Schriften zum Öffentlichen Recht

Band 1388

Die Gewährleistung der IT-Sicherheit Kritischer Infrastrukturen

Am Beispiel der Pflichten des IT-Sicherheitsgesetzes und der RL (EU) 2016/1148

Von

Christoph Freimuth

Duncker & Humblot · Berlin

CHRISTOPH FREIMUTH

Die Gewährleistung der IT-Sicherheit Kritischer Infrastrukturen

Schriften zum Öffentlichen Recht

Band 1388

Die Gewährleistung der IT-Sicherheit Kritischer Infrastrukturen

Am Beispiel der Pflichten des IT-Sicherheitsgesetzes und der RL (EU) 2016/1148

Von

Christoph Freimuth

Duncker & Humblot · Berlin

Gedruckt mit Unterstützung
des Förderungsfonds Wissenschaft der VG WORT

Die Rechts- und Wirtschaftswissenschaftliche Fakultät
der Universität Bayreuth hat diese Arbeit im Jahr 2018
als Dissertation angenommen.

Bibliografische Information der Deutschen Nationalbibliothek

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in
der Deutschen Nationalbibliografie; detaillierte bibliografische Daten
sind im Internet über http://dnb.d-nb.de abrufbar.

Fremddatenübernahme: L101 Mediengestaltung, Fürstenwalde
Druck: CPI buchbücher.de gmbh, Birkach
Printed in Germany

ISSN 0582-0200
ISBN 978-3-428-15563-7 (Print)
ISBN 978-3-428-55563-5 (E-Book)
ISBN 978-3-428-85563-6 (Print & E-Book)

Gedruckt auf alterungsbeständigem (säurefreiem) Papier
entsprechend ISO 9706 ♾

Internet: http://www.duncker-humblot.de

Vorwort

Die Arbeit wurde im Wintersemester 2017/2018 von der Rechts- und Wirtschaftswissenschaftlichen Fakultät der Universität Bayreuth als Dissertation angenommen.

Herzlich danken möchte ich zuallererst meinem Doktorvater Herrn Prof. Dr. Markus Möstl. Er förderte die Arbeit wohlwollend und gab mir während meiner Tätigkeit an dessen Lehrstuhl als wissenschaftlicher Mitarbeiter stets genügend Freiraum. Er hatte immer ein offenes Ohr und unterstützte mich mit wertvollen Anregungen und Hinweisen. Dank gebührt auch Prof. Dr. Heinrich Amadeus Wolff für die Mühen der Zweitkorrektur und die hilfreichen Anregungen aus dem von ihm veranstalteten Doktorandenkolloquium.

Besonders bedanken möchte ich mich zudem bei meiner Frau Hanna. Sie hat mir nicht nur den Rücken freigehalten und so den zügigen Abschluss des Promotionsvorhabens gefördert, sondern auch die Bürde des Korrekturlesens übernommen. Ebenso bedanke ich mich bei meinen Eltern Jutta und Peter. Sie haben meine Ausbildung ermöglicht, mich vielfältig unterstützt und damit den Grundstein gelegt. Für das Korrekturlesen bedanke ich mich auch bei meinem Schwiegervater Harald.

Für die Unterstützung meines Studiums und meines Promotionsvorhabens mit Stipendien schulde ich der Hanns-Seidel-Stiftung e. V. großen Dank.

Gewidmet ist diese Arbeit meiner Familie.

Bayreuth, im Juni 2018 *Christoph Freimuth*

Inhaltsübersicht

Teil 4

Inhaltsverzeichnis

Abkürzungsverzeichnis

a. A.	andere Ansicht
ABl.	Amtsblatt der Europäischen Union
Abs.	Absatz
a. E.	am Ende
AEG	Allgemeines Eisenbahngesetz
AEUV	Vertrag über die Arbeitsweise der Europäischen Union
a. F.	alte Fassung
Anm.	Anmerkung
AöR	Archiv des öffentlichen Rechts
APuZ	Aus Politik und Zeitgeschichte
Art.	Artikel
Artt.	Artikel (Plural)
AtG	Gesetz über die friedliche Verwendung der Kernenergie und den Schutz gegen ihre Gefahren (Atomgesetz)
Aufl.	Auflage
BaFin	Bundesanstalt für Finanzdienstleistungsaufsicht
BayLStVG	Gesetz über das Landesstrafrecht und das Verordnungsrecht auf dem Gebiet der öffentlichen Sicherheit und Ordnung (Landesstraf- und Verordnungsgesetz) (Bayern)
BayObLG	Bayerisches Oberstes Landesgericht
BayPAG	Gesetz über die Aufgaben und Befugnisse der Bayerischen Staatlichen Polizei (Polizeiaufgabengesetz)
BayVBl.	Bayerische Verwaltungsblätter
BayVGH	Bayerischer Verwaltungsgerichtshof
BB	Betriebs-Berater
BCM	Business Continuity Management
BDSG	Bundesdatenschutzgesetz
BGB	Bürgerliches Gesetzbuch
BGBl.	Bundesgesetzblatt
BGH	Bundesgerichtshof
BGHZ	Entscheidungen des Bundesgerichtshofes in Zivilsachen
BImSchG	Gesetz zum Schutz vor schädlichen Umwelteinwirkungen durch Luftverunreinigungen, Geräusche, Erschütterungen und ähnliche Vorgänge (Bundes-Immissionsschutzgesetz)

bitkom	Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V.
BlnDSG	Gesetz zum Schutz personenbezogener Daten in der Berliner Verwaltung (Berliner Datenschutzgesetz)
BSI	Bundesamt für Sicherheit in der Informationstechnik
BSIG	Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz)
BV	Verfassung des Freistaates Bayern
BVerfG	Bundesverfassungsgericht
BVerwG	Bundesverwaltungsgericht
BWPolG	Polizeigesetz (Baden-Württemberg)
BW VGH	Verwaltungsgerichtshof Baden-Württemberg
bzgl.	bezüglich
bzw.	beziehungsweise
CERT	Computer Emergency Response Team
CR	Computer und Recht
DÖV	Die Öffentliche Verwaltung
DSG-LSA	Gesetz zum Schutz personenbezogener Daten der Bürger (Datenschutzgesetz Sachsen-Anhalt)
DSG M-V	Gesetz zum Schutz des Bürgers bei der Verarbeitung seiner Daten (Landesdatenschutzgesetz) (Mecklenburg-Vorpommern)
DSG NW	Datenschutzgesetz Nordrhein-Westfalen
DuD	Datenschutz und Datensicherheit
Ed.	Edition
EGV	Vertrag zur Gründung der Europäischen Gemeinschaft
EL	Ergänzungslieferung
ENISA	Europäische Agentur für Netz- und Informationssicherheit
EnWG	Gesetz über die Elektrizitäts- und Gasversorgung (Energiewirtschaftsgesetz)
EnWZ	Zeitschrift für das gesamte Recht der Energiewirtschaft
Erw.-Gr.	Erwägungsgrund, Erwägungsgründe
etc.	et cetera
EU	Europäische Union
EUGRCH	Charta der Grundrechte der Europäischen Union
EuR	Zeitschrift Europarecht
EUV	Vertrag über die Europäische Union
f.	folgende
ff.	fortfolgende
Fn.	Fußnote

gem.	gemäß
GenTG	Gesetz zur Regelung der Gentechnik (Gentechnikgesetz)
GG	Grundgesetz
GRUR	Gewerblicher Rechtsschutz und Urheberrecht
GVBl.	Gesetz- und Verordnungsblatt
HmbDSG	Hamburgisches Datenschutzgesetz
Hs.	Halbsatz
i. e. S.	im engeren Sinn(e)
ISMS	Informations-Sicherheits-Management-System
i. S. v./d./e.	im Sinne von/des/einer
IT	Informationstechnik
IT-	informationstechnische (r, s)
ITRB	Der IT-Rechts-Berater
IT-System	informationstechnisches System (einfachrechtlicher Begriff)
i. V. m.	in Verbindung mit
JR	Juristische Rundschau
jurisPR-ITR	juris PraxisReport IT-Recht
JuS	Juristische Schulung
JZ	JuristenZeitung
K&R	Kommunikation & Recht
lit.	littera/Buchstabe
Ls.	Leitsatz
LuftVG	Luftverkehrsgesetz
Mio.	Million(en)
MMR	MultiMedia und Recht
m. w. N.	mit weiteren Nachweisen
NATO	North Atlantic Treaty Organization
n. F.	neue Fassung
NJW	Neue Juristische Wochenschrift
N&R	Netzwirtschaften und Recht
NStZ	Neue Zeitschrift für Strafrecht
NVwZ	Neue Zeitschrift für Verwaltungsrecht
NVwZ-RR	NVwZ-Rechtsprechungs-Report Verwaltungsrecht
NWPolG	Polizeigesetz des Landes Nordrhein-Westfalen
OVG	Oberverwaltungsgericht
PTSG	Gesetz zur Sicherstellung von Postdienstleistungen und Telekommunikationsdiensten in besonderen Fällen (Post- und Telekommunikationssicherstellungsgesetz)

Rdnr.	Randnummer(n)
RDV	Recht der Datenverarbeitung
RL	Richtlinie
ROG	Raumordnungsgesetz
Rs.	Rechtssache
S.	Seite(n); Satz
SächsDSG	Sächsisches Datenschutzgesetz
Slg.	Sammlung der Rechtsprechung des Gerichtshofes und des Gerichts Erster Instanz
StGB	Strafgesetzbuch
ThürDSG	Thüringer Datenschutzgesetz
TKG	Telekommunikationsgesetz
TMG	Telemediengesetz
UAbs.	Unterabsatz
VerwArch	Verwaltungsarchiv
vgl.	vergleiche
Vorb.	Vorbemerkung(en)
VVDStRL	Veröffentlichungen der Vereinigung der Deutschen Staatsrechtslehrer
VwGO	Verwaltungsgerichtsordnung
VwVfG	Verwaltungsverfahrensgesetz
Wistra	Zeitschrift für Wirtschafts- und Steuerstrafrecht
WiVerw	Wirtschaft und Verwaltung
ZD	Zeitschrift für Datenschutz
ZG	Zeitschrift für Gesetzgebung
ZLR	Zeitschrift für das gesamte Lebensmittelrecht
ZRP	Zeitschrift für Rechtspolitik
ZSKG	Gesetz über den Zivilschutz und die Katastrophenhilfe des Bundes (Zivilschutz- und Katastrophenhilfegesetz)
ZUM	Zeitschrift für Urheber- und Medienrecht

Einführung

A. Bestrebungen der normativen Gewährleistung der IT-Sicherheit

Die IT-Sicherheit zu gewährleisten, ist eine der großen Herausforderungen unserer Gesellschaft. Ohne eine sichere IT[1] geraten die Grundstrukturen unserer Informationsgesellschaft ins Wanken, da weitreichende Abhängigkeiten von der IT bestehen.[2] Dies verdeutlicht das allgemein auf Sicherheit bezogene folgende Zitat:

„Sicherheitsvorsorge ist häufig Grundvoraussetzung dafür, dass wirtschaftliches Handeln stattfinden kann, und ist damit Garant für künftiges wirtschaftliches Wachstum und Prosperität". (Norbert Walter)[3]

In Zeiten der Informationsgesellschaft trifft dies besonders auf die IT-Sicherheit als Grundvoraussetzung zu.

Dass die Gewährleistung der IT-Sicherheit nicht immer gelingt, zeigt eine Vielzahl von IT-Sicherheitsvorfällen. Besonders deutlich wird dies, wenn sie Auswirkungen auf die Dienstleistungserbringung zeitigen. Letzteres ist aber nicht zwingend. Zum Teil bleiben IT-Sicherheitsvorfälle selbst dem Betroffenen unbekannt. Doch allein die Zahl an IT-Sicherheitsvorfällen mit Auswirkungen auf die Dienstleistungserbringung, von denen auch die Kunden betroffen sind, kann inzwischen nicht mehr überblickt werden. Obwohl IT-Sicherheitsvorfälle vor allem wegen der Auswirkungen auf die Dienstleistungen in den Medien präsent sind, ist diese mediale Aufmerksamkeit häufig nur von kurzer Dauer. Oftmals wird sie durch neue IT-Sicherheitsvorfälle überholt.

Eine Auswahl aktueller IT-Sicherheitsvorfälle zeigt die Bandbreite der Betroffenen. Dies sind nicht nur bestimmte Branchen, sondern die gesamte

---

1 Informationstechnik.

2 BT-Drs. 18/4096, S. 1; BT-Drs. 13/11002, S. 31; vgl. *Sonntag,* IT-Sicherheit kritischer Infrastrukturen, S. 54; *Spannowsky,* in: Spannowsky/Runkel/Goppel, Raumordnungsgesetz (ROG), § 2, Rdnr. 89; *Höhne/Pöhls,* Grund und Grenzen staatlicher Schutzpflichten für die IT-Infrastruktur, in: Taeger, Digitale Evolution, S. 827, 830.

3 Zitiert nach *Schäuble,* Schutz kritischer Infrastrukturen als Aufgabe der Politik, in: Kloepfer, Schutz kritischer Infrastrukturen, S. 21, 24.

Wirtschaft, aber auch staatliche Einrichtungen sowie Private. Bei der Fluglinie British Airways kam es im Mai 2017 wegen einer Computerpanne über zwei Tage lang zu erheblichen Flugausfällen. Am Londoner Flughafen Heathrow mussten an einem Tag sämtliche Flüge gestrichen werden.[4]

Wenige Tage zuvor waren IT-Systeme weltweit von der Erpressungssoftware „Wanna Cry" betroffen. Ziel der Software ist, Daten zu verschlüsseln und nur gegen Lösegeld wieder freizugeben. Die Verbreitung dieser Software betraf wichtige Einrichtungen in Wirtschaft und Staat. In Deutschland waren Anzeigetafeln und Fahrkartenautomaten der Deutschen Bahn, in Großbritannien mehrere Krankenhäuser, in den USA das Logistikunternehmen FedEx, in Spanien und Portugal Telekommunikationsunternehmen sowie in Russland das Innenministerium betroffen. Nur durch Zufall konnte eine noch weitere Verbreitung gestoppt werden.[5]

Allein die Bundeswehr war im Jahr 2016 von 47 Mio. IT-Angriffen betroffen. Davon konnten neun Mio. nicht mehr durch herkömmliche Virenschutzprogramme oder eine Firewall abgewehrt werden und waren in die Gefahrengruppe „hoch" einzustufen. Nennenswerte Schäden sind jedoch nicht entstanden.[6] Auch der Deutsche Bundestag ist immer wieder Ziel von Angriffen auf die IT-Sicherheit. Aufgrund eines Angriffes auf das IT-System des Bundestages kam es im Frühjahr 2015 zu einem Datenabfluss. Das IT-System selbst bedurfte in Teilen einer Neuaufsetzung.[7] Auch für das Jahr 2017 werden Cyber-Angriffe auf den Bundestag erwartet.[8] Allein bei Bundesbehörden

---

4 http://www.sueddeutsche.de/wirtschaft/british-airways-computerpanne-1.3524219 (besucht am 12.06.2018); http://www.sueddeutsche.de/wirtschaft/panne-flugverkehr-normalisiert-sich-nach-ausfall-1.3526301 (besucht am 12.06.2018).

5 http://www.spiegel.de/netzwelt/netzpolitik/cyberattacke-weltweit-bundeskriminalamt-ermittelt-zu-hacker-angriff-a-1147520.html (besucht am 12.06.2018); https://www.heise.de/tp/features/Weltweiter-Erpressungstrojaner-Angriff-auf-Computernetzwerke-3713480.html (besucht am 12.06.2018); http://www.zeit.de/digital/internet/2017-05/cyberangriff-grossbritannien-krankenhaeuser-hacker (besucht am 12.06.2018).

6 https://www.heise.de/newsticker/meldung/Ueber-47-Millionen-IT-Angriffe-auf-die-Bundeswehr-im-Jahr-2016-3595632.html (besucht am 12.06.2018).

7 Deutscher Bundestag, Bundestagspräsident Lammert informiert Abgeordnete über Angriff auf das Datennetz des Parlaments, https://www.bundestag.de/presse/pressemitteilungen/2015/pm_15061112/378140 (besucht am 12.10.2017); BT-Drs. 18/10759, S. 4; https://netzpolitik.org/2016/wir-veroeffentlichen-dokumente-zum-bundestagshack-wie-man-die-abgeordneten-im-unklaren-liess/ (besucht am 12.06.2018); https://www.heise.de/newsticker/meldung/Bundestags-Hack-Angriff-mit-gaengigen-Methoden-und-Open-Source-Tools-3129862.html (besucht am 12.06.2018); zu weiteren Angriffen im August 2016 auf den Bundestag und Parteien http://www.sueddeutsche.de/politik/bundesregierung-ist-alarmiert-hackerangriff-aufdeutsche-parteien-1.3170347 (besucht am 12.06.2018).

8 BT-Drs. 18/10759, S. 3 f.

wurden im Jahr 2016 pro Monat durchschnittlich 44.000 mit Schadprogrammen infizierte E-Mails abgefangen.[9]

Selbst Forschungsinstitute wie die Bayreuther Fraunhofer-Projektgruppe Prozessinnovation sind vor Angriffen auf ihre IT nicht bewahrt. Im Februar 2016 wurden sämtliche Daten des Instituts durch das Programm „*.locky" verschlüsselt, was einen erheblichen Schaden zur Folge hatte, der nur durch vorhandene Backups der verschlüsselten Daten in Grenzen gehalten werden konnte.[10]

Angriffe auf die IT bilden keine theoretischen Gedankenspiele,[11] sondern sind Realität. Obwohl sie erhebliche wirtschaftliche Schäden verursachen können, werden die sich stellenden Probleme nicht selten unterschätzt. Nach einer Pressemitteilung des Branchenverbandes bitkom sind nur 49 % der Unternehmen auf IT-Notfälle vorbereitet.[12]

Dass aus IT-Sicherheitsvorfällen erhebliche wirtschaftliche Schäden entstehen können, zeigen auch die aufgeführten Beispiele. Die British Airways verliert Schätzungen zufolge an einem Tag ohne Flugbewegungen 30 Mio. britische Pfund Umsatz und vier Mio. britische Pfund Betriebsgewinn. Dabei wurden zu zahlende Entschädigungen noch nicht mit eingerechnet.[13] Schäden folgen nicht nur aus den Auswirkungen auf die Erbringung von Dienstleistungen, sondern auch aus der Wiederherstellung der IT-Sicherheit der jeweiligen IT-Systeme. Hierdurch können Kosten in erheblicher Höhe entstehen.

Dies verdeutlicht, dass die Integration von IT in die Prozesse von Wirtschaft und Verwaltung sowie in den privaten Alltag nicht nur positive Folgen zeitigt, sondern auch neuartige, sich verwirklichende Schadenspotentiale in sich birgt.

Als Akteur versucht der Staat daher einen Ordnungsrahmen für die IT-Sicherheit zu setzen. Dieser ist nicht aus einem Guss, sondern besteht aus vielen Bausteinen. Mit jedem Einzelnen wird versucht, auf dem Weg zur Gewährleistung der IT-Sicherheit ein Stück voranzugehen. Dem Staat stehen dabei vielfältigste Instrumente zur Verfügung. Zentrale Aufgabe des Staates ist es, für die Gewährleistung der IT-Sicherheit einen ausreichenden und ge-

---

9 *BSI,* Die Lage der IT-Sicherheit in Deutschland 2016, S. 33 f.

10 *Lapp*, Trojaner legt Fraunhofer lahm, Nordbayerischer Kurier, http://www.nordbayerischer-kurier.de/nachrichten/trojaner-legt-fraunhofer-institut-lahm_448847 (besucht am 12.06.2018).

11 *Hutter,* APuZ B 41-42 2000, S. 31 ff.

12 bitkom, Jedes zweite Unternehmen nicht auf IT-Notfälle vorbereitet, https://www.bitkom.org/Presse/Presseinformation/Jedes-zweite-Unternehmen-nicht-auf-IT-Notfaelle-vorbereitet.html (besucht am 12.06.2018).

13 http://www.sueddeutsche.de/wirtschaft/panne-flugverkehr-normalisiert-sich-nach-ausfall-1.3526301 (besucht am 12.06.2018).