werden.

Vinzenz Heußler, 26. August 2018

Inhaltsverzeichnis

Abkürzungen

A

ABl	Amtsblatt
Abs	Absatz
AbwA	Heeres-Abwehramt
AdD	Anbieter digitaler Dienste
AEC	Austrian Energy CERT
AEUV	Vertrag über die Arbeitsweise der Europäischen Union
ANSSI	Agence nationale de la sécurité des systèmes d'information
APCIP	Austrian Program for Critical Infrastructure Protection
Art	Artikel
A-SIT	Zentrum für sichere Informationstechnologie – Austria

B

BGH	Bundesgerichtshof
BKA	Bundeskanzleramt
BKA-G	Bundeskriminalamt-Gesetz
BMDW	Bundesministerium für Digitalisierung und Wirtschaftsstandort
BMG	Bundesministeriengesetz
BM.I	Bundesministerium für Inneres
BMLV	Bundesministerium für Landesverteidigung
BlgNr	Beilagen zu den Stenographischen Protokollen des Nationalrats
BSI	Bundesamt für Sicherheit in der Informationstechnik
bspw.	beispielsweise

BVT	Bundesamt für Verfassungsschutz und Terrorismusbekämpfung
B-VG	Bundes-Verfassungsgesetz
BwD	Betreiber wesentlicher Dienste

C

C4	Cyber Crime Competence Center
CERT	Computer Emergency Response Team
CSIRT	Computer Security Incident Response Team
CDC	Cyber Defence Center
CSC	Cyber Security Center
CSS	Cyber Sicherheit Steuerungsgruppe
CTI	Cyber Threat Intelligence

D

d.h.	das heißt
DDoS	Distributed Denial of Service
DSG	Datenschutzgesetz
DS-GVO	Datenschutz-Grundverordnung
DSRL	Datenschutzrichtlinie
DSRL-PJ	Datenschutzrichtlinie für den Bereich Polizei und Justiz (Strafverfolgung)

E

ECG	E-Commerce-Gesetz
EGMR	Europäischer Gerichtshof für Menschenrechte
ErwG	Erwägungsgrund/-gründe

EMRK	Europäische Menschenrechtskonvention
ErläutRV	Erläuterungen der Regierungsvorlagen
EU	Europäische Union
EuGH	Europäischer Gerichtshof
EUR	Euro

F

f	folgende
ff	folgenden

G

GovCERT Austria	Austrian Government Computer Emergency Response Team

H

HNaA	Heeresnachrichtenamt
hM	herrschende Meinung

I

idF	in der Fassung
idR	in der Regel
IKDOK	Innerer Kreis der operativen Koordinierungsstrukturen
IKT	Informations- und Kommunikationstechnologie
IoC	Indicators of Compromise
iSd	im Sinne der/des
iVm	in Verbindung mit

K

KMU	kleine und mittlere Unternehmen
KSÖ	Kuratorium Sicheres Österreich

L

lit	litera/ae

M

MBG	Militärbefugnisgesetz
milCERT	Military Computer Emergency Readiness Team
mwN	mit weiteren Nachweisen

N

NAT	Network Address Translation
NCCIC	National Cybersecurity and Communications Integration Center
NIS	Netz- und Informationssystemsicherheit
NISG	Netz- und Informationssystemsicherheitsgesetz
NIS-RL	Richtlinie (EU) 2016/1148 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen
Nr	Nummer

O

ÖMZ	Österreichische Militärzeitschrift
ÖSCS	Österreichische Strategie für Cyber Sicherheit

P

PStSG	Polizeiliches Staatschutzgesetz

R

Rn	Randnummer
Rz	Randziffer

S

s.	siehe
SPG	Sicherheitspolizeigesetz
SPOC	Single Point of Contact
StGB	Strafgesetzbuch

T

TKG 2003	Telekommunikationsgesetz 2003

U

u.a.	unter anderem
URL	Uniform Resource Locator
u.U.	unter Umständen

W

WG 2001	Wehrgesetz 2001
WWW	World Wide Web

Z

Z	Ziffer
z.B.	zum Beispiel
z.T.	zum Teil

1. Einleitung

1.1. Hintergrund

Mit der voranschreitenden Digitalisierung und Verlagerung ganzer Lebensbereiche sowie wirtschaftlicher und politischer Prozesse in das Internet sind nicht nur ungemeine Chancen, sondern auch Risiken verbunden. Die Risiken ergeben sich dabei u.a. aus zunehmend und verstärkt professionell gestalteten politischen wie auch kriminellen Aktivitäten im Cyberraum. Der seit Jahren zu beobachtende Trend hin zu einer signifikanten Steigerung von sicherheitsrelevanten Aktivitäten und Vorfällen im Cyberraum setzt sich fort.[1/2]

Vor dem Hintergrund, dass die Sicherheit von Netz- und Informationssystemen mit den zugehörigen Diensten eine zentrale Rolle für wirtschaftliche und gesellschaftliche Tätigkeiten spielt, wurde auf europäischer Ebene mit der Richtlinie (EU) 2016/1148 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union[3] (im Folgenden: NIS-RL) die erste EU-weite Rechtsetzung zur Cybersicherheit verabschiedet.[4] In Österreich soll die NIS-RL durch das Cybersicherheitsgesetz umgesetzt werden.[5]

1.2. Problemaufriss

Im Zuge eines Angriffs auf Netz- und Informationssysteme ist es oftmals erforderlich, zum Zwecke der Prävention sowie Bewältigung eines Sicherheitsvorfalls Informationen auszutauschen oder sogar die Öffentlichkeit zu benachrichtigen. In diesem Sinne unterzeichneten bspw. das EU-CERT und dessen NATO-Pendant im Jahr 2016 eine Vereinbarung über den Austausch von technischen

---

[1] Vgl. *CSS*, Bericht Cyber Sicherheit 2017, 42.

[2] Zu den aktuellen Trends bei Ransomware und insbesondere bei Kryptowährungen (Cryptocurrency Malware bzw. Crime) s. *BSI*/*ANSSI*, Deutsch-französisches IT-Sicherheitslagebild (2018).

[3] Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union, ABl L 2016/194, 1.

[4] *Europäische Kommission*, The Directive on security of network and information systems (NIS Directive), <ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive>.

[5] S. Kapitel 5.6.

Informationen zur Erkennung, Abwehr von und Reaktion auf Cyberangriffe.[6] Das an sich selbstverständliche Teilen von Informationen über Angriffe auf die Netz- und Informationssystemsicherheit (NIS) stellt sich rechtlich jedoch komplex dar. Erst muss eine Prüfung der einschlägigen Rechtsvorschriften vorgenommen werden, um Rechtssicherheit darüber zu haben, was weitergegeben bzw. veröffentlicht werden darf.

Wenn die zu teilende Information keine personenbezogenen Daten, Geschäftsgeheimnisse oder urheberrechtlich geschütztes Material enthält und auch keine Persönlichkeitsrechte verletzt, so ergeben sich keine besonderen Rechtsfragen. Sollten jedoch geschützte Rechtspositionen in der Information enthalten oder geschützte Rechtspositionen von der Weitergabe der Informationen betroffen sein, so ist vor dem Teilen der Information eine Abwägung vorzunehmen und speziell auf rechtliche Zulässigkeitsschranken, die sich z.B. aus dem Datenschutzrecht ergeben können, zu achten. Besteht kein Recht oder keine Pflicht zur Informationsweitergabe, so kann die Information folglich nur weitergegeben werden, wenn keine der vielfältigen Beschränkungen der Informationsweitergabe verletzt werden.

Inhalt der vorliegenden Arbeit ist eine Abhandlung über die rechtlichen Problemstellungen, die sich aus dem Austausch von Informationen, die relevant für die Sicherheit von Netz- und Informationssystemen sind – im Folgenden wird der gebräuchliche Begriff „Cyber Threat Intelligence“[7] (CTI) verwendet –, zwischen den in Österreich maßgeblichen privaten und staatlichen Akteuren unter Fokussierung auf die datenschutzrechtlichen Fragestellungen bei der Umsetzung der NIS-RL sein.

[6] Vgl. *CSS*, Bericht Cyber Sicherheit 2017, 19.

[7] S. Kapitel 4.

2. Relevante Akteure

Um eine datenschutzrechtliche Prüfung des Austauschs von CTI vornehmen zu können, muss zunächst eine Festlegung und Abgrenzung der Akteure, zwischen denen der Informationsaustausch erfolgt, vorgenommen werden. Da im Cyberraum zahlreiche Strukturen bestehen, innerhalb derer Akteure zusammen – oder auch für sich alleine – an Cybersicherheit arbeiten, soll im Folgenden eine Fokussierung auf die für die Cybersicherheit in Österreich wesentlichen Akteure erfolgen. Die Fokussierung orientiert sich dabei an der Österreichischen Strategie für Cyber Sicherheit (ÖSCS)[8], welche eine Schaffung einer Struktur zur Koordination auf der operativen Ebene vorsieht, die u.a. den unverzüglichen Austausch aktueller Informationen über Cybersicherheitsvorfälle sicherstellen und in deren Rahmen ein periodisches und anlassbezogenes operatives Cyberlagebild für Österreich erstellt werden soll.[9] Im Rahmen der Struktur zur Koordination auf der operativen Ebene soll durch Sammeln, Bündeln, Auswerten und Weitergeben von relevanten Informationen ein kontinuierlicher Überblick über die aktuelle Situation im Cyberraum, welcher den Beteiligten als Grundlage für zu treffende planerische, präventive und reaktive Maßnahmen dienlich sein soll, gewährleistet werden. Die Struktur setzt sich neben Behörden auch aus Vertretern der Wirtschaft und dabei insbesondere aus Betreibern von kritischen Infrastrukturen zusammen.[10]

2.1. Behörden

Der ÖSCS entsprechend wurde eine Struktur zur Koordination auf der operativen Ebene geschaffen (s. Abbildung 1). Die zentralen Aufgaben der operativen Koordinierungsstruktur werden dabei vom Inneren Kreis der operativen Koordinierungsstrukturen (IKDOK) wahrgenommen, der von einem äußeren Kreis der operativen Koordinierungsstruktur unterstützt wird. Beim IKDOK handelt es sich um eine interministerielle Gruppe, die sich aus Vertretern des Bundeskanzleramts (BKA), des Bundesministeriums für Inneres (BM.I) und des Bundesministeriums für Landesverteidigung (BMLV) zusammensetzt. Für das BM.I nimmt konkret das Cyber Security Center (CSC) und für das BMLV das Cyber Defence Center (CDC)[11] teil. Weitere staatliche Akteure in den Ressorts sind

[8] *BKA*, Österreichische Strategie für Cyber Sicherheit, 10.

[9] *CSS*, Bericht Cyber Sicherheit 2016, 29.

[10] *BKA*, ÖSCS, 10.

[11] Zu Deutsch: Cyber Verteidigungszentrum; kurz: CVZ.

für das BKA das GovCERT, für das BM.I das Cyber Crime Competence Center (C4) und für das BMLV das Abwehramt (AbwA), das Heeres-Nachrichtenamt (HNaA) und das milCERT.[12]

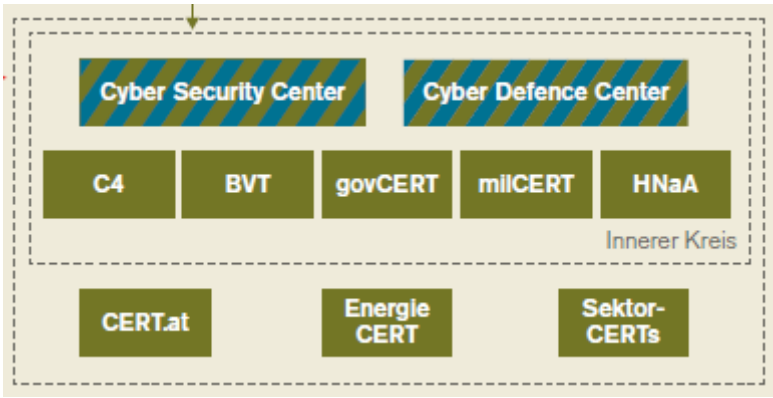

Abbildung 1: Die Operative Koordinierungsstruktur

2.1.1. BKA (GovCERT)

Im Bereich der Cybersicherheit kommen dem Bundeskanzler[13] nach dem Bundesministeriengesetz 1986 (BMG)[14] im Rahmen der Angelegenheiten der allgemeinen Regierungspolitik, einschließlich der Koordination der gesamten Verwaltung des Bundes, die Angelegenheiten der strategischen Netz- und Informationssicherheit zu.[15] Es handelt sich dabei aber nicht um operative Aufgaben wie z.B. den Austausch von CTI. Durch das BKA wird seit dem Jahr 2008 jedoch das Austrian Government Computer Emergency Response Team (GovCERT Austria) betrieben. Da es die Behandlung bzw. Verhinderung von Sicherheitsvorfällen im Bereich der

[12] *CSS*, Bericht Cyber Sicherheit 2017, 31.

[13] Der Bundeskanzler leitet gemäß Art 77 Abs 3 B-VG das BKA.

[14] Anlage 2 zu § 2, Teil 2, A.1 des Bundesgesetzes über die Zahl, den Wirkungsbereich und die Einrichtung der Bundesministerien (Bundesministeriengesetz 1986 - BMG), BGBl 1986/76 idF BGBl I 2017/164.

[15] Mit der Entschließung des Bundespräsidenten, mit der die sachliche Leitung bestimmter, zum Wirkungsbereich des Bundeskanzleramtes gehörender Angelegenheiten einem eigenen Bundesminister übertragen wird, BGBl II 2018/3, wurde dem Bundesminister im BKA die sachliche Leitung der Angelegenheiten der strategischen Netz- und Informationssicherheit übertragen.

Informations- und Kommunikationstechnologien (IKT) übernimmt[16] und Teil des IKDOK ist,[17] arbeitet das GovCERT operativ.

2.1.2. BM.I (CSC und C4)

Dem BM.I obliegen unter anderem Angelegenheiten des Sicherheitswesens, wozu insbesondere auch die Aufrechterhaltung der öffentlichen Ruhe, Ordnung und Sicherheit und die internationale polizeiliche Kooperation gehören.[18] Die Aufrechterhaltung der öffentlichen Ruhe, Ordnung und Sicherheit, ausgenommen die örtliche Sicherheitspolizei, und die erste allgemeine Hilfeleistungspflicht bilden zusammen die sogenannte Sicherheitspolizei. Gemäß § 3 des Sicherheitspolizeigesetzes (SPG)[19] umfasst die Aufrechterhaltung der öffentlichen Sicherheit u.a. die Gefahrenabwehr, den vorbeugenden Schutz von Rechtsgütern und die sicherheitspolizeiliche Beratung. Zum vorbeugenden Schutz von Rechtsgütern wiederum zählt der besondere Schutz kritischer Infrastrukturen.[20]

Im BM.I ist das CSC der zentrale Akteur in Bezug auf Cybersicherheit. Es soll Informationen über IKT-Sicherheitsvorfälle in Betrieben, die zur kritischen Infrastruktur zählen, entgegennehmen, eine Koordinierungsstelle anbieten sowie Handlungsempfehlungen für Bedarfsträger und technische Lagebilder für staatliche Entscheidungsträger bereitstellen.[21] Da das CSC eine Organisationseinheit des Bundesamtes für Verfassungsschutz und Terrorismusbekämpfung (BVT) ist, stellt das Polizeiliche Staatschutzgesetz (PStSG)[22] die primäre Rechtsgrundlage dar.[23]

---

[16] *BKA*, GovCERT in Österreich, <http://www.govcert.gv.at/home/index/index.html>.

[17] *CSS*, Bericht Cyber Sicherheit 2016, 30.

[18] Anlage 2 zu § 2, Teil 2, H.1 BMG.

[19] Bundesgesetz über die Organisation der Sicherheitsverwaltung und die Ausübung der Sicherheitspolizei (Sicherheitspolizeigesetz – SPG), BGBl 1991/566 idF BGBl 1992/662.

[20] § 22 Abs 1 Z 6 SPG; s. Kapitel 2.3.

[21] *BM.I*, Abteilung 3 (Sicherheit und Schutz), <https://www.bvt.gv.at/101/Abteilung_3/cyber_security/info.aspx>.

[22] Bundesgesetz über die Organisation, Aufgaben und Befugnisse des polizeilichen Staatsschutzes (Polizeiliches Staatsschutzgesetz – PStSG), BGBl I 2016/5.

[23] Aufgrund des PStSG kommen die Aufgaben und Befugnisse des Staatsschutzes nur noch dem BVT zu; *Salimi*, Polizeiliches Staatsschutzgesetz und Neuerungen im SPG, 1.

Die Kriminalpolizei besteht in der Wahrnehmung von Aufgaben im Dienste der Strafrechtspflege,[24] insbesondere in der Aufklärung strafbarer Handlungen nach den Bestimmungen der Strafprozessordnung 1975.[25] Obzwar die Kriminalpolizei den Sicherheitsbehörden obliegt,[26] und zwar grundsätzlich dem Bundeskriminalamt,[27] ist sie nicht Teil der Sicherheitsverwaltung.[28] In Bezug auf Cybersicherheit ist das Bundeskriminalamt für die Aufklärung gerichtlich strafbarer Handlungen, welche im Internet stattfinden (Cybercrime), zuständig. Zu diesem Zwecke ist beim Bundeskriminalamt das C4 angesiedelt.

2.1.3. BMLV (milCERT, AbwA [CDC] und HNaA)

Das BMLV ist für militärische Angelegenheiten zuständig, wobei zu den militärischen Angelegenheiten insbesondere Angelegenheiten der Besorgung der verfassungsgesetzlich festgelegten Aufgaben des Bundesheeres sowie der operativen und taktischen Führung des Bundesheeres gehören.[29] Verfassungsrechtlich obliegt dem Bundesheer die militärische Landesverteidigung.[30] In diesem Zusammenhang kommt dem BMLV der Bereich der Cyber Defence zu, welche aufgabenmäßig auf drei operative Einheiten aufgeteilt ist. So ist das military Computer Emergency Readiness Team (milCERT) das operative Cyber-Koordinierungs- und Kompetenzzentrum im Bundesheer.[31] Es ist primär für BMLV-interne Aufgabenstellungen vorgesehen und dient maßgeblich dem Schutz der militärischen IKT-Infrastruktur. Das CDC wurde als Organisationseinheit im AbwA etabliert und trägt gemeinsam mit dem milCERT zur Erfüllung von gesamtstaatlichen Aufgaben des BMLV bzw. des Bundesheeres iSd Souveränitätsschutzes im Rahmen der Umfassenden Landesverteidigung und Umfassenden Sicherheitsvorsorge bei.[32] Das

[24] § 18 Abs 1 der Strafprozeßordnung 1975 (StPO), BGBl 1975/631.

[25] § 5 Abs 2 des Bundesgesetzes über die Einrichtung und Organisation des Bundeskriminalamtes (Bundeskriminalamt-Gesetz – BKA-G), BGBl I 2002/22.

[26] § 18 Abs 2 StPO.

[27] § 4 Abs 3 BKA-G.

[28] Vgl. § 2 Abs 2 SPG.

[29] Anlage 2 zu § 2, Teil 2, I BMG.

[30] Art 79 Abs 1 B-VG.

[31] *BMLV,* milCERT ein wesentlicher Beitrag zur Cyber Defence, <http://www.bundesheer.at/truppendienst/ausgaben/artikel.php?id=1773>.

[32] *CSS,* Bericht Cyber Sicherheit 2017, 33.

HNaA ist für die Erarbeitung des strategischen Lagebildes insbesondere im Hinblick auf internationale Akteure und Entwicklungen zuständig. Dabei sollen frühzeitig potentielle Cyberbedrohungen aus dem Ausland erkannt und im Falle eines großangelegten Cyberangriffes auf nationale Infrastrukturen mit den zur Verfügung stehenden Methoden eine Identifikation der Angreifer unterstützt werden.[33]

2.2. Computer-Notfallteams

Wie in Abbildung 1 ersichtlich, gehören auch Computer-Notfallteams der Operativen Koordinierungsstruktur an. Das GovCERT wurde aufgrund seiner Zugehörigkeit bereits beim BKA thematisiert.[34]

An dieser Stelle soll daher insbesondere CERT.at als das österreichische nationale Computer-Notfallteam hervorgehoben werden. Dieses wurde im Jahr 2008 gemeinsam mit dem GovCERT vom BKA in Kooperation mit der nic.at eingerichtet.[35] CERT.at ist Ansprechpartner für IT-Sicherheit im nationalen Umfeld und gibt Warnungen, Alerts und Tipps für kleine und mittlere Unternehmen (KMU) heraus, koordiniert bei Angriffen auf Rechner auf nationaler Ebene und informiert die jeweiligen Netzbetreiber und die zuständigen lokalen Security Teams.[36] Die Zugehörigkeit betreffend ist CERT.at eine Initiative von nic.at und wird von dieser auch gesponsert.[37] In Österreich gibt es ferner eine steigende Anzahl an firmeninternen Computer-Notfallteams, wie z.B. das Raiffeisen Informatik CERT oder das A1-CERT.[38] Des Weiteren gibt es mit dem Austrian Energy CERT (AEC) bereits ein sektorenspezifisches Computer-Notfallteam.[39]

---

[33] *CSS*, Bericht Cyber Sicherheit 2017, 37.

[34] S. Kapitel 2.1.1.

[35] *CSS*, Bericht Cyber Sicherheit 2017, 35.

[36] *CERT.at*, Leitbild, <http://www.cert.at/about/missionstatement/content.html>.

[37] *CERT.at*, Zuständigkeit, <http://www.cert.at/about/scope/scope.html>.

[38] *BMDW/A-SIT*, Computer Emergency Response Teams (CERTs), <https://www.onlinesicherheit.gv.at/erste_hilfe/certs/249343.html>.

[39] *BMDW/A-SIT*, Austrian Energy CERT, <https://www.onlinesicherheit.gv.at/erste_hilfe/certs/austrian_energy_cert/249447.html>.

2.3. Kritische Infrastruktur (Privatsektor)

Aufgrund ihrer besonderen Bedeutung für das geordnete Zusammenleben und das „Funktionieren der Gesellschaft“ hat sich für jene Sektoren, die einer erhöhten Gefahr physischer und/oder virtueller Angriffe ausgesetzt sind, der Begriff „kritische Infrastruktur“ etabliert. Gemeint sind in erster Linie Sektoren (oder Teile davon) „die eine wesentliche Bedeutung für die Aufrechterhaltung wichtiger gesellschaftlicher Funktionen haben und deren Störung oder Zerstörung schwerwiegende Auswirkungen auf die Gesundheit, Sicherheit oder das wirtschaftliche und soziale Wohl der Bevölkerung oder die effektive Funktionsweise von Regierungen haben würden“[40].

Auf europäischer Ebene wurde zur Vereinheitlichung der Schutzstandards unter den Mitgliedstaaten der EU die Richtlinie 2008/114/EG[41] über die Ermittlung und Ausweisung kritischer Infrastrukturen und die Bewertung der Notwendigkeit, ihren Schutz zu verbessern, erlassen. Die Richtlinie sieht ein gemeinsames Verfahren zur Ermittlung und Ausweisung von „Europäischer kritischer Infrastrukturen“ vor.[42] Da die Vorgaben der Richtlinie jedoch nur auf die Energiewirtschaft und den Verkehr anzuwenden sind, ist der Anwendungsbereich eingeschränkt.

In Österreich wurde mit einem Ministerratsbeschluss im April 2008 ein nationales Programm zum Schutz kritischer Infrastrukturen (APCIP) lanciert, auf dessen Grundlage im November 2014 ein neuer Masterplan beschlossen wurde.[43] In die österreichische Rechtsordnung fand der Begriff der kritischen Infrastruktur erst im Jahr 2014 durch eine Novelle des SPG[44] Eingang. Gemäß § 22 Abs 1 Z 6 SPG sind kritische Infrastrukturen Einrichtungen, Anlagen, Systeme oder Teile davon, „die eine wesentliche Bedeutung für die Aufrechterhaltung der öffentlichen Sicherheit, die Funktionsfähigkeit öffentlicher Informations- und Kommunikationstechnologie, die Verhütung oder Bekämpfung von Katastrophen, den öffentlichen Gesundheitsdienst, die öffentliche Versorgung mit

---

[40] *BKA/BM.I*, Österreichisches Programm zum Schutz kritischer Infrastrukturen (APCIP), 6.

[41] Richtlinie 2008/114/EG des Rates vom 8. Dezember 2008 über die Ermittlung und Ausweisung europäischer kritischer Infrastrukturen und die Bewertung der Notwendigkeit, ihren Schutz zu verbessern, ABl L 2008/345, 75.

[42] Darunter ist gemäß Art 2 lit a der Richtlinie 2008/114/EG jede „in einem Mitgliedstaat gelegene kritische Infrastruktur, deren Störung oder Zerstörung erhebliche Auswirkungen in mindestens zwei Mitgliedstaaten hätte“, zu verstehen.

[43] *BKA*, Das österreichische Programm zum Schutz kritischer Infrastrukturen (APCIP), <https://www.bundeskanzleramt.gv.at/schutz-kritischer-infrastrukturen>.

[44] Bundesgesetz, mit dem das Sicherheitspolizeigesetz geändert wird (SPG-Novelle 2014), BGBl I 2014/43.

Wasser, Energie sowie lebenswichtigen Gütern oder den öffentlichen Verkehr haben“. Im Jahr 2015 wurde der Begriff der kritischen Infrastruktur durch das Strafrechtsänderungsgesetz 2015[45] in § 74 Abs 1 Z 11 StGB[46] auch in das Strafrecht eingeführt. Die Begriffsbestimmung in § 74 Abs 1 Z 11 StGB umfasst neben den in § 22 Abs 1 Z 6 SPG angeführten Bereichen noch die Landesverteidigung, den Schutz der Zivilbevölkerung gegen Kriegsgefahren sowie das öffentliche Abfallentsorgungs- und Kanalwesen. Dabei erfolgte eine Orientierung an der Begriffsbestimmung des Art 2 lit a der Richtlinie 2008/114/EG und berücksichtigt alle im APCIP festgelegten kritischen Sektoren.[47]

Mit der NIS-RL werden sogenannte „Betreiber wesentlicher Dienste“ (im Folgenden: BwD) in verschiedenen Sektoren adressiert, bei welchen es sich grundsätzlich um Betreiber kritischer Infrastrukturen handelt, ohne jedoch als solche bezeichnet zu werden.[48] Die Sektoren nach der NIS-RL decken sich nur zum Teil mit den § 22 Abs 1 Z 6 SPG und § 74 Abs 1 Z 11 StGB genannten Bereichen.[49] Obzwar die Begriffe daher nicht deckungsgleich sind, wird es tatsächlich die Regel sein, dass Einrichtungen, die als BwD ermittelt wurden, zugleich auch als „kritische Infrastruktur“ zu qualifizieren sind. Eine Besonderheit bei der Umsetzung der NIS-RL wird es folglich sein, dass wohl erstmals in der österreichischen Rechtsordnung rechtlich konkret – wenn auch nicht abschließend und umfassend – definiert werden wird, welche Dienste „wesentlich“ und somit als kritisch einzustufen sind.

An dieser Stelle sei noch angemerkt, dass die Eigentümer kritischer Infrastruktureinrichtungen für die (Cyber-)Sicherheit ihrer Anlagen grundsätzlich selbst verantwortlich sind. Dennoch hat der Staat bei Überschreitung einer gewissen Gefährdungsstufe bzw. ab einer gewissen Verdachtslage seiner Schutzaufgabe nachzukommen und durch öffentliche Organe zur Abwehr der Bedrohung aktiv zu werden.[50]

---

[45] BGBl I 2015/112.

[46] Bundesgesetz vom 23. Jänner 1974 über die mit gerichtlicher Strafe bedrohten Handlungen (Strafgesetzbuch – StGB), BGBl 1974/60.

[47] *Mahler*, Cyberterrorismus, 73.

[48] Vgl. *Haslinger*, Rechtliche und organisatorische Aspekte neuer Meldepflichten im Bereich der Netz- und Informationssicherheit, jusIT 2017, 218 (220).

[49] S. Kapitel 5.2.2.

[50] *Mahler*, Cyberterrorismus, 69.

3. Datenschutzrechtliche Einführung

Um die mögliche datenschutzrechtliche Betroffenheit von CTI und den Austausch von CTI datenschutzrechtlich beurteilen zu können, wird im Folgenden eine kurze Einführung in die datenschutzrechtlichen Grundlagen vorgenommen.

3.1. Europäischer Hintergrund

Auf dem Gebiet des Datenschutzes gibt es eine Reihe internationaler bzw. europarechtlicher Bestimmungen. Zunächst sei auf Art 8 Abs 1 der im Jahr 1950 in Rom unterzeichneten Europäischen Konvention zum Schutz der Menschenrechte und Grundfreiheiten (Europäische Menschenrechtskonvention; kurz: EMRK) hingewiesen, welcher lautet:

> *„Jedermann hat Anspruch auf Achtung seines Privat- und Familienlebens, seiner Wohnung und seines Briefverkehrs."*

Diese Bestimmung gewährt jedermann den Schutz der Privatsphäre.[51] Der Europäische Gerichtshof für Menschenrechte (EGMR) leitet aus dieser Bestimmung ein Recht auf Datenschutz ab.[52] Dass dieses Grundrecht nicht in absoluter Weise geschützt ist, sondern im Interesse der Allgemeinheit, oder wenn es mit anderen Grundrechten kollidiert, eingeschränkt werden kann, geht aus Abs 2 hervor, wonach der Eingriff einer öffentlichen Behörde in die Ausübung dieses Rechtes nur statthaft ist, „insoweit dieser Eingriff gesetzlich vorgesehen ist und eine Maßnahme darstellt, die in einer demokratischen Gesellschaft für die nationale Sicherheit, die öffentliche Ruhe und Ordnung, das wirtschaftliche Wohl des Landes, die Verteidigung der Ordnung und zur Verhinderung von strafbaren Handlungen, zum Schutz der Gesundheit und der Moral oder zum Schutz der Rechte und Freiheiten anderer notwendig ist". Österreich ist der EMRK im Jahr 1958 beigetreten. Seit dem Jahr 1964 ist klargestellt, dass diese in Österreich im Verfassungsrang steht und wie ein innerstaatlicher Grundrechtskatalog anzuwenden ist.[53]

---

[51] *Brühann* in *Grabitz*/*Hilf* (Hrsg) Das Recht der Europäischen Union[59], Vorbemerkung: Datenschutz und die Europäische Gemeinschaft, Rn 2.

[52] Siehe insbesondere EGMR 26.03.1987, 9248/81 (Leander), EGMR 25.03.1998, 9248/81 (Kopp), EGMR 16.02.2000, 27798/95 (Amann), EGMR 04.05.2000, 28341/95 (Rotaru).

[53] Art II Z 7 Bundesverfassungsgesetz vom 4. März 1964, mit dem Bestimmungen des Bundes-Verfassungsgesetzes in der Fassung von 1929 über Staatsverträge abgeändert und ergänzt werden, BGBl Nr 59/1964.

Eine bedeutende internationale Rechtsquelle eigens zum Datenschutz existiert mit dem Übereinkommen 108 des Europarats („Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten"; kurz: Datenschutzkonvention). Ihr Inhalt beeinflusste die Richtlinie 95/46/EG[54] („Datenschutzrichtlinie"; kurz: DSRL) wesentlich.[55] Die Datenschutzkonvention trat am 1. Oktober 1985 in Kraft und ist für Österreich seit 1. Juli 1988 rechtsverbindlich.[56] Vom Charakter her handelt es sich bei der Datenschutzkonvention um einen Mindeststandard, den Österreich völkerrechtlich verbindlich umzusetzen hat. Es lassen sich jedoch keine subjektiven Rechte des Einzelnen aus ihr ableiten. Die Bestimmungen der DSRL waren mit der Datenschutzkonvention kompatibel und gingen in einigen Punkten über diese hinaus.[57]

Abseits der EMRK und der Datenschutzkonvention ist auf europäischer Ebene mit den Art 7 und 8 der EU-Grundrechte-Charta[58] der Datenschutz primärrechtlich verankert worden. Art 7 normiert die Achtung des Privat- und Familienlebens und besagt, dass jede Person das Recht auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung sowie ihrer Kommunikation hat. Im Speziellen ist jedoch Art 8 für den Datenschutz essentiell, weil dessen Abs 1 verankert, dass jede Person das Recht auf Schutz der sie betreffenden personenbezogenen Daten hat. Art 8 Abs 2 schreibt den Grundsatz fest, dass personenbezogene nur nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden dürfen. Abs 2 normiert sohin den Grundsatz des Verbots mit Erlaubnisvorbehalt, wonach die Verarbeitung personenbezogener Daten nur dann erlaubt ist, wenn eine Einwilligung oder eine gesetzliche Grundlage dies vorsieht.[59] Ferner sieht Abs 2 die wesentlichen Betroffenenrechte vor, indem er jeder Person das Recht verleiht, Auskunft über die sie betreffenden erhobenen Daten zu erhalten und die Berichtigung der Daten zu erwirken. Art 8 Abs 3

---

[54] Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABl L 1995/281, 31.

[55] *Brühann* in *Grabitz*/*Hilf* (Hrsg) Das Recht der Europäischen Union[59], Vorbemerkung: Datenschutz und die Europäische Gemeinschaft, Rn 62.

[56] *Westphal,* Grundlagen und Bausteine des europäischen Datenschutzrechts, in *Bauer/Reimer* (Hrsg) Handbuch Datenschutzrecht, 54.

[57] *Westphal,* Grundlagen und Bausteine des europäischen Datenschutzrechts, in *Bauer/Reimer* (Hrsg) Handbuch Datenschutzrecht, 70.

[58] Charta der Grundrechte der Europäischen Union, ABl C 2012/326, 391.

[59] *Forgó*/*Zöchling-Jud,* Das Vertragsrecht des ABGB auf dem Prüfstand, 109.

normiert abschließend die Pflicht zur Überwachung der Einhaltung durch eine unabhängige Stelle. Die EU-Grundrechte-Charta schafft schließlich unabhängige Datenschutzbehörden.

Im Primärrecht findet sich darüber hinaus in Art 16 AEUV[60] eine datenschutzrechtliche Bestimmung, die eine Kompetenzgrundlage für das Datenschutzrecht in der EU schafft und ebenso die Überwachung der Einhaltung der datenschutzrechtlichen Anforderungen durch unabhängige Aufsichtsstellen vorsieht.

3.2. Datenschutz-Grundverordnung (DS-GVO)

3.2.1. Einleitung

Trotz Geltung der Datenschutzkonvention und der DSRL bestand in der EU kein einheitliches Datenschutzrecht, was bei der DSRL auf die wie bei jeder Richtlinie im Detail divergierende Umsetzung durch jeden einzelnen Mitgliedstaat zurückzuführen war.[61] U.a. weil die durch die unterschiedlichen Datenschutzniveaus in den Mitgliedstaaten entstandenen faktischen Handelsverzerrungen durch die DSRL nicht ausreichend beseitigt worden sind, präsentierte die Europäische Kommission am 25. Januar 2012 die Reform des EU-Datenschutzrechts, wodurch Europa fit für das digitale Zeitalter gemacht werden sollte.[62] Als Ergebnis der Reform des EU-Datenschutzrechts ging die Verordnung (EU) 679/2016 (im Folgenden: Datenschutz-Grundverordnung; kurz: DS-GVO)[63], die nunmehr sekundärrechtlich bedeutendste Grundlage des Datenschutzrechts, hervor. Sie trat am 25. Mai 2016 in Kraft und ist seit dem 25. Mai 2018 anwendbar.[64] Trotz ihres jungen Alters stellt die DS-GVO keine Neuerfindung des Datenschutzrechts dar, sondern übernimmt die Grundsätze für die Verarbeitung personenbezogener Daten aus der DSRL bzw. der Datenschutzkonvention.

---

[60] Vertrag über die Arbeitsweise der Europäischen Union, ABl C 2012/326, 47.

[61] *Jahnel*, Datenschutzrecht, Rz 1/15.

[62] Pressemitteilung Europäische Kommission, 25.01.2012, IP/12/46.

[63] Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG, ABl L 2016/119, 1 idF ABl L 2016/314, 72.

[64] Art 99 DS-GVO.

3.2.2. Anwendungsbereich

Zunächst ist festzuhalten, dass die DS-GVO nur auf Daten anzuwenden ist, die sich auf natürliche Personen beziehen.[65] Was den sachlichen Anwendungsbereich betrifft, ist die DS-GVO gemäß Art 2 Abs 1 auf ganz oder teilweise automatisierte Verarbeitungen personenbezogener Daten anzuwenden.[66] Vom Anwendungsbereich ausgenommen sind lediglich die Verarbeitungen im Rahmen einer Tätigkeit, die nicht in den Anwendungsbereich des Unionsrechts fällt, oder Tätigkeiten der Mitgliedstaaten im Rahmen der gemeinsamen Außen- und Sicherheitspolitik, Verarbeitungen durch natürliche Personen zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten sowie Verarbeitungen durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit.[67]

Den räumlichen Anwendungsbereich betreffend gilt die DS-GVO gemäß Art 3 Abs 1 für das Verarbeiten von personenbezogenen Daten für Tätigkeiten einer Niederlassung in der EU[68] sowie in bestimmten Fällen nach dem sogenannten Marktortprinzip[69] auch für die Verarbeitung durch einen nicht in der EU Niedergelassenen.[70]

3.2.3. Grundbegriffe

Von den Begriffsbestimmungen der DS-GVO sind für die Zwecke der Arbeit im Speziellen folgende von Relevanz:

Personenbezogene Daten sind alle Informationen, die sich auf identifizierte oder identifizierbare natürliche Personen (Menschen) beziehen, wobei eine natürliche Person als identifizierbar angesehen wird, wenn sie direkt oder indirekt, insbesondere mittels Zuordnung zu

---

[65] Vgl. Art 4 Nr 1 DS-GVO.

[66] Die DS-GVO gilt auch für die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen.

[67] Art 2 Abs 2 DS-GVO.

[68] Dabei ist es irrelevant, ob es sich um eine Niederlassung eines Verantwortlichen oder eines Auftragsverarbeiters handelt oder ob die Verarbeitung in der EU stattfindet.

[69] *Kunnert*, "Was kommt mit der neuen Datenschutz-Grundverordnung auf die Unternehmen zu?", in *Grabenwarter*/*Graf*/*Ritschl* (Hrsg), Neuerungen im europäischen Datenschutzrecht für Unternehmen (2017) 19 (24).

[70] Art 3 Abs 2 DS-GVO.

einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen (hinsichtlich der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität) identifiziert werden kann.[71]

Verarbeitung ist jeder Vorgang oder jede Vorgangsreihe im Zusammenhang mit personenbezogenen Daten, unabhängig davon, ob mit oder ohne Hilfe automatisierter Verfahren ausgeführt. Dieser denkbar weite Begriff umfasst u.a. das Erheben, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung oder Verbreitung, aber auch die Einschränkung, das Löschen oder die Vernichtung von Daten.

Verantwortlicher ist die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.[72]

Auftragsverarbeiter ist eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.[73]

Empfänger ist eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, der personenbezogene Daten offengelegt werden.[74]

3.2.4. Grundsätze

Nach den Grundsätzen für die Verarbeitung dürfen personenbezogene Daten gemäß Art 5 DS-GVO nur auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden („**Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz**“).[75] Ferner dürfen sie nur für festgelegte, eindeutige und legitime Zwecke erhoben werden und nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise

[71] Art 4 Nr 1 DS-GVO.

[72] Art 4 Nr 7 DS-GVO.

[73] Art 4 Nr 8 DS-GVO.

[74] Art 4 Nr 9 DS-GVO.

[75] Art 5 Abs 1 lit a DS-GVO.

weiterverarbeitet werden („**Zweckbindung**“).[76] Personenbezogene Daten müssen auch dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („**Datenminimierung**“)[77] und sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein („**Richtigkeit**“).[78] Hinsichtlich der Speicherung sind sie in einer Form zu speichern, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist („**Speicherbegrenzung**“).[79] Was die Datensicherheit betrifft, wird als abschließender Grundsatz normiert, dass personenbezogene Daten in einer Weise verarbeitet werden müssen, die eine angemessene Sicherheit dieser gewährleistet („**Integrität und Vertraulichkeit**“).[80] Darüber hinaus muss der Verantwortliche die Einhaltung der Grundsätze nachweisen können („**Rechenschaftspflicht**“).[81]

Die sine qua non-Bedingung einer zulässigen Datenverarbeitung ist deren Rechtmäßigkeit. Wann eine Datenverarbeitung rechtmäßig ist, wird in Art 6 DS-GVO vorgegeben. Danach ist die Verarbeitung nur rechtmäßig, wenn die betroffene Person ihre Einwilligung zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke gegeben hat,[82/83] oder die Verarbeitung für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich ist, die auf Anfrage der betroffenen Person erfolgen.[84] Als Rechtsgrundlage einer zulässigen Verarbeitung kommt ferner in Frage, dass die Verarbeitung zur Erfüllung einer rechtlichen Verpflichtung erforderlich ist, der der Verantwortliche unterliegt.[85] Eine Verarbeitung ist auch dann rechtmäßig, wenn sie erforderlich ist, um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen[86], oder für die Wahrnehmung einer Aufgabe erforderlich ist, die im öffentlichen Interesse

---

[76] Art 5 Abs 1 lit b DS-GVO.

[77] Art 5 Abs 1 lit c DS-GVO.

[78] Art 5 Abs 1 lit d DS-GVO.

[79] Art 5 Abs 1 lit e DS-GVO.

[80] Art 5 Abs 1 lit f DS-GVO.

[81] Art 5 Abs 2 DS-GVO.

[82] Art 6 Abs 1 lit a DS-GVO.

[83] Die Anforderungen an die Einwilligung werden in Art 7 f DS-GVO näher bestimmt.

[84] Art 6 Abs 1 lit b DS-GVO.

[85] Art 6 Abs 1 lit c DS-GVO.

[86] Art 6 Abs 1 lit d DS-GVO.

liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde.[87] Rechtmäßig ist die Verarbeitung ferner, wenn sie zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich ist, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen.[88]

Art 9 regelt die Verarbeitung besonderer Kategorien personenbezogener Daten. Dabei handelt es sich um „sensible Daten"[89], wie z.B. genetische oder biometrische Daten und Gesundheitsdaten. Die Verarbeitung sensibler Daten ist untersagt, wenn nicht einer der in Art 9 Abs 2 festgelegten Tatbestände dies erlaubt. Im Zusammenhang mit CTI[90] erscheint eine Verarbeitung sensibler Daten allerdings höchst unwahrscheinlich,[91] weshalb in dieser Arbeit auf die Ausnahmetatbestände vom Verarbeitungsverbot für sensible Daten nach Art 9 Abs 2 nicht näher eingegangen wird. Angemerkt sei nur, dass es eventuell bei Sicherheitsvorfällen im Sektor Gesundheitswesen zur Verarbeitung besonderer Kategorien personenbezogener Daten kommen kann.

3.3. Datenschutzrichtlinie für den Bereich Polizei und Justiz [Strafverfolgung]

Ein weiterer Eckpfeiler der Reform des EU-Datenschutzrechts ist die Richtlinie (EU) 216/680[92] (im Folgenden: Datenschutzrichtlinie für den Bereich Polizei und Justiz [Strafverfolgung]; kurz: DSRL-PJ). Wie aus dem Namen hervorgeht, enthält die DSRL-PJ Bestimmungen zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit. Sie folgt inhaltlich in weiten Teilen der DS-GVO. So gelten im Wesentlichen die gleichen Grundsätze

---

[87] Art 6 Abs 1 lit e DS-GVO.

[88] Art 6 Abs 1 lit f DS-GVO.

[89] Vgl. ErwG 10 DS-GVO.

[90] S. Kapitel 4.

[91] Ebenso erscheint die Verarbeitung von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten nach Art 10 DS-GVO im Kontext von CTI sehr unwahrscheinlich.

[92] Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates, ABl L 2016/119, 89.

in Bezug auf die Verarbeitung personenbezogener Daten.[93] Im Hinblick auf die Rechtmäßigkeit der Verarbeitung ist diese – anders als bei der DS-GVO mit ihren vielen Erlaubnistatbeständen – jedoch nur dann rechtmäßig, wenn und soweit sie für die Erfüllung einer Aufgabe erforderlich ist, die von der Behörde zu Zwecken der Strafverfolgung oder der Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit, wahrgenommenen wird und auf Grundlage des Unionsrechts oder des Rechts der Mitgliedstaaten erfolgt.[94] Die DSRL-PJ enthält an diversen Stellen weitere spezielle Regelungen. So wird bspw. vorgeschrieben, dass die Mitgliedstaaten zwischen den personenbezogenen Daten verschiedener Kategorien betroffener Personen klar zu unterscheiden haben, wie z.B. zwischen Verdächtigen, verurteilten Straftätern und Opfern.[95]

3.4. Datenschutzgesetz

Obgleich es sich bei der DS-GVO um eine in jedem Mitgliedstaat der EU unmittelbar anwendbare Verordnung handelt, enthält sie zahlreiche Öffnungsklauseln, von denen einige fakultativ und andere obligatorisch durch nationalstaatliches Recht durchzuführen sind.[96] In Österreich wurde das Datenschutzgesetz 2000[97] zur Durchführung der Öffnungsklauseln zuerst durch das Datenschutz-Anpassungsgesetz 2018[98] und zuletzt durch das Datenschutz-Deregulierungs-Gesetz 2018[99] novelliert. Das dritte Hauptstück (§§ 36-59) sowie der vierte Abschnitt des zweiten Hauptstücks (§§ 31-34) des DSG setzen die DSRL-PJ um. Abseits der Novellierungen des DSG wurden zahlreiche Materiengesetze zur Anpassung an die DS-GVO novelliert.

---

[93] Vgl. Art 4 DSRL-PJ.

[94] Art 8 Abs 1 DSRL-PJ.

[95] Art 6 DSRL-PJ.

[96] *Feiler*, Öffnungsklauseln in der Datenschutz-Grundverordnung – Regelungsspielraum des österreichischen Gesetzgebers, jusIT 2016/93, 210.

[97] Bundesgesetz über den Schutz personenbezogener Daten (Datenschutzgesetz 2000 - DSG 2000), BGBl I 1999/165.

[98] Bundesgesetz, mit dem das Datenschutzgesetz 2000 geändert wird (Datenschutz-Anpassungsgesetz 2018), BGBl I 2017/120.

[99] Bundesgesetz, mit dem das Datenschutzgesetz geändert wird (Datenschutz-Deregulierungs-Gesetz 2018), BGBl I 2018/24.

4. Cyber Threat Intelligence und ihre datenschutzrechtliche Beurteilung

Bei den Arten der zur Entdeckung und in weiterer Folge zur Abwehr bzw. Bewältigung einer Schwachstelle bzw. eines Sicherheitsvorfalles betroffenen Informationen handelt es sich in erster Linie um rein technische Informationen. So werden auf taktischer Ebene („Tactical Intelligence“) bei der Informationssammlung insbesondere Indikatoren im Zusammenhang mit einem Angreifer und der Bedrohungsart gesammelt. Die auf taktischer Ebene gesammelten Informationen werden verwendet, um das Verhalten eines Prozesses oder Akteurs während der Kompromittierung zu beobachten und zu beschreiben. Bei Angriffen kann auf diese Weise ein Lagebild in einem größeren Kontext generiert werden. Während in einem ersten Schritt nicht analysierte Bedrohungsdaten automatisiert erstellt werden können, indem IT-Sicherheits-Tools und -software verdächtige Aktivitäten erkennen und markieren („flagging“), ist in einem weiteren Schritt ein Analysevorgang der Informationen erforderlich, um den Kontext herzustellen.[100] Dazu sind im Besonderen die Indikatoren der Kompromittierung („Indicators of Compromise“; kurz: IoC) oder dokumentierte Angriffsmuster von Nutzen. Bei den Informationen handelt es sich auf Netzwerkebene konkret um E-Mail-Adressen, URLs, IP-Adressen oder Netzwerksignaturen. Dabei werden bspw. E-Mail-Adressen für Angriffe (z.B. Spear-Phishing-Attacken), URLs zum Hosten von Exploits und Malware, IP-Adressen von Command and Control-Servern bzw. von Bots, Netzwerksignaturen zur Erkennung der Kommunikation von Malware sowie Hashes als Prüfziffern zur Erkennung von Malware verwendet.[101] Ferner können durch „Scamming“ entwendete Domain-Namen verwendet werden, um E-Mails mit Spam, Viren oder Phishing-Köder zu versenden.[102] Selbiges gilt für die in Whois verfügbaren Informationen, da beim Missbrauch des Whois-Systems die öffentlichen Whois-Daten, wie z.B. Kontaktpersonen und persönliche Informationen von Registranten, für schädliche Handlungen wie Spam, Phishing, Identitätsdiebstahl oder Datendiebstahl verwendet werden.[103]

---

[100] *UK-CERT*, An introduction to threat intelligence, 10.

[101] *UK-CERT*, An introduction to threat intelligence, 11.

[102] *Krone/Smith*, Criminal misuse of the DNS, 30.

[103] *ICANNwiki*, Whois Misuse, <https://icannwiki.org/Whois_Misuse>.

Für die Netzwerksicherheit praktisch essentiell sind ferner sogenannte Logfiles. Diese protokollieren bspw. IP-Adressen, verwendete Browser, besuchte Seiten, Datum und Zeit der Zugriffe oder die von Zugreifenden genutzten Systeme, um Aktivitäten auf Netzwerken nachzuvollziehen und Fehler ausfindig machen zu können.[104]

Es ist nun zu fragen, inwiefern es sich bei solchen Informationen um personenbezogene Daten handelt. Einige dieser Informationen stellen vornehmlich rein technische Informationen ohne Personenbezug dar. So dienen Host-Namen der eindeutigen Bezeichnung eines Rechners im Netzwerk und URLs der Identifikation und Lokalisierung einer Ressource im WWW. Bei Domain-Namen und den in Whois verfügbaren Informationen wird hingegen ein expliziter Personenbezug sogar recht wahrscheinlich, weil hier u.U. der Klarname einer natürlichen Person abgebildet wird.

Doch selbst bei an sich vornehmlich technischen Informationen kann ein Personenbezug nicht ausgeschlossen werden. Das beste Beispiel hierfür sind IP-Adressen. In einem Verfahren („Breyer")[105] vor dem deutschen Bundesgerichtshof (BGH) betreffend die Zulässigkeit der Speicherung der IP-Adressen von Websitebesuchern durch den Websitebetreiber richtete der BGH die Frage an den Europäischen Gerichtshof (EuGH), ob „eine IP-Adresse, die ein Anbieter von Online-Mediendiensten im Zusammenhang mit einem Zugriff auf seine Internetseite speichert, für diesen schon dann ein personenbezogenes Datum darstellt, wenn ein Dritter (hier: Zugangsanbieter) über das zur Identifizierung der betroffenen Person erforderliche Zusatzwissen verfügt".[106] Im Kern bejahte der EuGH diese Frage und stellte fest, dass eine dynamische IP-Adresse für den Websitebetreiber „ein personenbezogenes Datum im Sinne der genannten Bestimmung darstellt, wenn er über rechtliche Mittel verfügt, die es ihm erlauben, die betreffende Person anhand der Zusatzinformationen, über die der Internetzugangsanbieter dieser Person verfügt, bestimmen zu lassen."[107] Dazu genügt es, wenn für den Anbieter rechtliche Möglichkeiten bestehen, „die es ihm erlauben, sich insbesondere im Fall von Cyberattacken an die zuständige Behörde zu wenden, damit

---

[104] Zu Logfiles generell und insbesondere den umfangreichen Anwendungen in der IT-Sicherheit s. *Friedberg*/*Wurzenberger*/*Balushi*/*Kang*, From Monitoring, Logging, and Network Analysis to Threat Intelligence Extraction, in *Skopik* (Hrsg) Collaborative Cyber Threat Intelligene (CRC Press 2018), 82 ff.

[105] EuGH 19.10.2016, C-582/14 (Breyer) = jusIT 2016/105, 252 (*Jahnel*) = jusIT 2017/9, 27 (*Kotschy*) = ZIIR 2017, 6 (*Eckhardt*) = MR-Int 2017, 73 (*Keppeler*).

[106] EuGH 19.10.2016, C-582/14 Rn 30.

[107] EuGH 19.10.2016, C-582/14 Rn 49.

diese die nötigen Schritte unternimmt, um die fraglichen Informationen vom Internetzugangsanbieter zu erlangen und die Strafverfolgung einzuleiten."[108] Aus der Entscheidung ist somit die Erkenntnis zu gewinnen, dass Informationen für deren Inhaber nicht schon dann als personenbezogene Daten einzustufen sind, wenn irgendein Dritter zur Herstellung des Personenbezugs in der Lage ist. Der Dateninhaber muss über Mittel verfügen, die vernünftigerweise eingesetzt werden könnten, um mit Hilfe Dritter (wie z.B. einer zuständigen Behörde und des Internetzugangsanbieters) die betreffende Person anhand der gespeicherten IP-Adressen bestimmen zu lassen.[109] Schlussfolgernd kann auch festgehalten werden, dass der Begriff der Bestimmbarkeit subjektiv auszulegen ist. Mit anderen Worten muss für jeden Dateninhaber individuell geprüft werden, ob er die Identität des Betroffenen bestimmen kann, womit Daten – abhängig von deren Inhaber – zugleich personenbezogen und nicht personenbezogen sein können.

Da die Entscheidung in der Sache Breyer noch zur DSRL erging, muss gefragt werden, ob die Erkenntnis auf die neue Rechtslage umgesetzt werden kann. Zur Auslegung des Begriffs der personenbezogenen Daten in Art 4 Z 1 DS-GVO ist ErwG 26 heranzuziehen, der dem bisherigen ErwG 26 zur Erläuterung des Begriffs der personenbezogenen Daten in Art 2 lit a DSRL sehr ähnlich ist: „Um festzustellen, ob eine natürliche Person identifizierbar ist, sollten alle Mittel berücksichtigt werden, die von dem Verantwortlichen oder einer anderen Person nach allgemeinem Ermessen wahrscheinlich genutzt werden, um die natürliche Person direkt oder indirekt zu identifizieren, wie beispielsweise das Aussondern." Das Wort „vernünftigerweise" wurde durch „nach allgemeinem Ermessen wahrscheinlich" ersetzt, wodurch klargestellt wird, dass es nicht bloß auf das zu erwartende Verhalten eines vernünftig handelnden Datenverwenders ankommen kann.[110] Da die Auslegung des Begriffs der personenbezogenen Daten gegenüber der alten Rechtslage voraussichtlich weitgehend unverändert bleibt, wird die Erkenntnis der Entscheidung Breyer auf die neue Rechtslage übertragen werden können.

Bei IP-Adressen bleibt noch zu ergänzen, dass diese oftmals nur mit einer gewissen Wahrscheinlichkeit einer Person zugeordnet werden können, weshalb die Frage aufgeworfen

---

[108] EuGH 19.10.2016, C-582/14 Rn 47.

[109] Vgl. EuGH 19.10.2016, C-582/14 Rn 48.

[110] Vgl. *Bergauer*, Personenbezogene Daten, in *Knyrim* (Hrsg) Datenschutz-Grundverordnung, 48.

werden kann, ob überhaupt ein Personenbezug vorliegt.[111] So teilen sich beim NAT-Verfahren in einem Netz mehrere Endgeräte, denen jeweils eine Person zugeordnet sein kann, einen gemeinsamen Zugang zum Internet, wodurch die Endgeräte nur über eine einzige im Internet sichtbare IP-Adresse verbunden sind.[112] Nach hM sind Daten aber auch dann als personenbezogen zu behandeln, wenn diese mit hoher Wahrscheinlichkeit einer Person zugeordnet werden können.[113]

Abseits der zur Entdeckung, Abwehr und Bewältigung einer Schwachstelle bzw. eines Sicherheitsvorfalles unmittelbar relevanten Informationen kommen noch weitere personenbezogene Daten in Frage, die im Zuge der Bewältigung des Sicherheitsvorfalls ausgetauscht werden. Dazu zählen insbesondere jene Daten, die aus rein praktischer Sicht für die Entgegennahme von Meldungen über Sicherheitsvorfälle notwendig sind, wie z.B. Daten der meldenden Person oder des Opfers. In Frage werden hierbei im Speziellen Identifikations- und Erreichbarkeitsdaten wie Namen, Adresse, Telefonnummern etc. kommen. Darüber hinaus sind die den Sachverhalt beschreibenden Daten von Bedeutung, wie etwa Informationen zu Zeit und Ort des Sicherheitsvorfalls.

Zusammenfassend kann festgehalten werden, dass es sich bei CTI in erster Linie um technische Informationen handelt, bei denen ein Personenbezug aber nicht ausgeschlossen werden kann. Gerade in der zeitlich angespannten Phase der Vorfallbewältigung wird kaum Zeit verbleiben, um eine rechtliche Prüfung der konkret auszutauschenden Information vorzunehmen. Unterbleibt der Austausch von CTI aus datenschutzrechtlicher Ungewissheit, ist dies der IT-Sicherheit jedoch stark abträglich, weil nur durch den Austausch von CTI und IoC Angriffsmuster erkannt werden können und ein organisationsübergreifendes Lagebild geschaffen werden kann. Zur Stärkung der Cybersicherheit bedarf es einer klaren rechtlichen Situation, denn je einfacher und rechtssicherer CTI ausgetauscht werden kann, desto rascher und effizienter kann auf Cyberangriffe reagiert und

---

[111] Zur Möglichkeit, IP-Adressen bzw. generell CTI zu anonymisieren, um den Anwendungsbereich der DS-GVO auszuschließen, sei angemerkt, dass IP-Adressen und CTI idR nur dann mit Nutzen ausgetauscht werden können, wenn sie unverändert sind; *Cormack*, Incident Response: Protecting Individual Rights Under the General Data Protection Regulation, SCRIPTed 2016, 258 (281).

[112] Vgl. *DATACOM Buchverlag*, NAT auf ITWissen.info, <http://www.itwissen.info/NAT-network-address-translation-NAT-Verfahren.html>.

[113] Vgl. *Löschnigg*, Datenschutz und Kontrolle im Arbeitsverhältnis, DRdA 2006, 459 (461); *Ennöckl*, Der Schutz der Privatsphäre in der elektronischen Datenverarbeitung, 119 f; *Jahnel*, Handbuch Datenschutzrecht, Rz 3/76 mwN.

somit die NIS gewährleistet werden.[114] Jedenfalls müssen, da nicht ausgeschlossen werden kann, dass es sich bei CTI um personenbezogene Daten handelt, für die Verarbeitung einschlägige datenschutzrechtrechtliche Grundlagen identifiziert werden.[115] Welche dies sind, wird in Kapitel 6 eruiert.

[114] *Tschohl*/*Hötzendorfer*/*Quirchmayr*/*Huber*/*Hellwig*, Die NIS-Richtlinie und der rechtliche Rahmen von CERTs, in *Schweighofer*/*Kummer*/*Hötzendorfer*/*Sorge* (Hrsg) Trend und Communities der Rechtsinformatik: Tagungsband des 20. Internationalen Rechtsinformatik Symposions IRIS 2017 (OCG 2017) 543 (550).

[115] Vgl. auch *Einzinger/Skopik*/*Fiedler*, Keine Cyber-Sicherheit ohne Datenschutz, DuD 2015, 723 (724).

5. NIS-Richtlinie

5.1. Einleitung

Die EU erachtete einen umfassenden Ansatz auf Unionsebene für erforderlich, um wirksam auf die Herausforderungen im Bereich der Sicherheit von Netz- und Informationssystemen reagieren zu können. Vor diesem Hintergrund wurde die Richtlinie (EU) 2016/1148 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen[116] (NIS-RL) erlassen. Bei der NIS-RL handelt es sich um die erste EU-weite Rechtsetzung über Cybersicherheit.[117]

Durch das Festlegen von Maßnahmen zur Erreichung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der EU soll das Funktionieren des Binnenmarkts verbessert werden.[118] Dies wird damit erklärt, dass die Verlässlichkeit und Sicherheit der Netz- und Informationssysteme von entscheidender Bedeutung für wirtschaftliche und gesellschaftliche Tätigkeiten und insbesondere für das Funktionieren des Binnenmarkts sind.[119]

Allgemein soll dieses hohe Sicherheitsniveau von Netz- und Informationssystemen im Wesentlichen erreicht werden durch eine Stärkung der Zusammenarbeit zwischen den Mitgliedstaaten (strategische Koordination und operationelle Kooperation) sowie durch die Einführung verpflichtender Sicherheitsstandards, eines angemessenen IT-Risikomanagements und der Meldepflicht signifikanter Störfälle. Konkreter sieht die NIS-RL vor, dass

- alle Mitgliedstaaten eine nationale Strategie für die Sicherheit von NIS festlegen,[120]

---

[116] Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union, ABl L 2016/194, 1.

[117] *Europäische Kommission*, The Directive on security of network and information systems (NIS Directive), <ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive>.

[118] Art 1 Abs 1 NIS-RL.

[119] ErwG 1 NIS-RL.

[120] Art 1 Abs 2 lit a NIS-RL.

- eine Kooperationsgruppe geschaffen wird, um die strategische Zusammenarbeit und den Informationsaustausch zwischen den Mitgliedstaaten zu unterstützen und zu erleichtern und Vertrauen zwischen ihnen aufzubauen,[121]
- ein Netzwerk von Computer-Notfallteams (CSIRTs-Netzwerk) geschaffen wird, um zum Aufbau von Vertrauen zwischen den Mitgliedstaaten beizutragen und eine rasche und wirksame operative Zusammenarbeit zu fördern,[122]
- Sicherheitsanforderungen und Meldepflichten für die Betreiber wesentlicher Dienste und für Anbieter digitaler Dienste vorgesehen werden,
- nationale Behörden, zentrale Anlaufstellen und CSIRTs mit Aufgaben im Zusammenhang mit der Sicherheit von Netz- und Informationssystemen benannt werden.[123]

Die NIS-RL war von den Mitgliedstaaten bis zum 9. Mai 2018 in nationales Recht umzusetzen.[124] Sie gibt in entscheidender Weise den Rechtsrahmen vor, in welchem sich die Akteure im Bereich der Cybersicherheit in Österreich zu bewegen haben.

5.2. Anwendungsbereich

5.2.1. Grundsätzliches zum Anwendungsbereich

Die NIS-RL gibt lediglich eine Mindestharmonisierung vor, d.h. die Mitgliedstaaten können Bestimmungen zur Erreichung eines höheren Sicherheitsniveaus von Netz- und Informationssystemen erlassen oder aufrechterhalten. Doch ist es den Mitgliedstaaten nicht erlaubt, Anbietern digitaler Dienste weitere Sicherheits- oder Meldepflichten aufzuerlegen.[125]

Ferner tritt die NIS-RL im Wege der „lex specialis“-Regel zurück, wenn ein sektorenspezifischer EU-Rechtsakt von den Betreibern wesentlicher Dienste oder den Anbietern digitaler Dienste auf mindestens gleichwertige Weise fordert, entweder die Sicherheit ihrer Netz- und Informationssysteme oder die Meldung von Sicherheitsvorfällen zu gewährleisten.[126]

[121] Art 1 Abs 2 lit b NIS-RL.

[122] Art 1 Abs 2 lit c NIS-RL.

[123] Art 1 Abs 2 lit e NIS-RL.

[124] Art 25 Abs 1 NIS-RL.

[125] Art 3 iVm Art 16 Abs 10 NIS-RL.

[126] Art 1 Abs 7 NIS-RL.

Dementsprechend gilt die NIS-RL explizit nicht für Unternehmen, die öffentliche Kommunikationsnetze oder öffentlich zugängliche elektronische Kommunikationsdienste iSd Richtlinie 2002/21/EG[127] bereitstellen, sowie für Vertrauensdiensteanbieter iSd Verordnung (EU) Nr 910/2014[128].[129]

Vom Anwendungsbereich der Richtlinie ausgenommen sind zudem die von den Mitgliedstaaten getroffenen Maßnahmen zum Schutz ihrer grundlegenden staatlichen Funktionen, insbesondere Maßnahmen zum Schutz der nationalen Sicherheit, einschließlich Maßnahmen zum Schutz von Informationen, deren Preisgabe nach Erachten der Mitgliedstaaten ihren wesentlichen Sicherheitsinteressen widerspricht, und zur Aufrechterhaltung von Recht und Ordnung, insbesondere zur Ermöglichung der Ermittlung, Aufklärung und Verfolgung von Straftaten.[130]

5.2.2. Betreiber wesentlicher Dienste

Die NIS-RL gilt zum einen für Betreiber wesentlicher Dienste (BwD). In gewisser Hinsicht handelt es sich dabei um Betreiber kritischer Infrastrukturen,[131] doch werden sie nicht als solche bezeichnet. Die Mitgliedstaaten haben BwD, die eine Niederlassung in ihrem Hoheitsgebiet haben, bis zum 9. November 2018 zu ermitteln.[132] In Betracht kommen dabei öffentliche oder private Einrichtungen, die in einem der in Anhang II taxativ aufgelisteten Sektoren tätig sind und den in Art 5 Abs 2 bestimmten Kriterien entsprechen.[133] Bei den Sektoren handelt es sich um Energie, Verkehr, Bankwesen, Finanzmarktinfrastrukturen, Gesundheitswesen, Trinkwasserlieferung und -versorgung sowie Digitale Infrastruktur, wobei Anhang II ferner Teilsektoren[134] und die Arten der

[127] Richtlinie 2002/21/EG des Europäischen Parlaments und des Rates vom 7. März 2002 über einen gemeinsamen Rechtsrahmen für elektronische Kommunikationsnetze und -dienste (Rahmenrichtlinie), ABl L 2002/108, 33.

[128] Verordnung (EU) Nr 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG, ABl L 2014/257, 73.

[129] Art 1 Abs 3 NIS-RL.

[130] Art 1 Abs 6 NIS-Richtlinie.

[131] S. Kapitel 2.3.

[132] Art 5 Abs 1 NIS-RL.

[133] Vgl. Art 4 Z 4 NIS-RL.

[134] Z.B. Luftverkehr im Sektor Verkehr.

Einrichtungen[135] näher bestimmt. Die drei in Art 5 Abs 2 postulierten Kriterien sind qualitativer Natur und müssen kumulativ erfüllt sein.[136] Danach muss der von der Einrichtung bereitgestellte Dienst

- für die Aufrechterhaltung kritischer gesellschaftlicher und/oder wirtschaftlicher Tätigkeiten unerlässlich sein,[137]
- die Bereitstellung abhängig von Netz- und Informationssystemen sein[138] und
- ein Sicherheitsvorfall würde eine erhebliche Störung bei der Bereitstellung dieses Dienstes bewirken. [139]

Die NIS-RL nennt somit nicht selbst konkrete BwD, sondern überlässt die Ermittlung dieser den Mitgliedstaaten, wobei sie in Anhang II bestimmte Branchen auflistet, innerhalb welcher die Betreiber zu ermitteln sind, und in Art 5 Abs 2 Kriterien vorgibt.

5.2.3. Anbieter digitaler Dienste

Ferner gilt die NIS-RL für „Anbieter digitaler Dienste“ (AdD). Ein Anbieter digitaler Dienste ist eine juristische Person, die einen digitalen Dienst anbietet.[140] Digitaler Dienst wiederum ist definiert als ein Dienst der Informationsgesellschaft[141], der einer in Anhang III genannten Art entspricht.[142] Konkret handelt es sich um Anbieter von Online-Marktplätzen, Online-Suchmaschinen und Cloud-Computing-Diensten.[143]

---

[135] Z.B. Betreiber von Handelsplätzen im Sektor Finanzmarktinfrastrukturen.

[136] *Haslinger*, jusIT 2017, 218 (221).

[137] Art 5 Abs 2 lit a NIS-Richtlinie.

[138] Art 5 Abs 2 lit b NIS-Richtlinie.

[139] Art 5 Abs 2 lit c NIS-Richtlinie; Bei der Bestimmung des Ausmaßes einer Störung gemäß Art 5 Abs 2 lit c sind sektorübergreifende Faktoren zu berücksichtigen. Diese sind in Art 6 Abs 1 geregelt und umfassen bspw. die Zahl der Nutzer oder den Marktanteil der Einrichtung.

[140] Art 4 Z 6 NIS-RL.

[141] Konkret referenziert die NIS-RL auf Art 1 Abs 1 lit b der Richtlinie (EU) 2015/1535 des Europäischen Parlaments und des Rates vom 9. September 2015 über ein Informationsverfahren auf dem Gebiet der technischen Vorschriften und der Vorschriften für die Dienste der Informationsgesellschaft, ABl L 2015/241, 1.

[142] Art 4 Z 5 NIS-RL.

[143] Die Begriffe Online-Marktplatz, Online-Suchmaschine und Cloud-Computing-Dienst werden in Art 4 Z 17 bis 19 NIS-RL definiert.

Doch sind solche AdD explizit von den Pflichten nach der NIS-RL ausgenommen, die Klein- und Kleinstunternehmen[144] sind,[145] also Unternehmen, die weniger als 50 Personen beschäftigen und deren Jahresumsatz bzw. Jahresbilanz 10 Mio. EUR nicht übersteigt.[146]

5.3. Vorgabe eines nationalen Rahmens

Kapitel II der NIS-RL schreibt einen nationalen Rahmen für die Sicherheit von Netz- und Informationssystemen in den Mitgliedstaaten vor.

5.3.1. Nationale Strategie für die Sicherheit von Netz- und Informationssystemen

Der nationale Rahmen hat zum einen eine nationale Strategie für die Sicherheit von Netz- und Informationssystemen zu umfassen, welche von den Mitgliedstaaten festzulegen ist und in welchem die strategischen Ziele und angemessene Politik- und Regulierungsmaßnahmen zu bestimmen sind, mit denen ein hohes Sicherheitsniveau von Netz- und Informationssystemen erreicht und aufrechterhalten werden soll.[147] Die nationale Strategie hat dabei u.a. einen Steuerungsrahmen zur Erreichung der Ziele und Prioritäten der nationalen Strategie, einschließlich der Aufgaben und Zuständigkeiten der staatlichen Stellen und der anderen einschlägigen Akteure, zu behandeln.[148/149]

5.3.2. Zuständige Behörde und zentrale Anlaufstelle

Als einen wesentlichen Bestandteil des nationalen Rahmens sieht die NIS-RL die Benennung entsprechender Behörden vor. So haben die Mitgliedstaaten eine (oder mehrere) für die Sicherheit von Netz- und Informationssystemen zuständige nationale Behörde zu benennen („zuständige Behörde“),[150] deren Aufgabe die Überwachung der Anwendung der Richtlinie auf nationaler Ebene ist.[151] Hierbei muss keine Behörde eigens geschaffen werden, vielmehr können die Mitgliedstaaten

---

[144] Die NIS-RL referenziert hierbei auf die Empfehlung 2003/361/EG der Kommission vom 6. Mai 2003 betreffend die Definition der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen, ABl L 2003/124, 36.

[145] Art 16 Abs 11 NIS-RL.

[146] Art 2 Abs 2 Empfehlung 2003/361/EG.

[147] Art 7 Abs 1 NIS-RL.

[148] Art 7 Abs 1 lit b NIS-RL.

[149] In Österreich wird dies eine Neufassung der ÖSCS erforderlich machen.

[150] Art 8 Abs 1 NIS-RL.

[151] Art 8 Abs 2 NIS-RL.

diese Funktion einer oder mehreren bereits bestehenden Behörden zuweisen.[152] Doch hat die zuständige Behörde zumindest die Sektoren (s. Kapitel 5.2.2.) sowie die Arten digitaler Dienste (s. Kapitel 5.2.3.) abzudecken.[153]

Ferner haben die Mitgliedstaaten eine für die Sicherheit von Netz- und Informationssystemen zuständige nationale zentrale Anlaufstelle („zentrale Anlaufstelle“)[154] zu benennen.[155] Diese dient als Verbindungsstelle zur Gewährleistung der grenzüberschreitenden Zusammenarbeit der Behörden der Mitgliedstaaten und der Zusammenarbeit mit den entsprechenden Behörden in anderen Mitgliedstaaten sowie mit der in Art 11 genannten Kooperationsgruppe und dem in Art 12 genannten CSIRTs-Netzwerk.[156] Auch hier kann diese Funktion einer bereits bestehenden Behörde zugewiesen werden. Wird nur eine zuständige Behörde benannt, so ist diese zuständige Behörde auch die zentrale Anlaufstelle.[157]

5.3.3. Computer-Notfallteams

Der nationale Rahmen für die Sicherheit von Netz- und Informationssystemen hat weiters sogenannte Computer-Notfallteams (CSIRTs)[158] zu umfassen. Jeder Mitgliedstaat hat ein oder mehrere CSIRTs zu benennen. Dabei kann ein CSIRT auch innerhalb einer zuständigen Behörde eingerichtet werden. Die CSIRTs sind für die Bewältigung von Risiken und Vorfällen nach einem genau festgelegten Ablauf zuständig.[159] Bezüglich der Anforderungen wird normiert, dass auch die CSIRTs die Sektoren sowie die Arten digitaler Dienste abzudecken haben.[160]

---

[152] Art 8 Abs 1 NIS-RL.

[153] Art 8 Abs 1 NIS-RL.

[154] Auf Englisch: Single Point of Contact; kurz: SPOC.

[155] Art 8 Abs 3 NIS-RL.

[156] Art 8 Abs 4 NIS-RL.

[157] Art 8 Abs 3 NIS-RL.

[158] Die englische Fassung der NIS-RL verwendet den in der Praxis geläufigen Begriff „Computer Security Incident Response Teams“ (kurz: CSIRTs), wobei die NIS-RL unter dem Begriff CSIRT auch Computer Emergency Response Teams (CERTs) versteht; vgl. ErwG 34.

[159] Art 9 Abs 1 NIS-RL.

[160] Darüber hinaus haben CSIRTs die Anforderungen des Anhangs I Nr 1 zu erfüllen; Art 9 Abs 1 NIS-RL.

Die Aufgaben der CSIRTs werden in Anhang I Nr 2 geregelt und sind angemessen und genau festzulegen und durch nationale Strategien und/oder Vorschriften zu stützen. Demnach umfassen die Aufgaben zumindest die

- Überwachung von Sicherheitsvorfällen auf nationaler Ebene;
- Ausgabe von Frühwarnungen und Alarmmeldungen sowie Bekanntmachung und Verbreitung von Informationen über Risiken und Vorfälle unter den einschlägigen Interessenträgern;
- Reaktion auf Sicherheitsvorfälle;
- dynamische Analyse von Risiken und Vorfällen und Lagebeurteilung;
- Beteiligung am CSIRTs-Netzwerk.[161]

Ferner haben CSIRTs Kooperationsbeziehungen zum Privatsektor aufzubauen[162] und zur Erleichterung der Zusammenarbeit die Annahme und Anwendung gemeinsamer oder standardisierter Verfahren einerseits für Abläufe zur Bewältigung von Sicherheitsvorfällen und Risiken sowie andererseits Systeme zur Klassifizierung von Sicherheitsvorfällen, Risiken und Informationen zu fördern.[163]

5.4. Meldepflichten[164] und freiwillige Meldung

5.4.1. Meldepflicht für BwD

Die BwD werden nach Art 14 Abs 3 NIS-RL verpflichtet, der zuständigen Behörde oder dem CSIRT Sicherheitsvorfälle, die erhebliche Auswirkungen auf die Verfügbarkeit der von ihnen bereitgestellten wesentlichen Dienste haben, unverzüglich zu melden. Inhaltlich betrachtet müssen die Meldungen einen Informationsgehalt aufweisen, der es der zuständigen Behörde oder dem CSIRT ermöglicht zu bestimmen, ob der Sicherheitsvorfall grenzübergreifende Auswirkungen

[161] Anhang I Nr 2 lit a NIS-RL.

[162] Anhang I Nr 2 lit b NIS-RL.

[163] Anhang I Nr 2 lit c NIS-RL.

[164] Für eine ausführliche Darstellung der Meldepflicht und möglicher Umsetzungsmöglichkeiten s. *Appl*, Netz- und Informationssicherheit im Lichte der NIS-Richtlinie, 28 ff.

hat.[165] Die NIS-RL gibt auch einige Parameter vor, welche zur Feststellung des Ausmaßes der Auswirkungen eines Sicherheitsvorfalls zu berücksichtigen sind.[166] Es handelt sich dabei um eine bloß demonstrative Aufzählung.

Kommt die zuständige Behörde oder das CSIRT auf Grund der in der Meldung bereitgestellten Informationen zu dem Schluss, dass der Sicherheitsvorfall erhebliche Auswirkungen auf die Verfügbarkeit wesentlicher Dienste in einem anderen Mitgliedstaat hat, so ist dieser Mitgliedstaat zu unterrichten. Dabei müssen jedoch die Sicherheit und das wirtschaftliche Interesse des BwD sowie die Vertraulichkeit der in der Meldung bereitgestellten Informationen gewahrt werden.[167]

Ferner sind dem meldenden BwD von der zuständigen Behörde oder dem CSIRT, wenn es den Umständen nach möglich ist, einschlägige Informationen für die weitere Behandlung der Meldung zur Verfügung zu stellen. Solche Informationen können bspw. Informationen sein, die für die wirksame Bewältigung des Sicherheitsvorfalls von Nutzen sein könnten.[168]

Die zuständige Behörde oder das CSIRT können des Weiteren die Öffentlichkeit über einzelne Sicherheitsvorfälle unterrichten, was jedoch von einem konkreten Mehrwert für diese abhängig ist. So darf die zuständige Behörde oder das CSIRT die Öffentlichkeit nur informieren, wenn die Sensibilisierung dieser zur Verhütung von Sicherheitsvorfällen oder zur Bewältigung aktueller Sicherheitsvorfälle erforderlich ist. Auch haben sie zuvor jedenfalls den meldenden BwD anzuhören.[169]

5.4.2. Meldepflicht für AdD

Die AdD trifft nach Art 16 Abs 3 NIS-RL ebenso eine Pflicht zur Meldung von Sicherheitsvorfällen. Aufgrund der fast gleichlautenden Formulierung mit der Meldepflicht für BwD ist sie in Bezug auf den Meldeweg, den Inhalt der Meldung, die Unterrichtung anderer Mitgliedstaaten und der Öffentlichkeit ident, weshalb auf die in Kapitel 5.4.1. ausgeführten Inhalte

[165] Art 14 Abs 3 NIS-RL.

[166] Z.B. die Zahl der von der Unterbrechung der Erbringung des wesentlichen Dienstes betroffenen Nutzer, die Dauer des Sicherheitsvorfalls oder die geografische Ausbreitung in Bezug auf das von dem Sicherheitsvorfall betroffene Gebiet; Art 14 Abs 4 NIS-RL.

[167] Art 14 Abs 5 Unterabsatz 1 NIS-RL.

[168] Art 14 Abs 5 Unterabsatz 2 NIS-RL.

[169] Art 14 Abs 6 NIS-RL.

verwiesen werden kann. Ein wichtiger Unterschied besteht allerdings darin, dass die Meldepflicht nur dann gilt, wenn der AdD Zugang zu den Informationen hat, die benötigt werden, um die Auswirkung eines Sicherheitsvorfalls gemessen an den Parametern zu bewerten.[170] Ferner hat die Europäische Kommission in einem Durchführungsrechtsakt[171] die Parameter zur Meldepflicht für AdD näher bestimmt.[172]

5.4.3. Freiwillige Meldung

Die NIS-RL sieht in Art 20 vor, dass Einrichtungen, die nicht als BwD ermittelt wurden und die keine AdD sind, auf freiwilliger Basis Sicherheitsvorfälle melden können.[173] Voraussetzung ist lediglich, dass die Sicherheitsvorfälle erhebliche Auswirkungen auf die Verfügbarkeit der angebotenen Dienste haben.[174] Die Mitgliedstaaten haben sodann nach dem für die BwD in Art 14 vorgesehenen Verfahren tätig zu werden.[175]

Abseits der freiwilligen Meldung nach der NIS-RL besteht ein allgemeiner Bedarf am freiwilligen Informationsaustausch, da diesem auch die Absicht zu Grunde liegt, das Verständnis von Unternehmen und Behörden zu Cybergefahren zu verbessern, auch wenn kein konkreter Sicherheitsvorfall oder Anlassfall vorliegt. So soll schon gegenseitige Hilfe und Erfahrungsaustausch zum Umgang mit Gefahren sowie zu Präventions- und Abwehrmaßnahmen

---

[170] Art 16 Abs 4 Unterabsatz 2 NIS-RL.

[171] Art 3 f der Durchführungsverordnung (EU) 2018/151 der Kommission vom 30. Januar 2018 über Vorschriften für die Anwendung der Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates hinsichtlich der weiteren Festlegung der von Anbietern digitaler Dienste beim Risikomanagement in Bezug auf die Sicherheit von Netz- und Informationssystemen zu berücksichtigenden Elemente und der Parameter für die Feststellung erheblicher Auswirkungen eines Sicherheitsvorfalls, ABl L 2018/26, 48.

[172] Art 16 Abs 9 NIS-RL.

[173] Abseits der freiwilligen Meldung iSd NIS-RL besteht ein allgemeines Bedürfnis am freiwilligen Informationsaustausch, da diesem auch die Absicht zu Grunde liegt, das Verständnis von Unternehmen und Behörden zu Cybergefahren zu verbessern, unabhängig von einem konkreten Anlassfall. So soll schon gegenseitige Hilfe und Erfahrungsaustausch zum Umgang mit Gefahren sowie zu Präventions- und Abwehrmaßnahmen bei Auffälligkeiten, die nicht auf einen Angriff zurückzuführen sein müssen, möglich sein.

[174] Art 20 Abs 1 NIS-RL.

[175] Art 20 Abs 2 NIS-RL.

bei Auffälligkeiten, die nicht auf einen Angriff oder eine technische Störung zurückzuführen sein müssen, möglich sein.[176]

5.4.4. Kooperationserfordernis

Die NIS-RL legt in Art 10 fest, dass auf nationaler Ebene eine Kooperation zu erfolgen hat, wenn die zuständige Behörde und das CSIRT getrennte Einrichtungen sind. Regelungen zur Weitergabe bzw. dem Teilen von Informationen, wie etwa der Zugang zu erfolgten Meldungen oder zumindest zu den Daten betreffend Sicherheitsvorfälle, und eine Unterrichtung der zentralen Anlaufstelle werden gefordert.[177]

Erwähnt werden soll an dieser Stelle noch, dass die Mitgliedstaaten BwD und AdD dazu anhalten sollten, Sicherheitsvorfälle mit einem Verdacht auf einen schwerwiegenden kriminellen Hintergrund den Strafverfolgungsbehörden zu melden.[178]

5.5. Datenschutzrechtliche Aspekte

Die NIS-RL enthält, wie auch die DS-GVO oder die DSRL-PJ, keine ausdrücklichen gesetzlichen Ermächtigungen für die Verarbeitung und Übermittlung personenbezogener Daten innerhalb und zwischen AdD, BwD, CSIRTs, zuständigen Behörden und anderen Stellen,[179] jedenfalls nicht im Hinblick auf die Gewährleistung der NIS als Verarbeitungszweck.

Die NIS-RL sieht in Art 2 Abs 1 lediglich vor, dass die Verarbeitung personenbezogener Daten nach Maßgabe der Richtlinie 95/46/EG erfolgt.[180] Werden personenbezogene Daten durch Organe und Einrichtungen der EU verarbeitet, so geschieht dies gemäß Art 2 Abs 2 der NIS-RL nach

---

[176] *KSÖ*, KSÖ Rechts- und Technologiedialog Whitepaper. Version 2, Wien 2016, 25 f.

[177] Art 10 Abs 2 NIS-RL; vgl. auch *Haslinger*, Rechtliche und organisatorische Aspekte neuer Meldepflichten im Bereich der Netz- und Informationssicherheit, jusIT 2017, 218 (221).

[178] ErwG 62 NIS-RL.

[179] Vgl. *Einzinger/Skopik*, Über die datenschutzrechtliche Problematik in CERTs/CSIRTs-Netzwerken, DuD 2017, 572 (573).

[180] Verweise auf die „alte" Datenschutz-Richtlinie, die mit Wirkung vom 25. Mai 2018 durch die DS-GVO aufgehoben wurde, gelten nunmehr gemäß Art 94 Abs 2 DS-VGO als Verweise auf die DS-GVO.

Maßgabe der Verordnung (EG) Nr 45/2001[181]. ErwG 72 zweiter Satz besagt nur, dass die Verarbeitung mit der Richtlinie 95/46/EG und der Verordnung (EG) Nr 45/2001 vereinbar sein sollte. Es lässt sich daher aus der NIS-RL nichts Näheres zur Lösung der datenschutzrechtlichen Problematik beim Austausch von Informationen über Vorfälle gewinnen, weil sie nur auf Rechtsakte verweist, die ohnehin Geltung haben und anzuwenden sind.[182] Art 2 der NIS-RL weist keinen eigenen Normungsgehalt auf, sondern dient vielmehr der Schaffung von Rechtssicherheit.

Zur Beleuchtung der datenschutzrechtlichen Aspekte lohnt sich jedoch ein Blick in den ursprünglichen Vorschlag für die NIS-RL[183]. Dieser sah zunächst in Art 1 Abs 5 – auch mehr dem Gedanken der Schaffung von Rechtssicherheit verpflichtet – vor, dass die Richtlinie 95/46/EG, die Richtlinie 2002/58/EG[184] und die Verordnung (EG) Nr 45/2001 unberührt bleiben. Der Richtlinienentwurf enthielt darüber hinausgehend in Art 1 Abs 6 weitere datenschutzrechtlich relevante Bestimmungen. So erörterte der Richtlinienvorschlag, dass der Austausch von Informationen über das (im Vorschlag noch so vorgesehene) Kooperationsnetz und die Meldung von Vorfällen die Verarbeitung von personenbezogenen Daten erforderlich machen könnten, und bestimmte, dass eine solche Verarbeitung personenbezogener Daten, die notwendig ist, um die mit der NIS-RL verfolgten Ziele des öffentlichen Interesses zu erreichen, von den Mitgliedstaaten nach Art 7 der Richtlinie 95/46/EG und der Richtlinie 2002/58/EG in ihrer in einzelstaatliches Recht umgesetzten Form genehmigt wird. Im zugehörigen ErwG 39 wird ferner festgehalten, dass im Hinblick auf diesen legitimen Zweck die Datenverarbeitung nicht unverhältnismäßig ist und es sich dabei nicht um einen nicht tragbaren Eingriff, der das in Art 8 der Charta der Grundrechte verbriefte Recht auf den Schutz personenbezogener Daten in ihrem Wesensgehalt antastet, handelt. Diese im Vorschlag der NIS-RL enthaltenen Bestimmungen finden sich mit Ausnahme des wenig aussagekräftigen Art 2 nunmehr in den ErwG der finalen Fassung der NIS-RL. So hält ErwG 72

---

[181] Verordnung (EG) Nr 45/2001 des Europäischen Parlaments und des Rates vom 18. Dezember 2000 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der Gemeinschaft und zum freien Datenverkehr, ABl L 2001/8, 1.

[182] Vgl. *Einzinger/Skopik*, DuD 2017, 572 (573).

[183] Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über Maßnahmen zur Gewährleistung einer hohen gemeinsamen Netz- und Informationssicherheit in der Union, KOM(2013) 48 endg.

[184] Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation, ABl L 2002/201, 37.

erster Satz fest, dass der Austausch von Informationen über Risiken und Vorfälle in der Kooperationsgruppe und im CSIRTs-Netzwerk und die Einhaltung der Verpflichtung zur Meldung von Sicherheitsvorfällen bei den zuständigen nationalen Behörden oder den CSIRTs die Verarbeitung personenbezogener Daten erfordern könnte, und anerkennt somit die möglichen datenschutzrechtlichen Fragestellungen. ErwG 72 erster Satz übernimmt in seinem Wesensgehalt demnach Art 1 Abs 6 ersten Satz des Richtlinienvorschlags.

Der Vorschlag der NIS-RL hielt vereinfacht gesagt fest, dass wenn eine Verarbeitung personenbezogener Daten beim Informationsaustausch über das Kooperationsnetz und der Meldung von Vorfällen notwendig ist, um die mit der Richtlinie verfolgten Ziele des öffentlichen Interesses zu erreichen, diese somit nach Art 7 der Richtlinie 95/46/EG[185] zulässig ist. Das explizite Anerkenntnis in Art 1 Abs 6, dass mit der NIS-RL Ziele des öffentlichen Interesses verfolgt werden, ist von entscheidender Bedeutung, weil nach Art 7 lit e 7 der Richtlinie 95/46/EG die Verarbeitung erfolgen darf, wenn sie für die Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt, erforderlich ist. Dieser Zulässigkeitstatbestand findet sich ebenso in Art 6 Abs 1 lit e DS-GVO, der diesbezüglich als „Nachfolger" von Art 7 lit e der Richtlinie 95/46/EG zu verstehen ist. Es fällt jedoch auf, dass die Nennung des öffentlichen Interesses im finalen Text der NIS-RL nicht mehr in diesem Kontext zu finden ist. Es ist dennoch von davon auszugehen, dass mit der NIS-RL öffentliche Ziele verfolgt werden. Diese Ansicht kann insbesondere aus folgendem Umstand argumentiert werden: Art 20 NIS-RL regelt die freiwillige Meldung (s. Kapitel 5.4.3.). ErwG 67 erörtert diesbezüglich, dass wenn Einrichtungen, die nicht in den Geltungsbereich der NIS-RL fallen, der Ansicht sind, „dass es im öffentlichen Interesse liegt, das Auftreten derartiger Sicherheitsvorfälle zu melden"; sie dies auf freiwilliger Basis tun können sollten. Wenn schon bei Einrichtungen, die nicht in den Anwendungsbereich der NIS-RL fallen, ein öffentliches Interesse vorliegt, ergibt sich per Größenschluss, dass das verpflichtende Melden von Sicherheitsvorfällen bei Einrichtungen, die in den Geltungsbereich der NIS-RL fallen, im öffentlichen Interesse liegt.

Zusammenfassend lassen eine Zusammenschau und ein Vergleich des Richtlinienvorschlags mit der finalen Fassung der NIS-RL folgende Schlussfolgerungen zu:

[185] Art 7 der Richtlinie 95/46/EG regelte die Grundsätze in Bezug auf die Zulässigkeit der Verarbeitung von personenbezogenen Daten und spezifizierte, unter welchen Voraussetzungen die Verarbeitung erfolgen darf.

1.) Es wird ausdrücklich anerkannt, dass es zu einer Verarbeitung personenbezogener Daten kommen kann,
   - wenn Informationen über Risiken und Vorfälle auf europäischer – und ergo auch auf nationaler Ebene – ausgetauscht werden, und
   - wenn Sicherheitsvorfälle an die zuständigen nationalen Behörden oder die CSIRTs gemeldet werden.

2.) Es wird in der NIS-RL keine Rechtsgrundlage für die Verarbeitung von personenbezogenen Daten geschaffen, sondern eine Verarbeitung ist mit den (von der NIS-RL unberührt) geltenden Datenschutzrechtsakten und deren nationalen Durchführungen bzw. Umsetzungen in Einklang zu bringen.

3.) Die NIS-RL verfolgt Ziele des öffentlichen Interesses, weshalb zur Beurteilung der Zulässigkeit der Verarbeitung von personenbezogenen Daten bei der Interessensabwägung das öffentliche Interesse zu berücksichtigen ist.

5.6. Nationale Umsetzung der NIS-RL

Obgleich die NIS-RL bis zum 9. Mai 2018 in nationales Recht umzusetzen war[186] und schon nach dem „alten" Regierungsprogramm aus dem Jahr 2013[187] ein „Bundesgesetz zur Cyber-Sicherheit" (im Folgenden: Cybersicherheitsgesetz) erarbeitet hätte werden sollen und zu diesem Zwecke eine legistische Arbeitsgruppe ihre Tätigkeit bereits im Februar 2016 aufnahm,[188] lag zum Zeitpunkt der Einreichung dieser Arbeit[189] kein öffentlicher Begutachtungs- oder gar nur Arbeitsentwurf, geschweige denn ein in Kraft befindliches Umsetzungsgesetz vor. Konsequenterweise hat die Europäische Kommission in dieser Sache am 19. Juli 2018 ein Mahnschreiben verschickt und somit das Vorverfahren zum Vertragsverletzungsverfahren gemäß Art 258 und 260 Abs 3 AEUV gegen Österreich eingeleitet.[190]

---

[186] Art 25 Abs 1 NIS-RL.

[187] *BKA*, Arbeitsprogramm der österreichischen Bundesregierung 2013-2018, 79, <https://www.justiz.gv.at/web2013/file/2c94848642ec5e0d0142fac7f7b9019a.de.0/regprogramm.pdf>.

[188] *CSS*, Bericht Cyber Sicherheit 2016, 33.

[189] Stand: August 2018.

[190] Vgl. Pressemitteilung Europäische Kommission, 19.07.2018, MEMO/18/4486.

Das Cybersicherheitsgesetz wird in entscheidendem Maße festlegen, wie sich die Cybersicherheit in Österreich in naher Zukunft gesetzlich bzw. regulatorisch darstellen wird. Dabei werden die inhaltlichen Schwerpunkte des Cybersicherheitsgesetzes maßgeblich durch die NIS-RL vorgegeben werden. So wird sich bspw. durch die nationalstaatliche Definition der BwD ergeben, welche Betreiber kritischer Infrastrukturen in Österreich konkret in den Cybersicherheits-Rechtsrahmen fallen werden. Es sei angemerkt, dass obwohl die NIS-RL in weiten Teilen eine Mindestharmonisierung vorgibt, aufgrund des politischen Willens, kein Gold Plating bei der Umsetzung von EU-Recht vorzunehmen,[191] und dessen rechtlichen Verankerung[192] nicht davon auszugehen ist, dass das Cybersicherheitsgesetz über die Inhalte der NIS-RL hinaus gehen wird.

Mangels Vorliegen eines öffentlichen Entwurfes des Cybersicherheitsgesetzes konnte bei dieser Arbeit leider nicht auf genauere Inhalte zurückgegriffen werden. Im Arbeitsprogramm der momentanen Bundesregierung finden sich zu digitalen Bedrohungen bzw. digitaler Sicherheit lediglich die Aussagen „Schaffung der notwendigen rechtlichen Rahmenbedingungen", „Weiterentwicklung des ‚Cyber Security Center' (CSC) und ‚Cybercrime Competence Center' (C4)" und „Einrichtung eines gemeinsamen nationalen Cyber-Sicherheitszentrums (NIS-Behörden)"[193]. Immerhin geht aus dem letzten Punkt hervor, dass es unterschiedliche zuständige Behörden iSd Art 8 Abs 1 NIS-RL geben wird, die in einem Cyber-Sicherheitszentrum zusammenarbeiten werden. Es wird für die Zwecke dieser Arbeit davon ausgegangen, dass es sich bei den „NIS-Behörden" um die in der Operativen Koordinierungsstruktur vertretenen Behörden handelt.

Die NIS-RL lässt bei der Meldepflicht offen, ob BwD und AdD der zuständigen Behörde oder dem CSIRT Sicherheitsvorfälle zu melden haben.[194] In diesem Zusammenhang finden sich im Bericht Cyber Sicherheit 2017 sehr relevante Hinweise auf die im Cybersicherheitsgesetz geplante organisatorische Umsetzung der in Art 14 Abs 3 und Art 16 Abs 3 NIS-RL offen gelassenen

---

[191] *BKA*, Regierungsprogramm 2017–2022, 23 <https://www.bundeskanzleramt.gv.at/documents/131008/569203/Regierungsprogramm_2017%E2%80%932022.pdf/b2fe3f65-5a04-47b6-913d-2fe512ff4ce6>

[192] § 1 Abs 4 des Deregulierungsgrundsätzegesetzes 2017, BGBl I 45/2017. Angemerkt werden muss, dass diese Vorgabe aufgrund ihrer nur einfachgesetzlichen Ausgestaltung durch übererfüllte einfachgesetzlich umgesetzte Unionsrechtsakte derogiert wird.

[193] *BKA*, Regierungsprogramm 2017–2022, 32.

[194] S. Kapitel 5.4.

Meldewege sowie der in Art 10 geforderten Kooperation. So sollen die Meldungen an sektorenspezifische Computer-Notfallteams erfolgen und von dort an das CSC weitergeleitet werden. Selbiges gilt auch für freiwillige Meldungen, wobei hier jedoch die Meldungen vor der Weiterleitung an das CSC von den sektorenspezifischen Computer-Notfallteams anonymisiert werden sollen. Zur Wahrnehmung dieser Meldestellenfunktion sieht das Cybersicherheitsgesetz die Existenz von sektorenspezifischen Computer-Notfallteams in jedem Sektor vor. Sollte es in einem Sektor kein Computer-Notfallteam geben, so erfüllt CERT.at die Aufgabe der Meldestelle.[195]

[195] *CSS*, Bericht Cyber Sicherheit 2017, 35.

6. Datenschutzrechtliche Beurteilung des Austausches von CTI zwischen den Akteuren des nationalen Rahmens

Wie eingangs in Kapitel 2 erläutert, soll CTI in einer Struktur zur Koordination auf der operativen Ebene gesammelt, gebündelt, ausgewertet und weitergegeben werden, um einen kontinuierlichen Überblick über die aktuelle Situation und ein operatives Cyberlagebild für Österreich zu erstellen. Nach der ÖSCS soll diese Struktur in ihrem inneren Kreis aus den in Kapitel 2.1. genannten Behörden bestehen. Folglich ist die datenschutzrechtliche Zulässigkeit des Austausches von CTI zwischen diesen Behörden zu prüfen.

In einem erweiterten Kreis der operativen Koordinierungsstrukturen sind die Computer-Notfallteams in die Struktur eingebunden, weshalb auch der Informationsfluss zwischen diesen und den Behörden geprüft werden muss.

Darüber hinaus wird eine Kommunikation mit dem Privatsektor, insbesondere mit den Betreibern kritischer Infrastrukturen, stattfinden. Diese Kommunikation wird einerseits im Wege von Pflichtmeldungen von Sicherheitsvorfällen und freiwilligen Meldungen von BwD und AdD an die Computer-Notfallteams erfolgen. Andererseits wird ein Rückfluss von Informationen an BwD und AdD stattfinden, weil eine Aufgabe der Computer-Notfallteams nach der NIS-RL die Ausgabe von Frühwarnungen und Alarmmeldungen sowie die Bekanntmachung und Verbreitung von Informationen über Risiken und Vorfälle unter den einschlägigen Interessenträgern ist.[196]

Die Informationsflüsse, welche in den folgenden Unterkapiteln untersucht werden sollen, werden in Abbildung 2 dargestellt:

[196] Weitere Informationsflüsse sind insbesondere zwischen Computer-Notfallteams sowie zwischen einzelnen Betreibern kritischer Infrastrukturen, und zwar auch auf internationaler Ebene, durchaus üblich. Diese Informationsflüsse datenschutzrechtlich zu untersuchen, würde den Rahmen der Arbeit sprengen. Es soll lediglich angemerkt werden, dass es zur Lösung dieses Problems in der Literatur Überlegungen gibt, bei denen unter Vorbildwirkung der Geldwäschemeldestellen, wo sich ein ähnliches datenschutzrechtliches Problem ergibt, technische Lösungen („privacy by design“) angedacht worden sind; s. dazu *Schweighofer*/*Heussler*/*Kieseberg*, Privacy by Design Data Exchange between CSIRTs, in *Schweighofer*/*Leitold*/*Mitrakas*/*Rannenberg* (Hrsg) Privacy Technologies and Policy, 5th Annual Privacy Forum, Revised Selected Papers (Springer 2017) 104.

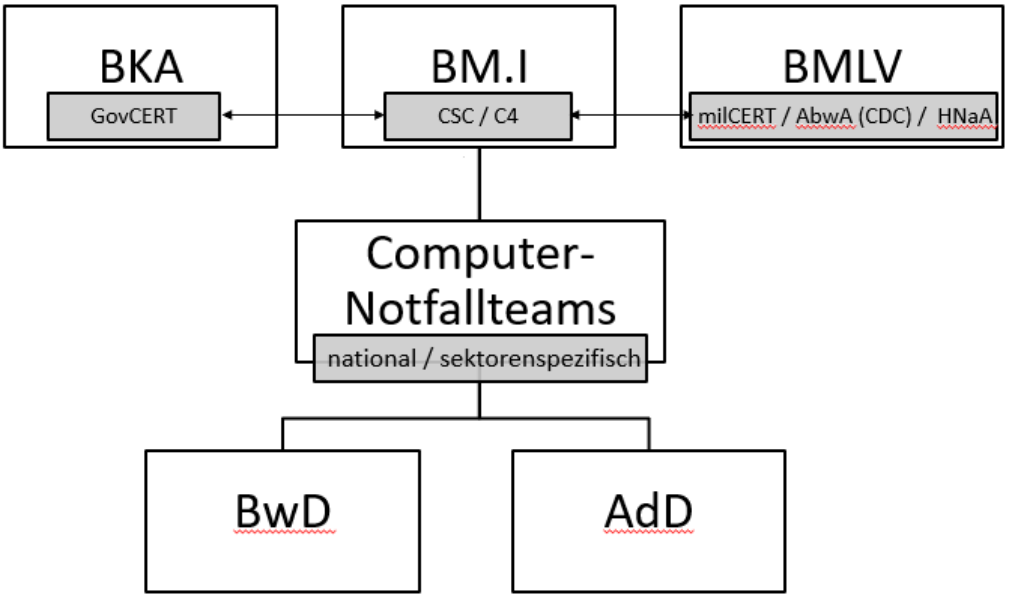

Abbildung 2: Austausch von CTI zwischen den Akteuren des nationalen Rahmens

6.1. Behörden

Von den datenschutzrechtlichen Zulässigkeitstatbeständen der DS-GVO ist im Hinblick auf die Verarbeitung von CTI als einschlägige Rechtsgrundlage Art 6 Abs 1 zu prüfen. Für Behörden kommt von den in Abs 1 genannten Bedingungen prinzipiell lit c und e in Betracht. Nach lit e ist die Verarbeitung rechtmäßig, wenn sie zur Erfüllung einer rechtlichen Verpflichtung erforderlich ist, der der Verantwortliche unterliegt. Laut lit e ist die Verarbeitung dann rechtmäßig, wenn sie für die Wahrnehmung einer Aufgabe erforderlich ist, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde. In beiden Fällen muss für die Verarbeitung eine Grundlage im Unionsrecht oder im Recht des Mitgliedstaats bestehen.[197] In dieser Rechtsgrundlage hat der Zweck der Verarbeitung bestimmt zu sein. Bei Verarbeitungen gemäß lit e muss diese für die Erfüllung einer Aufgabe erforderlich sein, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde.[198] Es ist dabei nicht vonnöten, dass für jede einzelne Verarbeitung ein spezifisches Gesetz vorhanden sein muss. Es genügt auch ein Gesetz für mehrere Verarbeitungsvorgänge, wenn die Verarbeitung aufgrund einer dem Verantwortlichen obliegenden rechtlichen Verpflichtung erfolgt

[197] Art 6 Abs 3 DS-GVO.

[198] Art 6 Abs 3 DS-GVO.

oder wenn die Verarbeitung zur Wahrnehmung einer Aufgabe im öffentlichen Interesse oder in Ausübung öffentlicher Gewalt erforderlich ist.[199]

Art 6 Abs 2 DS-GVO beinhaltet eine fakultative Öffnungsklausel,[200] wonach die Mitgliedstaaten zu lit c und e spezifischere Bestimmungen zur Anpassung der Anwendung der Vorschriften beibehalten oder einführen können, indem sie spezifische Anforderungen für die Verarbeitung sowie sonstige Maßnahmen präziser bestimmen.[201]

Infolge dieser rechtlichen Vorgaben der DS-GVO werden im Folgenden Rechtsgrundlagen für die Verarbeitung von personenbezogenen Daten durch die relevanten Behörden untersucht.

6.1.1. BKA (GovCERT)

Das BKA nimmt im Bereich der Cybersicherheit prinzipiell koordinative und strategische Aufgaben wahr. Mit dem GovCERT findet sich dennoch ein operativ tätiger Rollenträger im BKA. Nichtsdestotrotz findet sich, soweit ersichtlich, für die Einrichtung und den Betrieb des GovCERT keine eigene Rechtsgrundlage. Da keine rechtliche Verpflichtung zur Sicherstellung der Cybersicherheit die Verarbeitung erforderlich macht (vgl. lit c) und auch keine Rechtsgrundlage für die Verarbeitungen gemäß lit e vorliegt, befindet sich das GovCERT beim Austausch von CTI in einer datenschutzrechtlichen schwierigen Situation. Eventuell könnte als Grundlage nach Art 6 Abs 1 lit c DS-GVO die Pflicht zur Gewährleistung der Datensicherheit bei der Verarbeitung gemäß Art 32 DS-GVO die Verarbeitung dennoch gestatten. Da jede Verarbeitung personenbezogener Daten aber zugleich einen Eingriff in eine (sogar grundrechtlich[202]) geschützte Rechtsposition bedeutet, wären allein aufgrund des verfassungsrechtlichen Legalitätsprinzips nach Art 18 Abs 1 B-VG[203/204] die Aufgaben und Befugnisse des GovCERT rechtlich zu verankern. Es ist zu erwarten, dass eine solche Rechtsgrundlage durch das Cybersicherheitsgesetz geschaffen werden wird.

---

[199] ErwG 45 DS-GVO.

[200] *Feiler*, Öffnungsklauseln in der Datenschutz-Grundverordnung, jusIT 2016/93, 210.

[201] Art 6 Abs 2 DS-GVO.

[202] S. Kapitel 3.1.

[203] Art 18 Abs 1 B-VG: „Die gesamte staatliche Verwaltung darf nur auf Grund der Gesetze ausgeübt werden."

[204] S. dazu ausführlicher *Öhlinger*, Verfassungsrecht, 256.

6.1.2. BM.I (CSC und C4)

Für das CSC ist die zu prüfende Rechtsgrundlage das PStSG, subsidiär das SPG. Nach § 1 Abs 2 PStSG sind dem BVT im Rahmen des polizeilichen Staatsschutzes u.a. Aufgaben des Schutzes von kritischer Infrastruktur vor terroristisch, weltanschaulich oder religiös motivierter Kriminalität, vor Gefährdungen durch Spionage, durch nachrichtendienstliche Tätigkeit und durch Proliferation sowie die Wahrnehmung zentraler Funktionen der internationalen Zusammenarbeit in diesen Bereichen zugewiesen. Im Hinblick auf die Cybersicherheit relevant ist die in § 4 PStSG normierte Zentralstellenfunktionen des BVT. So fungiert das BVT nach § 4 Z 1 PStSG für den Bundesminister für Inneres als „Operative Koordinierungsstelle" für Meldungen über jede Form von Angriffen auf Computersysteme iSd § 74 Abs 1 Z 8 StGB[205] von kritischen Infrastrukturen[206] nach den Cybercrime-Delikten[207]. Kraft Rechtsgrundlage kann das CSC somit als operative Koordinierungsstelle für Meldungen über jede Form von Angriffen auf Computersysteme kritischer Infrastrukturen nach den Cybercrime-Delikten fungieren.

Als zentrale Aufgaben kommen dem BVT die erweiterte Gefahrenerforschung und der Schutz vor verfassungsgefährdenden Angriffen zu. Während § 6 Abs 1 Z 1 PStSG die erweiterte Gefahrenerforschung bei Gruppierungen definiert, regelt § 6 Abs 1 Z 2 PStSG den vorbeugenden Schutz vor verfassungsgefährdenden Angriffen durch Einzelpersonen, wobei ein begründeter Gefahrenverdacht für einen solchen Angriff bestehen muss. Die Aufgabe der erweiterten Gefahrenerforschung bei Einzelpersonen ist demnach im vorbeugenden Schutz von Rechtsgütern angesiedelt, eingeschränkt auf verfassungsgefährdende Angriffe, sofern ein begründeter Gefahrenverdacht besteht.[208] Was ein verfassungsgefährdender Angriff ist, wird in § 6 Abs 2 PStSG definiert. Für diese Arbeit relevant ist im Speziellen § 6 Abs 2 Z 5 PStSG, weil hiernach die Bedrohung von Rechtsgütern durch die rechtswidrige Verwirklichung des Tatbestandes eines

[205] Computersystem: sowohl einzelne als auch verbundene Vorrichtungen, die der automationsunterstützten Datenverarbeitung dienen; § 74 Abs 1 Z 8 StGB.

[206] § 22 Abs 1 Z 6 SPG.

[207] Konkret genannt werden die §§ 118a, 119, 119a, 126a, 126b und 126c StGB.

[208] Es müssen hinreichende Anhaltspunkte für die Annahme, dass ein verfassungsgefährdender Angriff vorbereitet werde, vorliegen. Das Erfordernis eines begründeten Gefahrenverdachts, dass der Betroffene einen verfassungsgefährdenden Angriff in absehbarer Zeit begehen werde, bedeutet mehr als die bloße Möglichkeit oder Nichtausschließbarkeit eines Angriffes, aber weniger als mit Gewissheit zu erwarten; ErläutRV 763 BlgNr 25. GP 4.

Cybercrime-Deliktes gegen kritische Infrastrukturen einen verfassungsgefährdenden Angriff darstellt. Aus datenschutzrechtlicher Sicht relevant ist, dass das CSC auf Grundlage von § 10 Abs 1 PStSG im Zuge des Ermittlungsdienstes für Zwecke des polizeilichen Staatsschutzes personenbezogene Daten sowohl für die erweiterte Gefahrenerforschung nach § 6 Abs 1 Z 1 als auch für den vorbeugenden Schutz vor verfassungsgefährdenden Angriffen nach § 6 Abs 1 Z 2 verarbeiten darf, womit eine Grundlage für das Verarbeiten von CTI im Zusammenhang mit Cyberangriffen auf kritische Infrastrukturen vorliegt.

Als spezielle Aufgabe wird in § 6 Abs 1 Z 3 PStSG der Schutz vor verfassungsgefährdenden Angriffen aufgrund von Informationen u.a. von Dienststellen inländischer Behörden zu Personen, die im Verdacht stehen, im Ausland verfassungsgefährdende Angriffe gesetzt zu haben, normiert. Unter Informationen zu Personen werden dabei auch technische Informationen zu verstehen sein. Aufgrund dieser Bestimmung können folglich Informationen vom HNaA oder dem AbwA über Personen, die der Verwirklichung eines einem verfassungsgefährdenden Angriff entsprechenden Sachverhalts im Ausland verdächtig sind, entgegengenommen werden. Diese Informationen können sodann auf Grundlage von § 10 PStSG als Aufgabe der Staatsschutzbehörden verarbeitet werden.[209] Dadurch liegt eine wichtige Grundlage für das Entgegennehmen und Verarbeiten von Informationen über aktuelle Situationen im Cyberbereich, die im Zuge nachrichtendienstlicher Aufklärung oder Abwehr gesammelt wurden, durch das BVT vor, weil Cyberkriminelle oder Cyberterroristen global und idR aus dem Ausland agieren.

Des Weiteren ist die in § 8 PStSG statuierte Aufgabe der Information verfassungsmäßiger Einrichtungen zu erwähnen. Danach hat das BVT staatsschutzrelevante Bedrohungslagen, die sich auch aus verfassungsgefährdenden Entwicklungen im Ausland ergeben können, zu analysieren und zu beurteilen und anschließend die verfassungsmäßigen Einrichtungen zu informieren.[210] Eine staatsschutzrelevante Bedrohungslage kann dabei durchaus auch die Gefährdung von kritischen Infrastrukturen durch Cybercrime-Delikte sein. Auch für diese Aufgabe liegt nach § 10 Abs 1 PStSG eine Ermächtigung zur Verarbeitung personenbezogener Daten vor.

Für die datenschutzrechtliche Prüfung ausschlaggebend sind die im 3. Hauptstück des PStSG befindlichen Normen zum Verwenden (Verarbeiten und Übermitteln) personenbezogener Daten auf

---

[209] ErläutRV 763 BlgNr 25. GP 4.

[210] Allerdings nur, sofern dadurch nicht der Vollziehungsbereich des BMLV betroffen ist; vgl. ErläutRV 763 BlgNr 25. GP 5.

dem Gebiet des polizeilichen Staatsschutzes. §§ 9 ff PStSG normieren die zentralen Befugnisse des Staatschutzes, wobei § 9 Abs 2 PStSG festhält, dass personenbezogene Daten vom BVT gemäß den §§ 10 ff PStSG nur verwendet werden dürfen, wenn dies zur Erfüllung ihrer Aufgaben notwendig ist („Aufgabenbezogenheit"). §§ 11 und 12 PStSG wirken insofern begrenzend, als sie besondere Datenverwendungsbefugnisse und besondere Voraussetzungen vorsehen. Weiters enthält § 13 PStSG Löschungsverpflichtungen

Als Aufgaben, für die Daten verwendet werden dürfen, kommen die oben beschriebenen und in §§ 6 bis 8 PStSG festgelegten Aufgaben in Frage. Nach § 9 Abs 2 bleiben Ermächtigungen nach anderen Bundesgesetzen unberührt, weshalb insbesondere die Datenverarbeitungsprivilegien der §§ 53 ff SPG in Anspruch genommen werden können.[211]

Nach § 10 Abs 3 PStSG darf das BVT Auskünfte von den Dienststellen der Gebietskörperschaften, den anderen Körperschaften des öffentlichen Rechtes und den von diesen betriebenen Anstalten verlangt werden, die sie zur Erfüllung ihrer Aufgaben nach § 10 Abs 1 Z 1 und 2 PStSG benötigen. Eine Verweigerung der Auskunft ist nur zulässig, soweit andere öffentliche Interessen überwiegen oder eine über die Amtsverschwiegenheit[212] hinausgehende sonstige gesetzliche Verpflichtung zur Verschwiegenheit besteht.

Des Weiteren kann das BVT auf Grundlage von § 10 Abs 5 PStSG zur Erfüllung seiner Aufgaben nach § 10 Abs 1 PStSG personenbezogene Daten aus allen anderen verfügbaren Quellen, insbesondere durch Zugriff auf im Internet öffentlich zugängliche Daten, ermitteln und weiterverarbeiten. Öffentlich zugängliche Daten sind nach den Materialien solche, die einem nicht im Vorhinein beschränkten Personenkreis im Internet zugänglich sind (offene Blogs, Foren, Newsgroups, auch wenn der Zugang lediglich eine Anmeldung durch Zulegen eines „Nicknames" erfordert).[213]

Zur Ermittlung von Daten für die erweiterte Gefahrenerforschung und zum vorbeugenden Schutz vor verfassungsgefährdenden Angriffen ist das BVT u.a. gemäß § 11 Abs 1 Z 5 PStSG

---

[211] Weil es den Umfang der Arbeit überschreiten würde und das CSC mit dem PStSG über eine zugeschnittene Rechtsgrundlage verfügt, wird nicht näher auf die Aufgaben und Datenverarbeitungsbefugnisse des SPG eingegangen.

[212] Art 20 Abs 3 B-VG.

[213] ErläutRV 763 BlgNr 25. GP 6.

ermächtigt, Auskünfte nach den §§ 53 Abs 3a Z 1 bis 3 und 53 Abs 3b SPG zu einer Gruppierung (§ 6 Abs 1 Z 1 PStSG) oder einem Betroffenen (§ 6 Abs 1 Z 2 PStSG) von Betreibern öffentlicher Telekommunikationsdienste[214] und sonstigen Diensteanbietern[215] einzuholen. Die Erfüllung der Aufgabe durch den Einsatz anderer Ermittlungsmaßnahmen muss dafür aber aussichtslos sein. Unter derselben Voraussetzung dürfen von Betreibern öffentlicher Telekommunikationsdienste und sonstigen Diensteanbietern weiters Auskünfte über Verkehrsdaten[216], Zugangsdaten[217] und Standortdaten[218] zu einer Gruppierung oder einem Betroffenen eingeholt werden, wenn dies zur Vorbeugung eines verfassungsgefährdenden Angriffs, dessen Verwirklichung mit beträchtlicher Strafe (§ 17 SPG) bedroht ist,[219] erforderlich erscheint.

In Bezug auf Datenanwendungen normiert § 12 PStSG, dass der Bundesminister für Inneres und die Landespolizeidirektionen als gemeinsam Verantwortliche iSd Art 26 DS-GVO in einer Datenverarbeitung zum Zwecke der Bewertung von wahrscheinlichen Gefährdungen sowie zum Erkennen von Zusammenhängen und Strukturen mittels operativer oder strategischer Analyse Daten verarbeiten dürfen. Inhaltlich dürfen nur gewisse Daten verarbeitet werden, von denen aber keine eine Relevanz in Bezug auf CTI besitzen.

Eine sehr weite Übermittlungsbefugnis wird in § 12 Abs 4 PStSG normiert. Danach sind Übermittlungen zulässig an Sicherheitsbehörden für Zwecke der Sicherheitspolizei und Strafrechtspflege, an Staatsanwaltschaften und ordentliche Gerichte für Zwecke der Strafrechtspflege, an verfassungsmäßige Einrichtungen nach Maßgabe des § 8 PStSG und darüber hinaus an Dienststellen inländischer Behörden, soweit dies eine wesentliche Voraussetzung zur Wahrnehmung einer ihr gesetzlich übertragenen Aufgabe ist.[220] Der Begriff „Dienststellen inländischer Behörden“ umfasst auch andere staatliche Rollenträger im Cybersicherheitsbereich, wie etwa das GovCERT oder milCERT.

---

[214] § 92 Abs 3 Z 1 Telekommunikationsgesetz 2003 (TKG 2003), BGBl I 2003/70.

[215] § 3 Z 2 E-Commerce-Gesetz (ECG), BGBl I 2001/152.

[216] § 92 Abs 3 Z 4 TKG 2003.

[217] § 92 Abs 3 Z 4a TKG 2003.

[218] § 92 Abs 3 Z 6 TKG 2003.

[219] Mit beträchtlicher Strafe bedroht sind gerichtlich strafbare Handlungen, die mit mehr als einjähriger Freiheitsstrafe bedroht sind; § 17 SPG.

[220] § 12 Abs 4 PStSG.

Es kann zusammenfassend festgehalten werden, dass das CSC mit dem PStSG eine sehr breite und taugliche Rechtsgrundlage iSd Art 6 Abs 2 DS-GVO besitzt, um CTI von Angriffen auf kritische Infrastrukturen zu verarbeiten und auch mit einschlägigen Akteuren austauschen zu dürfen.

Im Bereich des BM.I sei weiters kurz auf das C4 eingegangen. Dieses ist beim Bundeskriminalamt angesiedelt und übernimmt dort die Aufklärung gerichtlich strafbarer Handlungen, welche im Internet stattfinden (Cybercrime). Hierzu wird ein Ermittlungsverfahren geführt, wobei die Rolle der Kriminalpolizei in § 99 ff StPO geregelt wird. Im Zuge der Ermittlungstätigkeiten werden Informationen, die zur Aufklärung des Verdachts einer Straftat dienen, gewonnen, sichergestellt, ausgewertet und verarbeitet.[221] Bei den Informationen im Zusammenhang mit Cybercrime verarbeiteten Informationen ist jedenfalls CTI enthalten. Da das C4 gemäß § 75 StPO in seiner Rolle als Kriminalpolizei und im Rahmen seiner Aufgaben die hierfür erforderlichen personenbezogenen Daten verarbeiten, ist auch eine Verarbeitung von CTI möglich. In Bezug auf die im IKDOK vertretenen Akteure ist eine Übermittlung allerdings nur an das CSC als Sicherheitsbehörde für Zwecke der Sicherheitsverwaltung zulässig.[222]

Zum C4 kann abschließend zusammengefasst werden, dass das C4 für seine Ermittlungstätigkeiten eine sehr breite Datenverarbeitungsbefugnis besitzt, die eine Verarbeitung von CTI im Zusammenhang mit Cybercrime problemlos erlaubt, doch die Übermittlung von CTI stark eingeschränkt ist.

6.1.3. BMLV (milCERT, AbwA [CDC] und HNaA)

Die maßgebenden einfachgesetzlichen Regelungen finden sich im Wehrgesetz 2001 (WG 2001)[223] sowie im Militärbefugnisgesetz (MBG)[224]. Das WG 2001 normiert u.a. die Organisation des Wehrsystems bzw. des Bundesheeres und konkretisiert in § 2 die Aufgaben des Bundesheeres. Demnach umfasst die militärische Landesverteidigung u.a. die allgemeine Einsatzvorbereitung und

[221] Vgl. § 91 Abs 2 StPO.

[222] Vgl. § 76 Abs 4 StPO.

[223] Wehrgesetz 2001 (WG 2001), BGBl I 2001/146.

[224] Bundesgesetz über Aufgaben und Befugnisse im Rahmen der militärischen Landesverteidigung (Militärbefugnisgesetz - MBG), BGBl I 2000/86.

die unmittelbare Einsatzvorbereitung.[225] Hervorzuheben ist, dass die allgemeine Einsatzvorbereitung der Sicherstellung der ständigen Einsatzbereitschaft des Bundesheeres dient und die Schaffung aller, insbesondere personeller und materieller Voraussetzungen, die für eine unverzügliche und wirksame Durchführung eines Einsatzes erforderlich sind, umfasst.[226] Aufgrund der bloß demonstrativen Aufzählung sind daher auch Vorkehrungen immaterieller Natur und daher grundsätzlich auch einsatzbezogene Vorkehrungen in Sachen Cybersicherheit darunter zu verstehen.[227] Die unmittelbare Vorbereitung eines Einsatzes dient hingegen der Verstärkung und Erhöhung der Einsatzbereitschaft des Bundesheeres durch die hierfür erforderlichen militärischen Maßnahmen, sofern, insbesondere auf Grund der ständigen Beobachtung der militärischen und damit im Zusammenhang stehenden sicherheitspolitischen Lage, der Eintritt von Gefahren für die Unabhängigkeit nach außen oder für die Unverletzlichkeit oder Einheit des Bundesgebietes vorherzusehen ist.[228] Konsequenterweise wird eine ständige Beobachtung der militärischen und sicherheitspolitischen Lage vorausgesetzt, wobei die zu beobachtende Lage mangels einer einschränkenden Formulierung grundsätzlich auch die Dimension des Cyberraums umfasst.

Das MBG stellt die zentrale Rechtsgrundlage für militärische Organe und Dienststellen[229] dar und regelt deren Aufgaben und Befugnisse. Es listet die zu schützenden Rechtsgüter ausdrücklich in § 7 auf und ist in seinem Anwendungsbereich auf den Schutz dieser militärischen Rechtsgüter beschränkt. Von den militärischen Rechtsgütern sind für den Bereich Cybersicherheit insbesondere „Heeresgut“[230] (z.B. Server des Bundesheeres) und „militärische Geheimnisse“ (z.B. IoC)[231] von Bedeutung.[232] Der militärische Eigenschutz umfasst einerseits den Wachdienst zum Schutz vor

---

[225] § 2 Abs 2 WG 2001.

[226] § 2 Abs 3 WG 2001.

[227] *Unger/Stadlmeier/Troll*, Cyber Defence, ÖMZ 2014, 674.

[228] § 2 Abs 4 WG 2001.

[229] Unter militärischen Dienststellen sind alle Dienststellen im Vollziehungsbereich des BMLV zu verstehen; § 1 Abs 2 MBG.

[230] Heeresgut sind bewegliche Sachen, die militärischen Organen zur Erfüllung der ihnen übertragenen Aufgaben zur Verfügung stehen; § 1 Abs 4 MBG.

[231] Militärische Geheimnisse sind alle militärisch bedeutsamen Tatsachen, Erkenntnisse, Nachrichten und Vorhaben, die nur einem begrenzten Personenkreis zugänglich sind und ihrer Art nach offenbar nicht ohne Gefahr für die Erfüllung einer Aufgabe des Bundesheeres preisgegeben werden können; § 1 Abs 5 MBG.

[232] § 1 Abs 7 Z 3 MBG.

drohenden und zur Abwehr von gegenwärtigen Angriffen[233] oder vergleichbarer Tatbestände von Verwaltungsübertretungen gegen militärische Rechtsgüter[234] sowie anderseits die nachrichtendienstliche Abwehr.[235/236] Ergo unterliegen Cyberattacken dann dem militärischen Eigenschutz, wenn sie Straftatbestände (bspw. Cybercrime-Delitke) oder vergleichbare Verwaltungsübertretungen verwirklichen und dabei direkt gegen Heeresgut (bspw. militärische IT-Infrastruktur) oder gegen militärische Geheimnisse gerichtet sind.[237]

Zur Erfüllung der in §§ 20 bis 25 MBG festgelegten Aufgaben und Befugnisse der nachrichtendienstlichen Aufklärung und Abwehr sind nach der Heeresorganisation das HNaA und das AbwA, bei welchem wiederum das CDC angesiedelt ist, eingerichtet.

Die vom HNaA betriebene nachrichtendienstliche Aufklärung besteht in der Beschaffung, Bearbeitung, Auswertung und Darstellung von Informationen über das Ausland oder über internationale Organisationen oder sonstige zwischenstaatliche Einrichtungen betreffend militärische und damit im Zusammenhang stehende sonstige Tatsachen, Vorgänge und Vorhaben dient.[238] Nach den Erläuterungen umfassen diese Tatsachen, Vorgänge und Vorhaben sämtliche militärrelevanten Informationen im weiteren Sinn,[239] womit auch Informationen über den Cyberraum umfasst sind.

Die nachrichtendienstliche Abwehr ist die Aufgabe des AbwA. Sie ist in § 20 Abs 2 MBG geregelt und dient dem militärischen Eigenschutz durch die Beschaffung, Bearbeitung, Auswertung und Darstellung von Informationen über Bestrebungen und Tätigkeiten, die vorsätzliche Angriffe gegen militärische Rechtsgüter zur Beeinträchtigung der militärischen Sicherheit erwarten

---

[233] Unter Angriff ist die Bedrohung eines geschützten (militärischen) Rechtsgutes durch die rechtswidrige Verwirklichung des Tatbestandes einer gerichtlich strafbaren Handlung, die nicht bloß auf Begehren eines Beteiligten verfolgt wird, zu verstehen, einschließlich Vorbereitungshandlungen; § 1 Abs 8 MBG.

[234] § 2 Abs 1 Z 1 MBG.

[235] § 2 Abs 1 Z 2 MBG.

[236] Der militärische Eigenschutz ist subsidiär zum Schutz der öffentlichen Ordnung und Sicherheit durch die Sicherheitsbehörden, da ein Handeln nach dem MBG zur Abwehr eines Angriffes gegen militärische Rechtsgüter, der eine allgemeine Gefahr iSd § 16 SPG darstellt, nur zulässig ist, wenn und solange nicht Sicherheitsbehörden zur Gefahrenabwehr einschreiten; § 2 Abs 2 MBG.

[237] *Unger/Stadlmeier/Troll*, Cyber Defence, ÖMZ 2014, 674 (675).

[238] § 20 Abs 1 MBG.

[239] ErläutRV 76 BlgNr 21. GP 66.

lassen,.[240] Demnach soll das AbwA vorsätzliche Angriffe auf militärische Rechtsgüter und damit die Beeinträchtigung der militärischen Sicherheit[241] vorzeitig erkennen und Straftaten verhindern. Auch das Ermitteln im Vorfeld von Cyberangriffen durch das CDC ist daher Bestandteil der nachrichtendienstlichen Abwehr.

Zur Wahrnehmung ihrer Aufgaben stehen den Nachrichtendiensten mehrere Befugnisse zur Verfügung,[242] von welchen im Rahmen dieser Arbeit die Verarbeitung von Daten nach § 22 MBG von Interesse ist. Grundsätzlich dürfen militärische Organe und Dienststellen, die mit Aufgaben der nachrichtendienstlichen Aufklärung oder Abwehr betraut sind, zur Wahrnehmung der damit verbundenen Aufgaben personenbezogene Daten[243] verarbeiten.[244]

In § 25 Abs 1 MBG werden jene Voraussetzungen näher geregelt, unter denen eine Datenübermittlung im Bereich der militärischen Landesverteidigung zulässig ist. Militärische Organe und Dienststellen, die mit Aufgaben der nachrichtendienstlichen Aufklärung oder Abwehr betraut sind, dürfen Daten anderen militärischen Dienststellen übermitteln, soweit dies der Wahrung eines wichtigen öffentlichen Interesses dient.[245] Auf Grundlage dieser Datenübermittlungsbefugnis kann CTI bspw. an das milCERT übermittelt werden. Doch muss stets das Kriterium des wichtigen öffentlichen Interesses erfüllt sein, was z.B. in der Bewältigung eines Sicherheitsvorfalls, der die IT-Infrastruktur des Bundesheeres betrifft, liegen könnte. Darüber hinaus dürfen Daten an inländische Behörden übermittelt werden, soweit dies für den Empfänger eine wesentliche Voraussetzung zur Wahrnehmung einer ihm gesetzlich übertragenen Aufgabe bildet und die Übermittlung der Wahrung eines wichtigen öffentlichen Interesses dient.[246] Auf dieser Grundlage können dem BVT etwa jene personenbezogenen Daten übermittelt werden, die eine wesentliche Voraussetzung für die Wahrnehmung der Aufgabe des Schutzes vor verfassungsgefährdenden Angriffen aufgrund von Informationen von Dienststellen inländischer Behörden darstellen. Es

---

[240] § 20 Abs 2 MBG.

[241] Militärische Sicherheit ist der Schutzzustand militärischer Rechtsgüter, der der Art und Schutzwürdigkeit dieser Rechtsgüter sowie der Art und Intensität einer möglichen Gefährdung entspricht; § 1 Abs 11 MBG.

[242] S. §§6a MBG.

[243] § 36 Abs 2 Z 1 DSG.

[244] § 22 Abs 1 MBG.

[245] § 25 Abs 1 Z 1 MBG.

[246] § 25 Abs 1 Z 2 MBG.

findet sich jedoch nirgends eine Ermächtigung, personenbezogene Daten an Computer-Notfallteams zu übermitteln, die nicht bei einer inländischen Behörde eingerichtet sind.

Auffallend ist, dass bei den Datenverarbeitungsbefugnissen eine Anknüpfung für das milCERT nicht möglich ist. Da § 22 MBG nur für die nachrichtendienstliche Aufklärung oder Abwehr gilt und das milCERT nach der Heeresorganisation weder bei AbwA noch bei HNaA angesiedelt ist, kann die Verwendung personenbezogener Daten nicht auf § 22 MBG gestützt werden.[247]

Aufgrund von § 5a MBG, mit dem eine für das gesamte MBG grundlegende Regelung über die Verarbeitung personenbezogener Daten geschaffen wurde, können personenbezogene Daten zur Erfüllung der nach dem MBG festgelegten Aufgaben verarbeitet werden. Es könnte überlegt werden, ob das milCERT zum Schutz der IKT des Bundesheeres eine Aufgabe aus dem MBG ableiten könnte, um eine Verarbeitung nach § 5a MBG vornehmen zu dürfen. So läge bspw. in der Abwehr von rechtswidrigen Cyberangriffen gegen militärische Rechtsgüter eine Aufgabe des Wachdienstes vor. Problematisch ist hierbei jedoch, dass der Wachdienst prinzipiell nur Organen und nicht Dienststellen zugänglich ist,[248] weshalb allenfalls nur dem milCERT angehörige Personen diesen wahrnehmen könnten. Ferner verweist § 5a MBG auf personenbezogene Daten iSd § 55a Abs 1 Z 1 und 3 bis 5 WG 2001[249], welche jedoch kaum Bedeutung für CTI besitzen,

Zusammenfassend kann daher festgehalten werden, dass mit § 20 Abs 1 und 2 iVm § 22 Abs 1 MBG für das HNaA und das im AbwA angesiedelte CDC eine geeignete Rechtsgrundlage vorhanden ist, um personenbezogene Daten, die in CTI bei Angriffen auf militärische Rechtsgüter enthalten sein können, zu verarbeiten. Ferner ist mit der Übermittlungsbefugnis eine Kooperation mit dem CSC sichergestellt. Als rechtlich problematisch ist jedoch die schwierige Situation des milCERT zu erachten. Dieses ist zwar im IKDOK vertreten, für eine Verarbeitung oder Übermittlung von Daten sind Anknüpfungspunkte jedoch kaum gegeben.

---

[247] *Einzinger/Skopik/Fiedler*, Keine Cyber-Sicherheit ohne Datenschutz, DuD 2015, 723 (726).

[248] Vgl. § 6 Abs 2 MBG.

[249] Das sind „Grunddaten“, „Daten über Ausbildung, Beruf und Fachkenntnisse“, „Daten über Einkommen, Unterhaltsverpflichtungen und Wohnsituation“ sowie „Militärspezifische Daten“; ErläutRV 65 BlgNr 26. GP 177.

6.1.4. Kooperation im Wege der Amtshilfe

Bisher wurde geprüft, inwieweit die oben genannten Akteure für Zwecke der Gewährleistung der Cybersicherheit rechtmäßig Daten verarbeiten dürfen. Aufgrund der Befugnisse ist es jedoch grundsätzlich möglich, dass insbesondere das CSC und das CDC einander CTI, die personenbezogene Daten enthält, übermitteln. Hinsichtlich der anderen Akteure, wie z.B. milCERT und GovCERT, könnte ein kooperatives Arbeiten im IKDOK auf Grundlage des Rechtsinstituts der Amtshilfe überlegt werden. So sind nach Art 22 B-VG alle Organe des Bundes, der Länder, der Gemeinden und der Gemeindeverbände sowie der sonstigen Selbstverwaltungskörper im Rahmen ihres gesetzmäßigen Wirkungsbereiches zur wechselseitigen Hilfeleistung verpflichtet. Wegen der rechtlichen Verpflichtung der ersuchten Behörde könnte eine Zulässigkeit der Datenverarbeitung und damit der Austausch von CTI auf Grundlage von Art 6 Abs 1 lit c DS-GVO begründet werden. Dennoch tritt hier das Problem auf, dass Amtshilfe stets ein Ersuchen voraussetzt.[250] Dies ist einer dauerhaften Koordination auf der operativen Ebene abträglich, weil dadurch kein unverzüglicher Austausch aktueller Informationen über Cybersicherheitsvorfälle sichergestellt werden kann. Da Amtshilfe nur eine ergänzende Unterstützung im Ausnahmefall[251] sein darf und eine regelmäßige Zusammenarbeit zwischen Behörden auf ihrer Grundlage nicht institutionalisiert werden darf,[252] womit die Errichtung von Datenverbünden mit direkten Abfragemöglichkeiten auf Basis von Art 22 B-VG nicht möglich sein sollen.

6.1.5. Gemeinsame Verantwortliche

Trotz der Übermittlungsbefugnis insbesondere zwischen CSC und CDC fehlt für eine umfassendere Behandlung im IKDOK eine Rechtsgrundlage. So sehen schon die bestehenden Rechtsnormen nicht eigens die Gewährleistung von Cybersicherheit als Aufgabe und Verarbeitungszweck vor. Vielmehr ist der Bereich Cybersicherheit über die Abwehr von allgemeiner Gefahr in Form von Cyberangriffen, die einem Cybercrime-Delikt des StGB entsprechen (und für die Anwendung des PStSG gegen kritische Infrastruktur gerichtet sein müssen) bzw. beim BMLV über Cyberangriffe auf Heeresgut oder militärische Geheimnisse, wobei hierbei insbesondere die Aufgaben und Befugnisse der nachrichtendienstlichen Aufklärung und Abwehr in Frage kommen, geregelt.

---

[250] *Wiederin* in *Korinek*/*Holoubek* (Hrsg) Österreichisches Bundesverfassungsrecht. Kommentar Art 22 Rz 13.

[251] *Wiederin* in Österreichisches Bundesverfassungsrecht Art 22 Rz 12.

[252] *Wiederin* in Österreichisches Bundesverfassungsrecht, Art 22 Rz 14.

Für eine umfassende Behandlung von CTI im IKDOK wäre daher eine eigene Rechtsgrundlage vonnöten. Datenschutzrechtlich wird in Art 26 DS-GVO die Möglichkeit dazu geboten. Art 26 DS-GVO sieht vor, dass wenn zwei oder mehr Verantwortliche gemeinsam die Zwecke und die Mittel der Verarbeitung festlegen, diese gemeinsam Verantwortliche sind. Es handelt sich dabei um eine Öffnungsklausel, von der folglich durch das Cybersicherheitsgesetz Gebrauch gemacht werden könnte. Denkbar wäre die Schaffung einer Rechtsgrundlage zum Zwecke der behördenübergreifenden Analyse der Cybersicherheitslage auf Basis der von den Akteuren gesammelten und zur Verfügung gestellten CTI. Hierbei könnte eine Orientierung an der in § 12 PStSG statuierten Datenverarbeitung zum Zwecke der Bewertung von wahrscheinlichen Gefährdungen sowie zum Erkennen von Zusammenhängen und Strukturen mittels operativer oder strategischer Analyse erfolgen.

6.2. Computer-Notfallteams

Computer-Notfallteams werden nach der NIS-RL konkrete Aufgaben zugewiesen,[253] bei deren Erfüllung sie CTI verarbeiten werden. In einem realistischen Szenario werden Computer-Notfallteams bspw. vor IP-Adressen warnen, von denen DDoS-Attacken[254] ausgehen, weil eine ihrer Aufgaben die Ausgabe von Frühwarnungen und Alarmmeldungen sowie die Bekanntmachung und Verbreitung von Informationen über Risiken und Vorfälle unter den einschlägigen Interessenträgern ist. Die Verarbeitung von personenbezogenen Daten durch die Computer-Notfallteams kann daher nicht ausgeschlossen werden. Von den Zulässigkeitstatbeständen des Art 6 Abs 1 DS-GVO kommen für Computer-Notfallteams insbesondere lit c, e und f in Frage.

Nach lit c ist die Verarbeitung rechtmäßig, wenn sie zur Erfüllung einer rechtlichen Verpflichtung erforderlich ist, der der Verantwortliche unterliegt. Bei der Umsetzung der NIS-RL werden im Cybersicherheitsgesetz aufgrund des Legalitätsprinzips die Aufgaben und Befugnisse der Computer-Notfallteams gemäß Art 9 iVm Anhang I Nr 2 NIS-RL normiert werden müssen. Da

[253] S. Kapitel 5.3.3.

[254] Bei Denial of Service-Attacken werden Server mit einer hohen Anzahl von Anfragen derart überlastet, dass sie für Nutzer nicht mehr verfügbar sind. Bei Distributed Denial of Service-Attacken gehen diese Anfragen verteilt von einer großen Anzahl infizierter Systeme (“Bots”) aus; s. ausführlich dazu NCCIC, Understanding Denial-of-Service Attacks. Security Tip (ST04-015), <https://www.us-cert.gov/ncas/tips/ST04-015>.

bereits bekannt ist,[255] dass die Pflichtmeldungen an sektorenspezifische Computer-Notfallteams bzw. an CERT.at erfolgen und von dort an das CSC weitergeleitet werden sollen, werden die Computer-Notfallteams aus verfassungsrechtlicher Sicht zur Wahrnehmung der im Cybersicherheitsgesetz festzulegenden Aufgaben und Befugnisse „beliehen“[256] werden. Zwar sind lit c grundsätzlich auf Behörden anzuwenden, doch es können die Bestimmungen auch auf eine andere unter das öffentliche Recht fallende natürliche oder juristische Person angewendet werden.[257] Das Computer-Notfallteam wäre dann trotz seiner Einrichtung in Formen des Privatrechts und im Hinblick auf die Weiterleitung der Meldepflicht in Vollziehung der Gesetze tätig und somit ein Verantwortlicher des öffentlichen Bereichs gemäß § 26 Abs 1 Z 2 DSG. Es könnte folglich argumentiert werden, dass mit der Auslagerung der hoheitlichen Aufgaben im Wege der Beleihung die Computer-Notfallteams einerseits verpflichtet werden, Meldungen weiterzuleiten, und andererseits funktional dem Staat zuzuordnen sind und in diesem Sinne unter das öffentliche Recht fallen. Konsequenterweise würden sie daher Daten verarbeiten, die erforderlich sind, um eine rechtliche Verpflichtung zu erfüllen (lit c). Nach lit e ist die Verarbeitung ferner dann rechtmäßig, wenn sie für die Wahrnehmung einer Aufgabe erforderlich ist, die im öffentlichen Interesse liegt. Da die NIS-RL Ziele des öffentlichen Interesses verfolgt, kann bei der Beurteilung der Zulässigkeit der Verarbeitung von personenbezogenen Daten bei der Interessensabwägung das öffentliche Interesse auch hier herangezogen werden. Allerdings muss die Rechtsgrundlage für die Verarbeitungen gemäß lit c und e durch Unionsrecht oder das Recht der Mitgliedstaaten festgelegt werden. Da die NIS-RL nicht unmittelbar anzuwenden ist[258] und sie in Österreich noch nicht umgesetzt wurde, können lit c und e als Rechtmäßigkeitsgrundlage derzeit nicht herangezogen werden. De lege ferenda können Computer-Notfallteams jedoch prinzipiell aufgrund von lit c oder e personenbezogene Daten verarbeiten, wenn im Zuge der Umsetzung der NIR-RL eine ausdrückliche gesetzliche Grundlage geschaffen wird – wovon im Hinblick auf die hoheitlichen

[255] S. Kapitel 5.6.

[256] Unter „Beleihung“ wird die Übertragung von Aufgaben der Hoheitsverwaltung auf natürliche oder juristische Personen des Privatrechts verstanden. Dabei werden die Aufgaben im eigenen Namen und in eigener Verantwortung der Personen des Privatrechts besorgt. In einem funktionellen Sinn handeln sie als Behörden, sind jedoch nicht in den Organisationsapparat des Staates eingegliedert. Das Rechtsinstitut der Beleihung stellt eine Form der mittelbaren Verwaltung dar; *Stelzer*, Grundzüge des Öffentlichen Rechts, 76.

[257] ErwG 45 DS-GVO.

[258] Vgl. Art 288 Unterabsatz 3 AUEV.

Aufgaben, die sie wahrnehmen sollen, iVm dem Legalitätsprinzip ausgegangen werden kann –, die sie dazu ermächtigt, personenbezogene Daten zu verarbeiten, sofern dies zur Erfüllung ihrer Aufgaben erforderlich ist.

Sohin bleibt de lege lata Art 6 Abs 1 lit f DS-GVO als Rechtsmäßigkeitstatbestand zu prüfen. Nach lit f ist die Verarbeitung rechtmäßig, wenn sie zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich ist, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt. Bei diesem Dritten könnte es sich bspw. um ein angegriffenes Unternehmen handeln. Es ist daher zu fragen, ob die Gewährleistung von Cybersicherheit ein berechtigtes Interesse darstellen kann. Diese Frage kann klar bejaht werden, weil die DS-GVO hierzu selbst eine Aussage trifft. Denn in ErwG 49 DS-GVO wird ausgeführt, dass die Verarbeitung von personenbezogenen Daten für die Gewährleistung der Netz- und Informationssicherheit prinzipiell ein berechtigtes Interesse von Computer-Notfallteams[259] darstellen kann. Unter Netz- und Informationssicherheit wird dabei die Gewährleistung der Fähigkeit eines Netzes oder Informationssystems verstanden, „mit einem vorgegebenen Grad der Zuverlässigkeit Störungen oder widerrechtliche oder mutwillige Eingriffe abzuwehren, die die Verfügbarkeit, Authentizität, Vollständigkeit und Vertraulichkeit von gespeicherten oder übermittelten personenbezogenen Daten sowie die Sicherheit damit zusammenhängender Dienste, die über diese Netze oder Informationssysteme angeboten werden bzw. zugänglich sind, beeinträchtigen.“ Im ErwG werden zudem Beispiele angeführt, wann ein solches berechtigtes Interesse vorliegen könnte. So wäre etwa die Verhinderung des Zugangs Unbefugter zu elektronischen Kommunikationsnetzen und die Verbreitung von Malware, aber auch die Abwehr von DDoS-Attacken, sowie von Schädigungen von Computer- und elektronischen Kommunikationssystemen ein berechtigtes Interesse. Die Verarbeitung muss zur Erreichung des Zwecks jedoch unbedingt notwendig und verhältnismäßig sein. Gemäß Art 6 Abs 1 lit f DS-GVO ist die Verarbeitung auch dann nicht rechtmäßig, wenn die berechtigten Interessen des Verantwortlichen durch die Interessen oder Grundrechte und -freiheiten der betroffenen Person

[259] Konkret wird der Begriff “Computer-Notdienste”, der im ErwG den Begriffen CERT und CSIRT gleichgesetzt wird, verwendet.

außer Kraft gesetzt werden. Es muss daher eine Interessensabwägung durchgeführt werden,[260] was auf Einzelfallbasis zu geschehen hat. Diesbezüglich kann aber zweifelsohne argumentiert werden, dass die Interessen eines Computer-Notfallteams (aber auch eines Betreibers kritischer Infrastruktur, der Opfer einer Cyberattacke ist), Daten zum Zwecke des Schutzes der IT-Systeme bzw. zur Abwehr einer Cyberattacke zu verarbeiten und auszutauschen, nicht durch die Interessen einer Person, dessen System eine angreifende IP-Adresse allokiert ist, überwogen werden können.[261]

Der ErwG referenziert auf „Computer-Notdienste" und nicht auf konkrete Einrichtungen. Doch darf daraus nicht gefolgert werden, dass alle Einrichtungen, die (den undefinierten Begriff) „Computer-Notdienste" erbringen, sich auf ErwG 49 stützen können. Da in der Klammer auf CERTs und CSIRTs verwiesen wird, werden hier in erster Linie Computer-Notfallteams adressiert. Hierbei ist dagegen eine Differenzierung, ob es sich um firmeninterne, regionale, nationale oder sektorenspezifische Computer-Notfallteams, unerheblich. Demzufolge könnte die Überlegung angestellt werden, ob nicht auch das GovCERT, welches ja Computer-Notdienste anbietet, mit ErwG 49 eine Argumentationsbasis für ein berechtigtes Interesse und somit einen Zulässigkeitstatbestand begründen könnte, zumal in ErwG 49 explizit auch Behörden als Verantwortliche genannt werden.[262] Da im ErwG Behörden genannt sind, könnte überhaupt die Überlegung angestellt werden, ob sich nicht auch die nach der NIS-RL in Zukunft für die NIS zuständigen Behörden auf ErwG 49 stützen könnten.

Dementgegen muss auf eine Paradoxie hingewiesen werden. Denn obwohl ErwG 49 Behörden im Zusammenhang mit dem berechtigten Interesse nach Art 6 Abs 1 lit f DS-GVO nennt, besagt Art 6 Abs 1 Unterabsatz 2, dass lit f „nicht für die von Behörden in Erfüllung ihrer Aufgaben vorgenommene Verarbeitung" gilt.[263] Da Art 296 AEUV vorschreibt, dass Rechtsakte der EU mit

---

[260] *Cormack*, Incident Response: Protecting Individual Rights Under the General Data Protection Regulation, SCRIPTed 2016, 258 (271).

[261] Vgl. *Schweighofer/Heussler/Hötzendorfer*, Implementation Issues and Obstacles from a Legal Perspective, in *Skopik* (Hrsg) Collaborative Cyber Threat Intelligene, 318.

[262] Überdies werden in ErwG 49 Betreiber von elektronischen Kommunikationsnetzen und -diensten und Anbieter von Sicherheitstechnologien und -diensten genannt.

[263] Dem liegt laut ErwG 47 die Überlegung zu Grunde, dass es dem Gesetzgeber obliegt, durch Rechtsvorschrift die Rechtsgrundlage für die Verarbeitung personenbezogener Daten durch die Behörden zu schaffen, weshalb lit f nicht für Verarbeitungen durch Behörden gelten soll, die sie in Erfüllung ihrer Aufgaben vornehmen.

einer Begründung zu versehen sind, werden die ErwG Teil des Rechtsakts und sind somit sehr wichtig für die Interpretation. Doch sollten Widersprüche zwischen ErwG und Artikel bestehen, so hat der Artikeltext unmittelbar Vorrang.[264] Zum Verhältnis von Artikel und ErwG vertritt der EuGH in ständiger Rechtsprechung die Ansicht, „dass die Begründungserwägungen eines Gemeinschaftsrechtsakts rechtlich nicht verbindlich sind und weder herangezogen werden können, um von den Bestimmungen des betreffenden Rechtsakts abzuweichen, noch, um diese Bestimmungen in einem Sinne auszulegen, der ihrem Wortlaut offensichtlich widerspricht."[265]

Im Falle, dass es sich tatsächlich um einen Widerspruch handelt, käme dem Wort „Behörden" im ErwG keinerlei Bedeutung zu.[266] Folglich könnte sich auch das GovCERT nicht auf ErwG 49 beziehen, weil das GovCERT innerhalb einer Behörde angesiedelt ist.

Es könnte aber auch denkbar sein, dass der Unionsrechtsgeber davon ausgegangen ist, dass Behörden idR die Gewährleistung der Netz- und Informationssicherheit nicht als eigene Aufgabe zugeschrieben wird. Wenn gemäß Art 6 Abs 1 Unterabsatz 2 das berechtigte Interesse nur nicht von Behörden herangezogen werden kann, wenn sie Daten in Erfüllung ihrer Aufgaben verarbeiten, die Gewährleistung der Netz- und Informationssicherheit aber einer Behörde üblicherweise nicht explizit durch Rechtsvorschrift als Aufgabe zugewiesen wird, wäre eine Verarbeitung zur Gewährleistung der Netz- und Informationssicherheit der Behörde als Zulässigkeitstatbestand gemäß Art 6 Abs 1 lit f zugänglich.

Zusammenfassend kann festgehalten werden, dass Computer-Notfallteams, jedenfalls sofern sie nicht innerhalb einer Behörde angesiedelt sind, auf Grundlage eines berechtigten Interesses Daten zur Gewährleistung der Cybersicherheit verarbeiten dürfen. Mit Umsetzung der NIS-RL werden sie voraussichtlich eine eigene Rechtsgrundlage zur Wahrnehmung ihrer Aufgaben erhalten bzw. zu bestimmten Aufgaben verpflichtet werden, weswegen auch Art 6 Abs 1 lit c und e als Rechtsgrundlagen in Betracht kommen könnten.

---

[264] *Pollirer/Weiss/Knyrim/Haidinger*, DSGVO – Datenschutz-Grundverordnung, III-IV.

[265] EuGH 19.06.2014, C‑345/13 (Karen Millen Fashions) Rn 31 mwN.

[266] So *Einzinger/Skopik*, Über die datenschutzrechtliche Problematik in CERTs/CSIRTs-Netzwerken, DuD 2017, 572 (574).

6.3. Kritische Infrastruktur (Privatsektor)

Zum Austausch von CTI von Betreibern kritischer Infrastrukturen zu Computer-Notfallteams stehen dem Anschein nach von den Zulässigkeitstatbeständen Art 6 Abs 1 lit a, c, e und f DS-GVO zur Verfügung.

Zunächst soll auf die Möglichkeit der Einholung einer Einwilligung der betroffenen Personen nach lit a eingegangen werden. Gegenstand solch einer Einwilligung könnte die Verarbeitung von Daten durch Betreiber kritischer Infrastrukturen für die Übermittlung an Computer-Notfallteams im Falle von Sicherheitsverletzungen sein. Bei dieser Lösung wäre das jederzeitige Widerrufsrecht der betroffenen Person[267] jedoch impraktikabel. Ferner werden in der Praxis wohl oftmals personenbezogene Daten Teil der CTI sein, die sich nicht auf Kunden oder sonstige Vertragspartner beziehen. Beispielsweise könnte eine IP-Adresse blockiert werden, die einem infizierten Client zuzuordnen ist, dessen Besitzer in keinerlei Beziehung zum angegriffenen Unternehmen steht. Aus diesem Grund ist die Möglichkeit der Einwilligung nur bis zu einem gewissen Grad hilfreich.

Als weitere Grundlage kann das berechtigte Interesse nach lit f in Erwägung gezogen werden. Angesichts der Ausführungen in Kapitel 6.2. könnte jedoch gefolgert werden, dass Betreiber kritischer Infrastrukturen, die keine elektronischen Kommunikationsnetze oder -dienste betreiben, wie z.B. Energieversorger, das Privileg des ErwG 49 mangels Nennung nicht heranziehen können, obwohl gerade die NIS-RL auf solche Betreiber abzielt.[268] Da jedoch gerade BwD und AdD als jene Einrichtungen ausgemacht wurden, deren Cybersicherheit für die Aufrechterhaltung kritischer gesellschaftlicher und wirtschaftlicher Tätigkeiten unerlässlich sowie das Funktionieren des Binnenmarktes von Bedeutung ist, wäre es nicht einsichtig, warum gerade diese Einrichtungen kein berechtigtes Interesse haben sollten, Daten zur Gewährleistung der NIS zu verarbeiten. Ein Grund könnte sein, dass dies als nicht strittig angesehen und daher nicht in ErwG 49 aufgenommen wurde. Hierbei gilt es jedoch zu beachten, dass DS-GVO und NIS-RL zeitgleich verhandelt wurden und ein gegenseitiges Referenzieren aufeinander noch nicht möglich war. Dass die Verarbeitung von Daten zur Gewährleistung der NIS grundsätzlich ein berechtigtes Interesse darstellen kann, hat zudem der EuGH judiziert. Danach kann die Speicherung von IP-Adressen durch den Betreiber einer Website

[267] Art 7 Abs 3 DS-GVO.

[268] Diese Meinung vertretend *Einzinger/Skopik*, Über die datenschutzrechtliche Problematik in CERTs/CSIRTs-Netzwerken, DuD 2017, 572 (574).

zum Zweck, die generelle Funktionsfähigkeit des Dienstes zu gewährleisten, als berechtigtes Interesse zulässig sein, wenn dieses Interesse des Websitebetreibers die Interessen der Betroffenen im Einzelfall überwiegt.[269]

Eine andere Verarbeitungsgrundlage könnte in Art 6 Abs 1 lit c und e erblickt werden. Die DS-GVO schließt im Rechtstext nämlich nicht aus, dass Art 6 Abs 1 lit c und e auch als Grundlage für Verantwortliche dienen kann, die keine Behörden oder andere unter das öffentliche Recht fallende natürliche oder juristische Personen sind. Im Gegenteil ergibt sich aus ErwG 45, dass es sich bei dem Verantwortlichen sehr wohl auch um natürliche oder juristische Personen des Privatrechts handeln kann, sofern dies durch das öffentliche Interesse gerechtfertigt ist. Dementsprechend könnten auf Grundlage von Art 6 Abs 2 und 3 DS-GVO spezifische gesetzliche Regelung vorgesehen werden. In Umsetzung von Art 14 Abs 3 NIS-RL läge mit einer im Cybersicherheitsgesetz vorzusehende Meldepflicht bei Sicherheitsvorfällen[270] an Computer-Notfallteams eine rechtliche Verpflichtung vor, zu deren Erfüllung der BwD Daten verarbeiten muss. Da Pflichtmeldungen (aber auch freiwilligen Meldungen) ein öffentliches Interesse zu Grunde liegt (s. Kapitel 5.5.), wäre die Verarbeitung in Form der Übermittlung an die Computer-Notfallteams durch das öffentliche Interesse gerechtfertigt. Hinsichtlich der freiwilligen Meldung wäre argumentierbar, dass bei BwD und AdD die Gewährleistung ihrer NIS eine Aufgabe ist, die im öffentlichen Interesse liegt, und freiwillige Meldungen (und damit die Verarbeitung von Daten) ein Mittel zur Erfüllung dieser Aufgabe darstellen.

---

[269] Vgl. EuGH 19.10.2016, C-582/14 Rn 64.

[270] Es gilt zu beachten, dass abseits der NIS-RL auch andere Meldepflichten bei Sicherheitsvorfällen bestehen, die in Frage kämen, wie z.B. sektorenspezifische oder datenschutzrechtlich begründete Meldepflichten. Für eine Darstellung s. *Schweighofer/Heussler/Hötzendorfer*, Implementation Issues and Obstacles from a Legal Perspective, in *Skopik* (Hrsg) Collaborative Cyber Threat Intelligene, 320 ff.

7. Conclusio

In der vorliegenden Arbeit wurde aufgezeigt, welche Behörden und Einrichtungen im Zuge der Umsetzung der NIS-RL die wesentlichen Akteure des künftigen nationalen Rechtsrahmens für Cybersicherheit sein werden, wobei die rechtlichen Grundlagen der Akteure kurz dargestellt wurden. Nach einer kurzen Einführung in das Datenschutzrecht wurde untersucht, welche Informationen bei Cybersicherheitsvorfällen typischerweise verarbeitet und ausgetauscht werden, um die Sicherheitsvorfälle zu erkennen, abzuwehren und zu bewältigen. Nach einer Verknüpfung mit dem datenschutzrechtlichen Teil wurde der Schluss gezogen, dass bei der in CTI enthaltenen Information ein Personenbezug nicht zwangsläufig besteht, aber auch nicht ausgeschlossen werden kann. Um einen Austausch von CTI zwischen den Akteuren zu ermöglichen, muss daher eine datenschutzrechtliche Zulässigkeitsprüfung vorgenommen werden. Um diese effizient vornehmen zu können, wurde der durch die NIS-RL vorgegebene Rahmen näher beschrieben und mit dem Wissen, das über die angedachte Umsetzung der NIS-RL bis dato öffentlich vorhanden ist, verbunden. Infolgedessen konnte der CTI-Informationsfluss der Akteure untereinander unter Berücksichtigung der Vorgaben der NIS-RL und der bestehenden Rechtslage geprüft werden.

Gegenstand der Untersuchung der Arbeit war, inwieweit die Akteure für Zwecke der Gewährleistung der Cybersicherheit rechtmäßig Daten verarbeiten und austauschen dürfen. Dabei zeigten sich einige Lücken in der Rechtsordnung, vor allem das GovCERT und das milCERT betreffend. Aufgrund der Befugnisse ist es zwar grundsätzlich möglich, dass insbesondere das CSC und das CDC einander CTI, die personenbezogene Daten enthält, übermitteln. Für eine umfassendere Behandlung im IKDOK fehlt es jedoch an einer Rechtsgrundlage. Die Amtshilfe ist diesbezüglich als nicht geeignet zu bezeichnen. Ferner sehen die bestehenden Rechtsnormen nicht eigens die Gewährleistung von Cybersicherheit als Aufgabe und Verarbeitungszweck vor. Vielmehr ist der Bereich Cybersicherheit über die Abwehr von allgemeiner Gefahr in Form von Cyberangriffen, die einem Cybercrime-Delikt des StGB entsprechen (und für die Anwendung des PStSG gegen kritische Infrastruktur gerichtet sein müssen) bzw. beim BMLV über Cyberangriffen auf Heeresgut oder militärische Geheimnisse, wobei hierbei insbesondere die Aufgaben und Befugnisse der nachrichtendienstlichen Aufklärung und Abwehr in Frage kommen, geregelt.

Im Hinblick auf die Computer-Notfallteams zeigte sich, dass diese schon jetzt aufgrund des berechtigten Interesses eine rechtliche Basis für den Austausch von CTI haben. Diese Basis könnte

durch das Cybersicherheitsgesetz aber gestärkt werden, indem die rechtliche Ungewissheit, die dem berechtigten Interesse argumentativ inhärent ist, durch klare Aufgaben und Befugnisse für Computer-Notfallteams beseitigt wird.

Im Bereich der kritischen Infrastruktur konnte festgestellt werden, dass auch diese durchaus Daten aufgrund eines berechtigten Interesses zur Gewährleistung der Funktionsfähigkeit ihrer Dienste verarbeiten dürfen. Auch hier wird es aber durch die in Umsetzung der NIS-RL einzuführende Meldepflicht bei Cybersicherheitsvorfällen und der Rechtsgrundlage für freiwillige Meldungen in Verbindung mit der Aufgabe von Computer-Notfallteams, BwD und AdD Informationen über Risiken und Vorfälle zukommen zu lassen, in absehbarer Zeit zu einer Stärkung der Rechtssicherheit kommen.

Abschließend bleibt daher nur zu hoffen, dass der nationale Gesetzgeber bei der Umsetzung der NIS-RL den Behörden klar formulierte Aufgaben und Befugnisse für die Sicherstellung der Cybersicherheit auf gesamtstaatlicher Ebene gibt und durch einen rechtlich gut durchdachten Rahmen einen datenschutzrechtlich reibungslosen Austausch von CTI zwischen den Betreibern kritischer Infrastruktur, den relevanten Behörden und den Computer-Notfallteams ermöglicht.

Abbildungsverzeichnis

Quellenverzeichnis

Entscheidungen

EGMR 26.03.1987, 9248/81 (Leander)

EGMR 25.03.1998, 9248/81 (Kopp)

EGMR 16.02.2000, 27798/95 (Amann)

EGMR 04.05.2000, 28341/95 (Rotaru)

EuGH 19.06.2014, C‑345/13 (Karen Millen Fashions)

EuGH 19.10.2016, C-582/14 (Breyer) = jusIT 2016/105, 252 (*Jahnel*) = jusIT 2017/9, 27 (*Kotschy*) = ZIIR 2017, 6 (*Eckhardt*) = MR-Int 2017, 73 (*Keppeler*)

Im Internet bezogenen Quellen (Zugriff am 24. August 2018)

Bundeskanzleramt Österreich, Österreichische Strategie für Cyber Sicherheit, Wien 2013, <http://archiv.bundeskanzleramt.at/DocView.axd?CobId=50748>

Bundeskanzleramt Österreich/*Bundesministerium für Inneres*, Österreichisches Programm zum Schutz kritischer Infrastrukturen (APCIP), Wien 2015, <http://archiv.bundeskanzleramt.at/DocView.axd?CobId=58907>

Bundeskanzleramt Österreich, Arbeitsprogramm der österreichischen Bundesregierung 2013-2018, Wien 2013, <https://www.justiz.gv.at/web2013/file/2c94848642ec5e0d0142fac7f7b9019a.de.0/regprogramm.pdf>

Bundeskanzleramt Österreich, Regierungsprogramm 2017–2022, 32 <https://www.bundeskanzleramt.gv.at/documents/131008/569203/Regierungsprogramm_2017%E2%80%932022.pdf/b2fe3f65-5a04-47b6-913d-2fe512ff4ce6>

BSI/ANSSI, Deutsch-französisches IT-Sicherheitslagebild (2018), <https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/DE-FR-Lagebild/de-fr_Lagebild.pdf?__blob=publicationFile&v=2>

Cyber Sicherheit Steuerungsgruppe, Bericht Cyber Sicherheit 2016, Wien 2016, <http://archiv.bundeskanzleramt.at/DocView.axd?CobId=63191>

Cyber Sicherheit Steuerungsgruppe, Bericht Cyber Sicherheit 2017, Wien 2017, <http://archiv.bundeskanzleramt.at/DocView.axd?CobId=66026>

Kuratorium Sicheres Österreich, KSÖ Rechts- und Technologiedialog Whitepaper. Version 2, Wien 2016, <https://kuratorium-sicheres-oesterreich.at/wp-content/uploads/2016/06/KS%C3%96-RTD-Whitepaper.pdf>

Salimi, Farsam, Neue Rechtsgrundlage für den Staatsschutz (Polizeiliches Staatsschutzgesetz - PStSG) und Neuerungen im SPG, <https://ales.univie.ac.at/fileadmin/user_upload/p_ales/Gesetzesvorhaben/PStSG.pdf>

UK-CERT, An introduction to threat intelligence, <ncsc.gov.uk/content/files/protected_files/guidance_files/An-introduction-to-threat-intelligence.pdf>

Internationale Dokumente und Verträge

Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (Konvention Nr 108)

Internetseiten (Zugriff am 24. August 2018)

Bundeskanzleramt Österreich, Das österreichische Programm zum Schutz kritischer Infrastrukturen (APCIP), <https://www.bundeskanzleramt.gv.at/schutz-kritischer-infrastrukturen>

Bundeskanzleramt Österreich, GovCERT in Österreich, <http://www.govcert.gv.at/home/index/index.html>

Bundesministerium für Digitalisierung und Wirtschaftsstandort/*A-SIT*, Austrian Energy CERT, <https://www.onlinesicherheit.gv.at/erste_hilfe/certs/austrian_energy_cert/249447.html

Bundesministerium für Digitalisierung und Wirtschaftsstandort/*A-SIT*, Computer Emergency Response Teams (CERTs), <https://www.onlinesicherheit.gv.at/erste_hilfe/certs/249343.html>

Bundesministerium für Inneres, Abteilung 3 (Sicherheit und Schutz), <https://www.bvt.gv.at/101/Abteilung_3/cyber_security/info.aspx>

Bundesministerium für Landesverteidigung, milCERT ein wesentlicher Beitrag zur Cyber Defence, <http://www.bundesheer.at/truppendienst/ausgaben/artikel.php?id=1773>

CERT.at, Leitbild, <http://www.cert.at/about/missionstatement/content.html>

CERT.at, Zuständigkeit, <http://www.cert.at/about/scope/scope.html>

Europäische Kommission, The Directive on security of network and information systems (NIS Directive), <ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive>

ICANNwiki, Whois Misuse, <https://icannwiki.org/Whois_Misuse>

National Cybersecurity and Communications Integration Center, Understanding Denial-of-Service Attacks. Security Tip (ST04-015), <https://www.us-cert.gov/ncas/tips/ST04-015>

Kommentare

Wiederin, *Ewald*, in *Korinek*, *Karl*/*Holoubek*, *Michael*/*Bezemek*, *Christoph*/*Fuchs*, *Claudia*/*Martin*, *Andrea*/*Zellenberg*, *Ulrich* (Hrsg) Österreichisches Bundesverfassungsrecht. Kommentar (Verlag Österreich 2011)

Monografien, Fachbeiträge und Qualifizierungsarbeiten

Appl Stephanie, Netz- und Informationssicherheit im Lichte der NIS-Richtlinie (Master-Thesis an der Universität Wien 2017)

Bergauer, Christian, Personenbezogene Daten: Begriff und Kategorien, in *Knyrim, Rainer* (Hrsg) Datenschutz-Grundverordnung: Das neue Datenschutzrecht in Österreich und der EU (Manz 2016)

Brühann, Ulf, Vorbemerkung: Datenschutz und die Europäische Gemeinschaft, in *Grabitz, Eberhard/Hilf, Meinhard* (Hrsg) Das Recht der Europäischen Union[59] (C.H.BECK 2016)

Cormack, Andrew, Incident Response: Protecting Individual Rights Under the General Data Protection Regulation, SCRIPTed 2016, 258

Einzinger, Kurt/Skopik, Florian, Über die datenschutzrechtliche Problematik in CERTs/CSIRTs-Netzwerken, DuD 2017, 572

Einzinger, Kurt/Skopik, Florian, Fiedler/Roman, Keine Cyber-Sicherheit ohne Datenschutz, Datenschutzrechtliche Herausforderungen bei der Etablierung von nationalen CERTs, DuD 2015, 723

Ennöckl, Daniel, Der Schutz der Privatsphäre in der elektronischen Datenverarbeitung (Verlag Österreich 2014)

Feiler, Lukas, Öffnungsklauseln in der Datenschutz-Grundverordnung – Regelungsspielraum des österreichischen Gesetzgebers, jusIT 2016/93, 210

Forgó, Nikolaus/Zöchling-Jud, Brigitta, Das Vertragsrecht des ABGB auf dem Prüfstand: Überlegungen im digitalen Zeitalter (Manz 2018)

Friedberg, Ivo/Wurzenberger, Markus/Balushi, Abdullah Al/Kang, Boojoong, From Monitoring, Logging, and Network Analysis to Threat Intelligence Extraction, in *Skopik, Florian* (Hrsg) Collaborative Cyber Threat Intelligene (CRC Press 2018)

Jahnel, Dietmar, Datenschutzrecht (Jan Sramek 2010)

Krone, Tony/Smith, Russell, Research Report: Criminal misuse of the Domain Name System (Australian Institute of Criminology 2018)

Kunnert, Gerhard, "Was kommt mit der neuen Datenschutz-Grundverordnung auf die Unternehmen zu?", in *Grabenwarter, Christoph/Graf, Ferdinand/Ritschl, Mercedes* (Hrsg), Neuerungen im europäischen Datenschutzrecht für Unternehmen (2017)

Löschnigg, Günther, Datenschutz und Kontrolle im Arbeitsverhältnis, DRdA 2006, 459

Mahler, Christian, Cyberterrorismus: europäische und österreichische Präventions- und Strafbarkeitsmechanismen zur Bekämpfung cyberterroristischer Angriffe gegen kritische Infrastruktureinrichtungen (Dissertation an der Universität Wien 2016)

Öhlinger, Theo/Eberhard, Harald, Verfassungsrecht[10] (Facultas 2014)

Pollirer, Hans-Jürgen/*Weiss, Ernst*/*Knyrim, Rainer*/*Haidinger, Viktoria*, DSGVO – Datenschutz-Grundverordnung (Manz 2017)

Schweighofer, Erich/*Heussler, Vinzenz*/*Kieseberg, Peter*, Privacy by Design Data Exchange between CSIRTs, in *Schweighofer, Erich*/*Leitold, Herbert*/*Mitrakas, Andreas*/*Rannenberg, Kai* (Hrsg) Privacy Technologies and Policy, 5th Annual Privacy Forum, Revised Selected Papers (Springer 2017) 104

Schweighofer, Erich/*Heussler, Vinzenz/Hötzendorfer, Walter*, Implementation Issues and Obstacles from a Legal Perspective, in *Skopik, Florian* (Hrsg) Collaborative Cyber Threat Intelligene (CRC Press 2018)

Stelzer, Manfred, Grundzüge des Öffentlichen Rechts (LexisNexis 2005)

Tschohl, Christoph/*Hötzendorfer, Walter*/*Quirchmayr, Gerald*/*Huber, Edith*/*Hellwig, Otto*, Die NIS-Richtlinie und der rechtliche Rahmen von CERTs, in *Schweighofer, Erich*/*Kummer, Franz*/*Hötzendorfer, Walter*/*Sorge, Christoph* (Hrsg) Trend und Communities der Rechtsinformatik: Tagungsband des 20. Internationalen Rechtsinformatik Symposions IRIS 2017 (OCG 2017) 543

Unger, Walter/Stadlmeier, Sigmar/Troll, Andreas, Cyber Defence – Eine nationale Herausforderung, ÖMZ 2014, 674

Westphal, Dietrich, Grundlagen und Bausteine des europäischen Datenschutzrechts, in *Bauer, Lukas/Reimer, Sebastian* (Hrsg) Handbuch Datenschutzrecht (Facultas 2010)

Nationale Gesetze

Bundesgesetz, mit dem das Datenschutzgesetz 2000 geändert wird (Datenschutz-Anpassungsgesetz 2018), BGBl I 2017/120

Bundesgesetz, mit dem das Datenschutzgesetz geändert wird (Datenschutz-Deregulierungs-Gesetz 2018), BGBl I 2018/24

Bundesgesetz, mit dem das Sicherheitspolizeigesetz geändert wird (SPG-Novelle 2014), BGBl I 2014/43

Bundesgesetz, mit dem das Strafgesetzbuch, das Suchtmittelgesetz, die Strafprozessordnung 1975, das Aktiengesetz, das Gesetz vom 6. März 1906 über Gesellschaften mit beschränkter Haftung, das Gesetz über das Statut der Europäischen Gesellschaft, das Genossenschaftsgesetz, das ORF-Gesetz, das Privatstiftungsgesetz, das Versicherungsaufsichtsgesetz 2016, und das Spaltungsgesetz geändert werden (Strafrechtsänderungsgesetz 2015), BGBl I 2015/112

Bundesgesetz, mit dem bestimmte rechtliche Aspekte des elektronischen Geschäfts- und Rechtsverkehrs geregelt werden (E-Commerce-Gesetz - ECG), BGBl I 2001/152

Bundesgesetz, mit dem ein Telekommunikationsgesetz erlassen wird (Telekommunikationsgesetz 2003 – TKG 2003), BGBl I 2033/70

Bundesgesetz über Aufgaben und Befugnisse im Rahmen der militärischen Landesverteidigung (Militärbefugnisgesetz - MBG), BGBl I 2000/86

Bundesgesetz über den Schutz personenbezogener Daten (Datenschutzgesetz 2000 - DSG 2000), BGB. I 1999/165

Bundesgesetz über die Einrichtung und Organisation des Bundeskriminalamtes (Bundeskriminalamt-Gesetz – BKA-G), BGBl I 2002/22

Bundesgesetz über die Grundsätze der Deregulierung (Deregulierungsgrundsätzegesetz), BGBl I 45/2017

Bundesgesetz über die Organisation der Sicherheitsverwaltung und die Ausübung der Sicherheitspolizei (Sicherheitspolizeigesetz – SPG), BGBl 1991/566 idF BGBl 1992/662

Bundesgesetz vom 23. Jänner 1974 über die mit gerichtlicher Strafe bedrohten Handlungen (Strafgesetzbuch – StGB), BGBl 1974/60

Bundesverfassungsgesetz vom 4. März 1964, mit dem Bestimmungen des Bundes-Verfassungsgesetzes in der Fassung von 1929 über Staatsverträge abgeändert und ergänzt werden, BGBl 1964/59

Strafprozeßordnung 1975 (StPO), BGBl 1975/631

Wehrgesetz 2001 - WG 2001, BGBl I 2001/146

Pressemittelungen

Pressemitteilung Europäische Kommission, 25.01.2012, IP/12/46

Pressemitteilung Europäische Kommission, 19.07.2018, MEMO/18/4486

Unionsrechtsakte

Charta der Grundrechte der Europäischen Union, ABl C 2012/326, 391

Durchführungsverordnung (EU) 2018/151 der Kommission vom 30. Januar 2018 über Vorschriften für die Anwendung der Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates hinsichtlich der weiteren Festlegung der von Anbietern digitaler Dienste beim Risikomanagement in Bezug auf die Sicherheit von Netz- und Informationssystemen zu berücksichtigenden Elemente und der Parameter für die Feststellung erheblicher Auswirkungen eines Sicherheitsvorfalls, ABl L 2018/26, 48

Empfehlung 2003/361/EG der Kommission vom 6. Mai 2003 betreffend die Definition der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen, ABl L 2003/124, 36

Richtlinie 2008/114/EG des Rates vom 8. Dezember 2008 über die Ermittlung und Ausweisung europäischer kritischer Infrastrukturen und die Bewertung der Notwendigkeit, ihren Schutz zu verbessern, ABl L 2008/345, 75

Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union, ABl L 2016/194, 1

Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates, ABl L 2016/119, 89

Richtlinie (EU) 2015/1535 des Europäischen Parlaments und des Rates vom 9. September 2015 über ein Informationsverfahren auf dem Gebiet der technischen Vorschriften und der Vorschriften für die Dienste der Informationsgesellschaft, ABl L 2015/241, 1

Richtlinie 2002/21/EG des Europäischen Parlaments und des Rates vom 7. März 2002 über einen gemeinsamen Rechtsrahmen für elektronische Kommunikationsnetze und -dienste (Rahmenrichtlinie), ABl L 2002/108, 33

Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABl L 1995/281, 31

Verordnung (EU) Nr 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG, ABl L 2014/257, 73

Verordnung (EG) Nr 45/2001 des Europäischen Parlaments und des Rates vom 18. Dezember 2000 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der Gemeinschaft und zum freien Datenverkehr, ABl L 2001/8, 1

Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG, ABl L 2016/119, 1 idF ABl L 2016/314, 72

Vertrag über die Arbeitsweise der Europäischen Union, ABl C 2012/326, 47

Abstract

Die voranschreitende Digitalisierung und die damit verbundene Verlagerung ganzer Lebensbereiche sowie wirtschaftlicher und politischer Prozesse in den Cyberraum ist mit diversen Risiken verbunden. Beispiele für diese Risiken sind im Besonderen die Gefahren, die von Cyberangriffen ausgehen. Da die Sicherheit der Netz- und Informationssysteme, insbesondere der kritischen Infrastruktur, mit den zugehörigen Diensten eine zentrale Rolle für wirtschaftliche und gesellschaftliche Tätigkeiten spielt, wurde mit der Richtlinie (EU) 2016/1148 (NIS-Richtlinie) die erste EU-weite Rechtsetzung zur Cybersicherheit verabschiedet. Ein wichtiger Bestandteil zur Abwehr von Cyberangriffen ist der Austausch von relevanten Informationen über die Angriffe (Cyber Threat Intelligence), bei welchem die Einhaltung datenschutzrechtlicher Vorschriften sicherzustellen ist. Diese Arbeit widmet sich der Frage, ob der österreichische Rechtsrahmen aus datenschutzrechtlicher Sicht geeignete Instrumentarien vorsieht, um vor dem Hintergrund der Umsetzung der NIS-Richtlinie Cybersicherheit gesamtstaatlich sicherstellen zu können.

The advancing digitization and the transfer of whole areas of life as well as of economic and political processes into the cyberspace entail various risks. These risks include the threats emerging from cyber-attacks. Since the security of network and information systems, in particular of the critical infrastructure, with their associated services play a key role in economic and social activities, the Directive (EU) 2016/1148 (NIS Directive) was passed as the first piece of EU-wide legislation on cybersecurity. An essential way to protect against cyber-attacks is the exchange of relevant information about the attacks (Cyber Threat Intelligence). Exchanging such information must comply with data protection law. This paper deals with the question of whether the Austrian legal framework provides, from a data protection point of view, apt instruments to ensure cybersecurity at the national level in the light of the implementation of the NIS Directive.