CENTER FOR INFORMATION TECHNOLOGY SOCIETY AND LAW — ITSL

Volume 9

Rolf H. Weber/Okan Yildiz

Cybersicherheit und Cyber-Resilienz in den Finanzmärkten

EIZ Publishing

CENTER FOR INFORMATION TECHNOLOGY SOCIETY AND LAW — ITSL

Schriften aus dem ITSL, herausgegeben von Florent Thouvenin und Rolf H. Weber

Volume 9

Rolf H. Weber/Okan Yildiz

Cybersicherheit und Cyber-Resilienz in den Finanzmärkten

EIZ Publishing

Verlag: EIZ Publishing (eizpublishing.ch)
Herausgeber: Center for Information Technology Society and Law ITSL, Florent Thouvenin (Hrsg.)
Produktion & Vertrieb: buch & netz (buchundnetz.com)
ISBN:
978-3-03805-473-3 (Print – Softcover)
978-3-03805-474-0 (PDF)
978-3-03805-475-7 (ePub)
DOI: https://doi.org/10.36862/eiz-473
Version: 1.01 – 20220404

Dieses Werk ist als gedrucktes Buch sowie als E-Book (open access) in verschiedenen Formaten verfügbar. Weitere Informationen finden Sie unter der URL: https://eizpublishing.ch/publikationen/cybersicherheit-und-cyber-resilienz-in-den-finanzmaerkten/.

Vorwort

Cybersicherheit und Cyber-Resilienz sind in den letzten Jahren, die sich durch eine immer stärkere Digitalisierung der ganzen Umwelt auszeichnen, zu einer zentralen Herausforderung für Unternehmen (und Privatpersonen) geworden, insbesondere im Finanzmarktbereich. Kaum ein Tag vergeht ohne eine Meldung, dass die IT-Infrastruktur eines Unternehmens angegriffen worden sei. Die Gefährdungslage und das steigende Risiko veranlassen deshalb auch die gesetzgebenden Organe, regulatorische Aktivitäten zu entwickeln. In der Schweiz und rund um den Globus spiessen neue Vorschriften und Standards aus dem Boden, die insbesondere präventiv dazu beitragen sollen, potenzielle Angriffe auf die Sicherheit und Resilienz von IT-Infrastrukturen abzufangen oder zumindest abzumildern.

Eine vertiefende Analyse des gegenwärtigen Regulierungsrahmens für Cybersicherheit und Cyber-Resilienz in der Finanzmarktbranche ist derzeit nicht verfügbar. Das vorliegende Buch soll diese Lücke schliessen. Bewusst wird nach einleitenden allgemeinen Überlegungen eine detaillierte rechtsvergleichende Auslegeordnung vorgenommen, die über Europa hinausreicht und wichtige Staaten mit fortgeschrittener Digitalisierung der Geschäftswelt miteinschliesst (insbesondere Ostasien). Gestützt auf diese Erkenntnisse steht die Ausarbeitung von Handlungsempfehlungen für Finanzunternehmen im Vordergrund der Ausführungen; konkret geht es also um die Frage, welche Vorkehren und Massnahmen die Unternehmen zur Gewährleistung von Cybersicherheit und Cyber-Resilienz treffen sollten.

Die ganze Thematik von Cybersicherheit und Cyber-Resilienz ist stark im Fluss, genauso wie die technologische Seite (mit den Stichworten Digitalisierung und Blockchain). Allgemeingültige Handlungsempfehlungen lassen sich deshalb kaum formulieren; vielmehr muss es um situationsbedingte Anregungen gehen. Die Ausführungen betreffen den Stand im Februar 2022; die Angaben auf weiterführende Dokumente sind verlinkt. Hinweise nehmen die Autoren, die hiermit auch der SIX Exchange Regulation AG für den Finanzierungsbeitrag zur Erstellung dieser Studie danken, gerne entgegen.

Zürich, Februar 2022 Rolf H. Weber Okan Yildiz

Inhaltsverzeichnis

Literaturverzeichnis

Alle Internet-Dokumente sind letztmals am 21. Februar 2022 besucht worden.

A

Aebi, 2020. Christian Aebi, Vermögenssicherung im Strafverfahren. Grundlagen, Tatverdacht, Praxis, Zürich/Basel/Genf 2020

Albrecht, 2021. Daniel Albrecht, New Developments in Chinese Data Protection Law in Contrast to the European GDPR, CRi 5/2021, 142–147

Albrecht, 2022. Daniel Albrecht, Chinese first Personal Information Protection Law in contrast to the European GDPR, CRi 1/2022, 1–5

Almansi, 2018. Aquiles A. Almansi, Financial Sector's Cybersecurity: Regulations and Supervision, World Bank Group, Washington D.C. 2018

Ang, 2021. Benjamin Ang, Cybersecurity and Legislation: The Case Study of Singapore. In: Gabi Simon/Libor Ezioni (Eds.), Cybersecurity and Legal-Regulatory Aspects, Singapore 2021, 89–102

Anttila/Jussila, 2017. Juhani Anttila/Kari Jussila, ISO 9001:2015 – a questionable reform. What should the implementing organisations understand and do?, Total Qual. Manag. Bus. Excell. 2017, 1090–1105

B

Bartlett, 2019. Benjamin Bartlett, How Japanese Cybersecurity Policy Changes, Harvard Program on U.S.-Japan Relations, Occasional Paper Series, 2019-01, Harvard, Cambridge MA 2019

Bendiek/Pander Maat, 2021. Annegret Bendiek/Eva Pander Maat, EU's Cybersecurity Policy. In: Gabi Siboni/Limor Ezioni (Eds.), Cybersecurity and Legal-Regulatory Aspects, Singapore 2021, 23–64

Bendiek/Porter, 2013. Annegret Bendiek/Andrew L. Porter, European Cyber Security Policy within a Global Multistakeholder Structure, Eur. Foreign Aff. Rev. 2013, 155–180

Beranek Zanon, 2014. Nicole Beranek Zanon, Big Data und Datensicherheit. In: Rolf H. Weber/Florent Thouvenin (Hrsg.), Big Data und Datenschutz – Gegenseitige Herausforderungen, Zürich 2014, 85-115

BK OR-Bearbeiter/in, 2020. Rolf H. Weber/Susan Emmenegger, Art. 97-109. Allgemeine Bestimmungen. Die Folgen der Nichterfüllung. Band VI: Obligationenrecht. 1. Abteilung: Allgemeine Bestimmungen. 5. Teilband: Die Folgen der Nichterfüllung Art. 97-109 OR, Berner Kommentar, Kommentar zum schweizerischen Privatrecht, 2. Aufl. Bern 2020

Blair/Lloyd/Sussman/Nonninger, 2021. Keily Blair/James Lloyd/Heather Egan Sussman/Lara Nonninger, United Kingdom. In: The Legal 500 Country Comparative Guides, Data Protection & Cyber Security, 3rd ed. London 2021

Bouveret, 2018. Antoine Bouveret, Cyber Risk for the Financial Sector: A Framework for Quantitative Assessment, IMF Working Paper, WP/18/143, Washington D.C. 2018

BSK FinfraG-Bearbeiter/in, 2019. Rolf Watter/Rashid Bahar (Hrsg.), Basler Kommentar, Finanzmarktaufsichtsgesetz, Finanzmarktinfrastrukturgesetz, 3. Aufl. Basel 2019

BSK OR I-Bearbeiter/in, 2020. Corinne Widmer Lüchinger/David Oser (Hrsg.), Obligationenrecht I, Basler Kommentar, Art. 1-529 OR, 7. Aufl. Basel 2020

BSK OR II-Bearbeiter/in, 2016. Heinrich Honsell/Nedim Peter Vogt/Rolf Watter (Hrsg.), Obligationenrecht II, Basler Kommentar, Art. 530-964 OR inkl. Schlussbestimmungen, 5. Aufl. Basel 2016

BSK StGB II-Bearbeiter/in, 2019. Marcel Alexander Niggli/Hans Wiprächtiger (Hrsg.), Strafrecht II, Art. 137-392 StGB, Jugendstrafgesetz, 4. Aufl. Basel 2019

Burnett, 2021. Emma Burnett, CMS Expert Guide: Data Law Navigator, Data protection and cybersecurity laws in the United Kingdom, March 2021, aufrufbar unter <https://cms.law/en/int/expert-guides/cms-expert-guide-to-data-protection-and-cyber-security-laws/united-kingdom>

C

Calliess/Baumgarten, 2020. Christian Calliess/Ansgar Baumgarten, Cybersecurity in the EU, The Example of the Financial Sector: A Legal Perspective, GLJ 2020, 1149–1179

Camillo, 2017. Mark Camillo, Cybersecurity: Risks and management of risks for global banks and financial institutions, J. Risk Manag. Financ. Inst. 2017, 196–200

Carter/Crumpler, 2019. William A. Carter/William D. Crumpler, Financial Sector Cybersecurity Requirements in the Asia-Pacific Region, A Report of the CSIS Technology Policy Program, Washington D.C. 2019

Chen, 2021. Jihong Chen, China. In: The Legal 500 Country Comparative Guides, Data Protection & Cyber Security, 3rd ed. London 2021

Crompton/Northcott/Buttoo, 2021. Jonathan Crompton/Stephanie Northcott/Sakshi Buttoo, Hong Kong. In: The Legal 500 Country Comparative Guides, Data Protection & Cyber Security, 3rd ed. London 2021

D

Didenko, 2020. Anton N. Didenko, Cybersecurity Regulation in Singapore's Financial Sector: Protecting FinTech 'Ants' in a Jungle Full of 'Elephants', University of New South Wales Law Research Series 45, Sydney 2020

Dierstein, 2004. Rüdiger Dierstein, Sicherheit in der Informationstechnik – der Begriff IT-Sicherheit, Informatik Spektrum 2004, 343–353

Drescher, 2017. Daniel Drescher, Blockchain Grundlagen, Frechen 2017

E

Eggen, 2015. Mirjam Eggen, Produktregulierung im Finanzmarktrecht, Bern 2015

F

Fellmann, 2008. Walter Fellmann, Der einfache Auftrag und die aktuelle Entwicklung im Recht der freien Berufe, recht 2008, 119–133

Fellmann, 2016. Walter Fellmann, Objektivierung der Sorgfaltspflichten im Auftragsrecht, HAVE 2016, 95–101

Füzesséry/Schneider, 2020. Simone Füzesséry/Danielle Schneider, La révision de la loi fédérale sur la protection des données. In: Astrid Epiney/Sophia Rovelli (Hrsg.), Datenschutzgrundverordnung (DSGVO): Tragweite und erste Erfahrungen/Le Règlement général sur la protection des données (RPDG): portée et premières expériences, Zürich 2020, 139–158

G

Gauch, 2019. Peter Gauch, Der Werkvertrag, 6. Aufl. Zürich 2019

Gauch/Schluep/Emmenegger, 2020. Peter Gauch/Walter R. Schluep/Susan Emmenegger, OR AT. Schweizerisches Obligationenrecht Allgemeiner Teil, Bd. II, 11. Aufl. Zürich 2020

Glatz, 2018. Florian Glatz, Blockchain. In: Stephan Breidenbach/Florian Glatz (Hrsg.), Rechtshandbuch Legal Tech, München 2018, 59–90

Guzman/Meyer, 2010. Andrew T. Guzman/Timothy L. Meyer, International soft law, J. Leg. Anal. 2010, 171–225

H

Hadlington, 2018. Lee Hadlington, The «Human Factor» in Cybersecurity: Exploring the Accidental Insider. In: John McAlaney/Lara A. Frumkin/Vladlena Benson (Eds.), Psychological and Behavioral Examinations in Cyber Security, Hershey 2018, 46–63

Hayashi/Yukawa/Tsuta, 2020. Hiromi Hayashi/Masaki Yukawa/Daisuke Tsuta, Japan. In: International Comparative Legal Guides, Cybersecurity 2021, A practical cross-border insight into cybersecurity law, 4th ed. London 2020

Hayes/Drury, 2020. Julian Hayes/Michael Drury, Cybersecurity in United Kingdom (England & Wales), Lexology, February 2020, aufrufbar unter <https://www.lexology.com/library/detail.aspx?g=09262dc8-609b-45b1-bba9-8291f6d9c112>

Henriksen, 2019. Anders Henriksen, The end of the road for the UN GGE process: The future regulation of cyberspace, J. Cybersecur. 2019, 1–9

I

Ishiara, 2020. Tomoki Ishiara, Japan. In: Alan Charles Raul (Ed.), The Privacy, Data Protection and Cybersecurity Law Review, 7th ed. London 2020, 263–282

Isler/Kunz/Müller/Schneider/Vasella, 2019. Michael Isler/Oliver M. Kunz/Thomas Müller/Jürg Schneider/David Vasella, Bekanntgabe von Bankkundendaten an Beauftragte im In- und im Ausland. Zur Zulässigkeit der Auslagerung nach Art. 47 BankG – Gutachten erstattet an die Schweizerische Bankiervereinigung am 14. Februar 2019, Jusletter vom 27. Mai 2019

Iwase/Shibata/Terada, 2018. Hitomi Iwase/Hiroko Shibata/Mitsukuni Terada, Data security and breach notification in Japan, Lexology, October 2018, aufrufbar unter <https://www.lexology.com/library/detail.aspx?g=dcfead6c-c9ef-4b59-8be9-8fd19992674l>

J

Jacob/Loh, 2021. Sheena Jacob/Denise Loh, CMS Expert Guide: Data Law Navigator, Data protection and cybersecurity laws in Singapore, February 2021, aufrufbar unter <https://cms.law/en/int/expert-guides/cms-expert-guide-to-data-protection-and-cyber-security-laws/singapore>

K

Kaur/Lashkari/Lashkari, 2021. Gurdip Kaur/Ziba Habibi Lashkari/Arash Habibi Lashkari, Understanding Cybersecurity Management in FinTech, Challenges, Strategies, and Trends, Cham 2021

Kay/Hutcherson/Keene/Zhang/Terwilliger, 2021. Amy Kay/Christian Hutcherson/Calen Keene/Xihui Zhang/Mark G. Terwilliger, How financial institutions address cybersecurity threats: A critical analysis, IIS 2021, 63–74

Kin/Alfred/Pichlmaier, 2020. Lim Chong Kin/David N. Alfred/Albert Pichlmaier, Singapore. In: International Comparative Legal Guides, Cybersecurity 2021, A practical cross-border insight into cybersecurity law, 4th ed. London 2020

Komm. NBG-Bearbeiter/in, 2021. Martin Plenio/Myriam Senn (Hrsg.), Nationalbankgesetz – Bundesgesetz über die Währung und die Zahlungsmittel, Kommentar, Zürich 2021

Komm. StromVG-Bearbeiter/in, 2016. Brigitta Kratz/Michael Merker/Renato Tami/Stefan Rechsteiner/Kathrin S. Föhse (Hrsg.), Kommentar zum Energierecht, Band I: WRG / EleG / StromVG / RLG, Bern 2016

Kosseff, 2018. Jeff Kosseff, Defining Cybersecurity Law, Iowa Law Rev. 2018, 985–1031

Krüger/Brauchle, 2021. Philipp S. Krüger/Jan-Philipp Brauchle, The European Union, Cybersecurity, and the Financial Sector: A Primer, Cyber Policy Initiative Working Paper Series, "Cybersecurity and the Financial System" #9, Washington, D.C. 2021

Kulesza/Weber, 2021. Joanna Kulesza/Rolf H. Weber, Protecting the Internet with International Law, CLSR 2021, 105531, 1–12

L

Laux/Hofmann/Schieweck/Hess, 2019. Christian Laux/Alexander Hofmann/Mark Schieweck/Jürg Hess, Nutzung von Cloud-Angeboten durch Banken. Zur Zulässigkeit nach Art. 47 BankG – Gutachten erstattet an die Schweizerische Bankiervereinigung am 14. Februar 2019, Jusletter vom 27. Mai 2019

Lewis, 2018. James Lewis, Economic Impact of Cybercrime – No Slowing Down, Washington D.C. 2018

Long/Blythe, 2020. William Long/Francesca Blythe, United Kingdom. In: Alan Charles Raul (Ed.), The Privacy, Data Protection and Cybersecurity Law Review, 7th ed. London 2020, 426–453

Long/Scali, 2019. William Long/Geraldine Scali, UK. In: Chambers Global Practice Guides, Data Protection & Cyber Security 2019, 2nd ed. London 2019

Long/Shankar, 2021. William Long/Vishnu Shankar, UK. In: Alan Charles Raul (Ed.), Chambers Global Practice Guides, Cybersecurity 2021, London 2021

M

Marble et al., 2015. Julie L. Marble/William F. Lawless/Ranjeev Mittu/Joseph Coyne/Myriam Abramson/Ciara Sibley, The Human Factor in Cybersecurity: Robust & Intelligent Defense. In: Sushil Jajodia/Paulo Shakarian/V.S. Subrahmanian/Vipin Swarup/Cliff Wang (Eds.), Cyber Warfare, Building the Scientific Foundation, Basel 2015, 173–206

Mathys/Hösli, 2019. Roland Mathys/Andreas Hösli, Cyberattacken – Meldung bei den Behörden?, Computerworld 2019, 54

Mathys/Zollinger-Löw, 2019. Roland Mathys/Floriane Zollinger-Löw, Cyberrisiken im Fadenkreuz rechtlicher Anforderungen, Recht relevant 2019, 2

Matsuda/Adachi/Kukimoto, 2021. Akira Matsuda/Makoto Adachi/Sayaka Kukimoto, Japan. In: The Legal 500 Country Comparative Guides, Data Protection & Cyber Security, 3rd ed. London 2021

Maull/Godsiff/Mulligan/Brown/Kewell, 2017. Roger Maull/Phil Godsiff/Catherine Mulligan/Alan Brown/Beth Kewell, Distributed ledger technology: Applications and implications, SC 2017, 481–489

McNicholas/Angle, 2020. Ed McNicholas/Kevin Angle, USA. In: International Comparative Legal Guides, Cybersecurity 2021, A practical cross-border insight into cybersecurity law, 4th ed. London 2020

McNicholas/Angle/Faircloth, 2021. Ed McNicholas/Kevin Angle/Fran Faircloth, USA. In: Alan Charles Raul (Ed.), Chambers Global Practice Guides, Cybersecurity 2021, London 2021

Meier/Schuppli, 2019. Julia Meier/Benedikt Schuppli, The DAO Hack and the Living Law of Blockchain. In: Alexandra Dal Molin-Kränzlin/Anne Mirjam Schneuwly/Jasna Stojanovic (Hrsg.), Digitalisierung – Gesellschaft – Recht, Analysen und Perspektiven von Assistierenden des Rechtswissenschaftlichen Instituts der Universität Zürich, Zürich/St. Gallen 2019, 27–43

Meyer, 2017. Paul Meyer, Norms of Responsible State Behaviour in Cyberspace. In: Markus Christen/Bert Gordijn/Michele Loi (Hrsg.), The Ethics of Cybersecurity, Cham 2017, 347–360

Moser, 1998. Martin Moser, Die Haftung für Dienstleistungen im Lichte eines zertifizierten Qualitätsmanagementsystems, AJP 1997, 181–195

N

Nagel, 2020. Sebastian Nagel, Stabilität und Resilienz des Finanzmarkts. In: Stefanie Hiss/Agnes Fessler/Gesa Griese/Sebastian Nagel/Daniela Woschnack (Hrsg.), Nachhaltigkeit und Finanzmarkt, Zur soziologischen Vermessung eines Reflexionsraums, Wiesbaden 2020, 143–161

Narayanan/Chandhoke, 2021. Anoop Narayanan/Rashi Chandhoke, India. In: The Legal 500 Country Comparative Guides, Data Protection & Cyber Security, 3rd ed. London 2021

Narayanan/Gupta, 2021. Anoop Narayanan/Priyanka Gupta, India. In: Alan Charles Raul (Ed.), Chambers Global Practice Guides, Cybersecurity 2021, London 2021

Ning/Wu, 2020. Susan Ning/Han Wu, China. In: International Comparative Legal Guides, Cybersecurity 2021, A practical cross-border insight into cybersecurity law, 4th ed. London 2020

Ning/Wu/Jiang, 2021. Susan Ning/Han Wu/Ke Jiang, China. In: Alan Charles Raul (Ed.), Chambers Global Practice Guides, Cybersecurity 2021, London 2021

O

Onodera/Tanaka/Shimamura, 2019. Yoshifumi Onodera/Hiroyuki Tanaka/Naoto Shimamura, Japan. In: Chambers Global Practice Guides, Data Protection & Cyber Security 2019, 2nd ed. London 2019

P

Parker/Charnock, 2020. Nigel Parker/Nathan Charnock, England & Wales. In: International Comparative Legal Guides, Cybersecurity 2021, A practical cross-border insight into cybersecurity law, 4th ed. London 2020

Probst, 2013. Thomas Probst, Die unbestimmte «Bestimmbarkeit» der von Daten betroffenen Personen im Datenschutzrecht, AJP 2013, 1423–1436

Pupillo/Griffith/Blockmans/Renda, 2018. Lorenzo Pupillo/Melissa K. Griffith/Steven Blockmans/Andrea Renda, Strengthening the EU's Cyber Defence Capabilities, Report of a CEPS Task Force, Centre for European Policy Studies, Brussels 2018

Q

Qi/Li, 2021. George Qi/Qianqian Li, China Finalizes Data Security Law, Greenberg Traurig, GT Alerts, July 2021, aufrufbar unter <https://www.gtlaw.com/en/insights/2021/7/china-finalizes-data-security-law>

R

Raul/Tapia, 2020. Alan Charles Raul/Snezhana Stadnik Tapia, United States. In: Alan Charles Raul (Ed.), The Privacy, Data Protection and Cybersecurity Law Review, 7th ed. London 2020, 454–482

Rosenthal, 2017. David Rosenthal, Der Entwurf für ein neues Datenschutzgesetz, Was uns erwartet und was noch zu korrigieren ist, Jusletter vom 27. November 2017

Rosenthal, 2020a. David Rosenthal, Mit Berufsgeheimnissen in die Cloud: So geht es trotz US CLOUD Act, Jusletter vom 10. August 2020

Rosenthal, 2020b. David Rosenthal, Das neue Datenschutzgesetz, Jusletter vom 16. November 2020

Ruggie, 2004. John Gerard Ruggie, Reconstituting the Global Public Domain – Issues, Actors and Practices, EJIR 2004, 499–531

Ryga, 1995. Barbara M. Ryga, Cyberporn: Contemplating the First Amendment in Cyberspace, Seton Hall Const. Law J. 1995, 221–253

S

Schulthess Komm. BankG-Bearbeiter/in, 2015. Dieter Zobl/Renate Schwob/Rolf H. Weber/Christoph Winzeler/Christine Kaufmann/Stefan Kramer (Hrsg.), Kommentar zum Bundesgesetz über die Banken und Sparkassen vom 8. November 1934 sowie zu der Verordnung vom 17. Mai 1972 (V) und der Vollziehungsverordnung vom 30. August 1961 (VV) – mit Hinweisen auf das Bankenrecht der Europäischen Union, auf das Allgemeine Dienstleistungsabkommen (GATS) und mit Erläuterungen zu den Massnahmen gegen die Geldwäscherei, 23. Lieferung, Zürich 2015

Schwarzenegger, 2008. Christian Schwarzenegger, Die Internationalisierung des Wirtschaftsstrafrechts und die schweizerische Kriminalpolitik: Cyberkriminalität und das neue Urheberstrafrecht, ZSR 2008 II, 399–503

Sethe, 2020. Rolf Sethe, Konsumentenschutz beim Vermögensaufbau. In: Helmut Heiss/Leander D. Loacker (Hrsg.), Grundfragen des Konsumentenrechts, Zürich/Basel/Genf 2020, 231–293

Shackelford/Raymond/Balakrishnan/Dixit/Gjonaj/Kavi, 2016. Scott Shackelford/Anjanette Raymond/Rakshana Balakrishnan/Prakhar Dixit/Julianna Gjonaj/Rachith Kavi, When Toasters Attack: A Polycentric Approach to Enhancing the Security of Things, Kelley School of Business Research Paper No. 16-6, 2016, 1–54

Soesanto, 2020. Stefan Soesanto, Japan's National Cybersecurity and Defense Posture Policy and Organizations, Cyberdefense Report, Cyber Defense Project (CDP), Center for Security Studies (CSS), ETH Zürich, Zürich 2020

Stevens, 2021. Jeremy Stevens – Regelungsvielfalt im IT-Sicherheitsrecht, Anforderungen an die IT-Sicherheit von Smart Metern, CR 2021, 841–848

Sussman/Tabatabai/Downey/Boyle, 2021. Heather Egan Sussman/Emily S. Tabatabai/Tori Downey/Kathryn Boyle, United States. In: The Legal 500 Country Comparative Guides, Data Protection & Cyber Security, 3rd ed. London 2021

T

Thakur/Khan Pathan, 2020. Kutub Thakur/Al-Sakib Khan Pathan, Cybersecurity Fundamentals, A Real-World Perspective, Abingdon 2020

Tham, 2020. Yuet Ming Tham, Hong Kong. In: Alan Charles Raul (Ed.), The Privacy, Data Protection and Cybersecurity Law Review, 7th ed. London 2020, 206–223

Thouvenin/Weber/Früh, 2019. Florent Thouvenin/Rolf H. Weber/Alfred Früh, Elemente einer Datenpolitik, Zürich 2019

Tikk, 2017. Eneken Tikk, Introduction. In: United Nations Office for Disarmement Affairs (Ed.), Voluntary, Non-Binding Norms for Responsible State Behaviour in the Use of Informations and Communications Technology, A Commentary, New York 2017, 1–8

U

V

W

Walker et al., 2006. Brian H. Walker/Lance H. Gunderson/Ann P. Kinzig/Carl Folke/Steve R. Carpenter/Lisen Schultz, A Handful of Heuristics and Some Propositions for Understanding Resilience in Social-Ecological Systems, Ecol. Soc. 2006, Art. 13 (online), 1–15

Warsinkse et al., 2019. John Warsinkse et al., CISSP: Certified Information Systems Security Professional, The Official (ISC)2®, CISSP® CBK®, Reference, 5th ed. Hoboken 2019

Weber, 1990. Rolf H. Weber, Praxis zum Auftragsrecht und zu den besonderen Auftragsarten, Bern 1990

Weber, 2006. Rolf H. Weber, Risikomanagement und Systemschutz bei Finanzinfrastrukturen. In: Rolf H. Weber/Dieter Zobl (Hrsg.), Risikomanagement durch Recht im Banken- und Versicherungsbereich, Zürich/Basel/Genf 2006, 107–136

Weber, 2009. Rolf H. Weber, Shaping Internet Governance: Regulatory Challenges, Zürich 2009

Weber, 2012. Rolf H. Weber, Overcoming the Hard Law/Soft Law Dichotomy in Times of (Financial) Crises, J. Gov. Regul. 2012, 8–14

Weber, 2014. Rolf H. Weber, Realizing a New Global Cyberspace Framework, Normative Foundations and Guiding Principles, Zürich 2014

Weber, 2017a, Rolf H. Weber, IT-Governance: unverzichtbar für jedes Unternehmen. In: Schulthess Manager Handbuch 2017, Zürich/Basel/Genf 2017, 37–42

Weber, 2017b. Rolf H. Weber, Liability in the Internet of Things, EuCML 2017, 207–212

Weber, 2020. Rolf H. Weber, Cybersecurity in International Law. In: Asian Academy of International Law (Ed.), 2019 Colloquium on International Law, Synergy and Security: The Keys to Sustainable Global Investment, Hong Kong 2020, 279–308

Weber, 2021a. Rolf H. Weber, Internet Governance at the Point of No Return, Zürich 2021

Weber, 2021b. Rolf H. Weber, Cybergovernance revisited, Regulierungserwartungen für die Zukunft, Jusletter IT vom 30. September 2021

Weber, 2021c. Rolf H. Weber, Duty of Co-Operation as New Cybergovernance Concept, Jusletter IT vom 25. Februar 2021

Weber, 2021d. Rolf H. Weber, Handel mit digitalen Aktiven. In: Rolf H. Weber/Hans Kuhn (Hrsg.), Entwicklungen im Schweizer Blockchain-Recht, Basel 2021, 165–197

Weber, 2021e. Rolf H. Weber, Sectoral Self-Regulation as Viable Tool. In: Klaus Mathis/Avishalom Tor (Hrsg.), Law and Economics of Regulation, Cham 2021, 25–36

Weber, 2021f. Rolf H. Weber, Cybersecurity Governance – international law as policy driver?, Jusletter IT vom 27. Mai 2021

Weber, 2021g. Rolf H. Weber, Integrity in the 'Infinite Space' – New Frontiers for International Law, ZaöRV 2021, 601–626

Weber, 2021h. Rolf H. Weber, Haftungsfragen beim Handel von digitalen Vermögenswerten, SJZ 2021, 679–687

Weber/Grosz, 2009. Rolf H. Weber/Mirina Grosz, Internet Governance – From Vague Ideas to Realistic Implementation, Medialex 2007, 119–135

Weber/Henseler, 2020. Rolf H. Weber/Simon Henseler, Daten-Governance und Cloud Banking im neuen Datenschutzrechtsumfeld, SZW 2020, 604–617

Weber/Studer, 2016. Rolf H. Weber/Evelyne Studer, Cybersecurity in the Internet of Things: Legal aspects, CLSR 2016, 715–728

Weber/Willi, 2006. Rolf H. Weber/Annette Willi, IT-Sicherheit und Recht, Grundlagen eines integrativen Gestaltungskonzepts, Zürich 2006

Webley/Hardy, 2015. Tom Webley/Peter Hardy, What Can Be Done to Mitigate Cyber Risk?, JIBFL 2015, 353–357

Wittmann/Haidenthaler, 2022. Jörn Wittmann/Gregor Haidenthaler, IT-Compliance in der Cloud – Rechtssicherheit durch Codes of Conduct?, MMR 2022, 8–18

Wright/Dunphy-Moriel, 2021. Emma Wright/Marta Dunphy-Moriel, UK. In: Antony Kim (Ed.), Mondaq Cybersecurity Comparative Guide, 2nd ed. Bristol/Essex/New York/Sydney 2021

X

Y

Z

Zhu, 2021. Ju Lindsay Zhu, China Passes New Data Privacy and Security Laws, Nat. Law Rev. 2021, Volume XI/235, 1–2

Zulauf et al., 2014. Urs Zulauf/David Wyss/Kathrin Tanner/Michel Kähr/Claudia M. Fritsche/Patric Eymann/Fritz Amman, Finanzmarktenforcement. Verfahren zur Durchsetzung des Schweizer Finanzmarktrechts, 2. Aufl. Bern 2014

Materialienverzeichnis

Alle Internet-Dokumente sind letztmals am 21. Februar 2022 besucht worden.

ACSC, 2021. Australian Cyber Security Center, Australian Government, Information Security Manual, Canberra 2021

BABS, 2016. Bundesamt für Bevölkerungsschutz, Nationale Cyber-Risiko Strategie NCS / Schutz kritischer Infrastrukturen SKI, Factsheet zum kritischen Teilsektor Finanzdienstleistungen, Bern 2016

Bank of England, 2021. Bank of England, Operational resilience of the financial sector, London 2021, aufrufbar unter <https://www.bankofengland.co.uk/financial-stability/operational-resilience-of-the-financial-sector>

BFE, 2021. Bundesamt für Energie, Cyber-Sicherheit und Cyber Resilienz für die Schweizer Stromversorgung, Bern 2021

BIS/IOSCO, 2012. Bank for International Settlements und International Organization of Securities Commissions, Principles for financial market infrastructures, 2012, aufrufbar unter <https://www.bis.org/cpmi/publ/d101a.pdf>

BIS/IOSCO, 2016. Bank for International Settlements und International Organization of Securities Commissions, Guidance on cyber resilience for financial market infrastructures, 2016, aufrufbar unter <https://www.bis.org/cpmi/publ/d146.pdf>

Bissell/Lasalle/Dal Cin, 2019. Kelly Bissell/Ryan M. Lasalle/Paolo Dal Cin, The Cost of Cybercrime, Ninth Annual Cost Of Cybercrime Study, Unlocking The Value Of Improved Cybersecurity Protection, North Traverse City 2019, aufrufbar unter <https://www.accenture.com/_acnmedia/PDF-96/Accenture-2019-Cost-of-Cybercrime-Study-Final.pdf#zoom%3d50>

Botschaft DSG, BBl 2017. Bundesrat, Botschaft zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz, BBl 2017, 6941–7192

Botschaft nationale Strategie, BBl 2018. Bundesrat, Botschaft vom 8. Dezember 2017 zur nationalen Strategie zum Schutz kritischer Infrastrukturen 2018–2022, BBl 2018, 503–540

Bundesrat, 2019. Varianten für Meldepflichten von kritischen Infrastrukturen bei schwerwiegenden Sicherheitsvorfällen, Bericht des Bundesrates vom 13. Dezember 2019 in Erfüllung des Postulates 17.3475 Graf-Litscher vom 15.06.17, Bern 2019

Bundesrat, 2022. Vernehmlassung 2021/70, Meldepflicht von Betreiberinnen kritischer Infrastrukturen für Cyberangriffe, Bern 2022

BWL, 2018. Bundesamt für wirtschaftliche Landesversorgung BWL, Minimalstandard zur Verbesserung der IKT-Resilienz, Bern 2018

CBIRC, 2009. China Banking and Insurance Regulatory Commission, 中国银行业监督管理委员会关于印发《商业银行信息科技风险管理指引》的通知 vom 3. März 2009 (englisch: Notice of China Banking Regulatory Commission on Issuing the Guidelines on the Information Technology Risk Management of Commercial Banks, CLI.4.115172, No. 19 [2009] of the CBRC), Beijing 2009; englische Übersetzung aufrufbar unter <http://www.lawinfochina.com/display.aspx?lib=law&id=7372&CGid=>

Cœuré, 2018. Benoît Cœuré, Europäische Zentralbank, The new frontier of payments and market infrastructure: on cryptos, cyber and CCPs, Welcome remarks by Benoît Cœuré, Chair of the Committee on Payments and Market Infrastructures of the Bank for International Settlements and Member of the Executive Board of the ECB, at the Economics of Payments IX Conference, Basel, 15 November 2018, aufrufbar unter <https://www.ecb.europa.eu/press/key/date/2018/html/ecb.sp181115.en.html>

CREST, 2014. CREST, An introduction to CBEST, Slough 2014, aufrufbar unter <https://www.crest-approved.org/wp-content/uploads/2014/05/CBEST-OVERVIEW.pdf>

CREST, 2019. CREST, What is Cyber Threat Intelligence and how is it used?, Slough 2019, aufrufbar unter <https://www.crest-approved.org/wp-content/uploads/CREST-Cyber-Threat-Intelligence.pdf>

Delfas, 2017. Nausicaa Delfas, Expect the unexpected – cyber security – 2017 and beyond, Speech by Nausicaa Delfas vom 24. April 2017

DND/NATO/*PfPC*, 2016. Sean S. Costigan/Michael A. Hennessy (Eds.), Cybersecurity, A generic reference curriculum, Ontario/Norfolk 2016

DV, 2021. Direktion für Völkerrecht (DV), Schweizer Positionspapier: Die Anwendung des Völkerrechts im Cyberraum, Annex UN GGE Cybersicherheit 2019/2021, Bern 2021

EBA, 2019. Europäische Bankenaufsichtsbehörde, EBA-Leitlinien für das Management von IKT- und Sicherheitsrisiken, EBA/GL/2019/04, Paris 2019

EDÖB, 2015. Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter EDÖB, Leitfaden zu den technischen und organisatorischen Massnahmen des Datenschutzes, Bern 2015

EDÖB, 2021. Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB), Das neue Datenschutzgesetz aus Sicht des EDÖB, Bern 2021

EFD, 2020. Eidgenössisches Finanzdepartement, Meldepflicht für schwerwiegende Sicherheitsvorfälle bei kritischen Infrastrukturen, Rechtliche Grundlagen, Bern 2020

EFD, 2022. Eidgenössisches Finanzdepartement, Einführung einer Meldepflicht für Cyberangriffe auf kritische Infrastrukturen, Änderung des Bundesgesetzes über die Informationssicherheit beim Bund (Informationssicherheitsgesetz, ISG) vom 18. Dezember 2020, Erläuternder Bericht zur Eröffnung des Vernehmlassungsverfahrens, Bern 2022

EFK, 2020. Eidgenössische Finanzkontrolle, Prüfung der Aufsicht über die Cybersicherheit bei Finanzdienstleistern, Bern 2020

EFK, 2021. Eidgenössische Finanzkontrolle, Jahresbericht 2020, Bern 2021

EIOPA, 2021. Europäische Aufsichtsbehörde für das Versicherungswesen und die betriebliche Altersversorgung, Leitlinien zu Sicherheit und Governance im Bereich der Informations- und Kommunikationstechnologie, EIOPA-BoS-20/600, Frankfurt am Main 2021

EJPD, 2021. Eidgenössisches Justiz- und Polizeidepartement, Totalrevision der Verordnung zum Bundesgesetz über den Datenschutz, Erläuternder Bericht zur Eröffnung des Vernehmlassungsverfahrens, 23. Juni 2021, Bern 2021

EY, 2021. Ernst & Young, EY Bankenbarometer 2021, Resilienz, Zürich 2021

EZB, 2018a. Europäische Zentralbank (EZB), Cyber resilience oversight expectations for financial market infrastructures, Frankfurt am Main 2018

EZB, 2018b. Europäische Zentralbank (EZB), European Framework for Threat-Intelligence Based Ethical Red Teaming, Frankfurt am Main 2018

EZB, 2020. Europäische Zentralbank (EZB), Cyber Information and Intelligence Sharing Initiative (CIISI-EU), Cyber information and intelligence sharing: a practical example, Euro Cyber Resilience Board Secretariat, Frankfurt am Main 2020

FCA, 2018. Financial Conduct Authority, Cyber and Technology Resilience: Themes from cross-sector survey 2017/2018, London 2018, aufrufbar unter <https://www.fca.org.uk/publication/research/technology-cyber-resilience-questionnaire-cross-sector-report.pdf>

FCA, 2019. Financial Conduct Authority, Cyber security – industry insights, London 2019, aufrufbar unter <https://www.fca.org.uk/publication/research/cyber-security-industry-insights.pdf>

FINMA, Aufsichtsmitteilung 05/2020. Eidgenössische Finanzmarktaufsicht FINMA, FINMA-Aufsichtsmitteilung 05/2020, Meldepflicht von Cyber-Attacken gemäss Art. 29 Abs. 2 FINMAG, Bern 2020

FINMA, Jahresbericht 2020. Eidgenössische Finanzmarktaufsicht FINMA, Jahresbericht 2020, Bern 2020

FINMA, Risikomonitor 2021. Eidgenössische Finanzmarktaufsicht FINMA, FINMA-Risikomonitor 2021, Bern 2021

FINMA, Rundschreiben 2008/21. Eidgenössische Finanzmarktaufsicht FINMA, Rundschreiben 2008/21 Operationelle Risiken – Banken, Eigenmittelanforderungen und qualitative Anforderungen für operationelle Risiken bei Banken, Bern 2008

FINMA, Rundschreiben 2017/1. Eidgenössische Finanzmarktaufsicht FINMA, Rundschreiben 2017/1 Corporate Governance – Banken, Bern 2017

FINMA, Rundschreiben 2018/3. Eidgenössische Finanzmarktaufsicht FINMA, Rundschreiben 2018/3 Outsourcing – Auslagerungen Banken, Versicherungsunternehmen und ausgewählten Finanzinstituten nach FINIG, Bern 2018

FINMA/SNB, 2017. Memorandum of Understanding im Bereich Finanzstabilität zwischen der Eidgenössischen Finanzmarktaufsicht FINMA und der Schweizerischen Nationalbank SNB, Bern 2017

FMA, Richtlinie 2021/3. Finanzmarktaufsicht Liechtenstein FMA, FMA-Richtlinie 2021/3 – Richtlinie IKT-Sicherheit, Richtlinie betreffend die Überwachung von Informations- und Kommunikationstechnologie (IKT)-Risiken, Vaduz 2021

FSB, 2020. Financial Stability Board (FSB), Effective Practices for Cyber Incident Response and Recovery, Consultative Document, Basel 2020

G-20, 2017. G-20 Germany, Communiqué, G20 Finance Ministers and Central Bank Governors Meeting Baden-Baden, Germany, 17–18 March 2017, abrufbar unter <http://www.g20.utoronto.ca/2017/170318-finance-en.pdf>

G7 Cyber Expert Group, 2016. G7 Cyber Expert Group, Fundamental Elements of Cybersecurity for the Financial Sector, 2016, aufrufbar unter <https://ec.europa.eu/info/sites/default/files/cybersecurity-fundamental-elements-11102016_en.pdf>

HKMA, 2003. Hong Kong Monetary Authority, Supervisory Policy Manual, General Principles for Technology Risk Management, TM-G-1, Hong Kong 2003, aufrufbar unter <https://www.hkma.gov.hk/media/eng/doc/key-functions/banking-stability/supervisory-policy-manual/TM-G-1.pdf>

HKMA, 2014. Hong Kong Monetary Authority, Customer Data Protection of 14 October 2014, Hong Kong 2014, aufrufbar unter <https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2014/20141014e1.pdf>

HKMA, 2015. Hong Kong Monetary Authority, Cyber Security Risk Management of 15 September 2015, Hong Kong 2015, aufrufbar unter <https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2015/20150915e1.pdf>

HKMA, 2016. Hong Kong Monetary Authority, Cybersecurity Fortification Initiative of 21 December 2016, Hong Kong 2016, aufrufbar unter <https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2016/20161221e1.pdf>

HKMA, 2018. Hong Kong Monetary Authority, Implementation of Cyber Resilience Assessment Framework of 12 June 2018, Hong Kong 2018, aufrufbar unter <https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2018/20180612e1.pdf>

HKMA, 2020. Hong Kong Monetary Authority, Cybersecurity Fortification Initiative 2.0 of 3 November 2020, Hong Kong 2020, aufrufbar unter <https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2020/20201103e1.pdf>

IRDAI, 2017. Insurance Regulatory and Development Authority of India (IRDAI), Guidelines on Information and Cyber Security for Insurers of 7 April 2017, Circular No. IRDA/IT/GDL/MISC/082/04/2017, Hyderabad 2017, aufrufbar unter <https://www.aicofindia.com/AICEng/General_Documents/Notices%20And%20Tenders/IRDAI-GUIDELINES.pdf>

JCSH, 2017. Cybersecurity Strategic Headquarters, Government of Japan, Cybersecurity Policy for Critical Infrastructure Protection (4th ed.) of 18 April 2017, Tokyo 2017, aufrufbar unter <https://www.nisc.go.jp/eng/pdf/cs_policy_cip_eng_v4.pdf>

JFSA, 2014. Japanese Financial Services Agency, 主要行等監督上の評価項目 of 2 July 2014 (englisch: Evaluation items for supervision of major banks, etc.), Tokyo 2014, aufrufbar unter <https://www.fsa.go.jp/common/law/guide/gaigin.pdf>

JFSA, 2018. Japanese Financial Services Agency, Comprehensive Guidelines for Supervision of Financial Market Infrastructures – Clearing Organizations, Fund Clearing Organizations, Book-entry Transfer Institutions, and Trade Repositories, Tokyo 2018, aufrufbar unter <https://www.fsa.go.jp/common/law/201802.pdf>

JMETI/JIPA, 2017. Ministry of Economy, Trade and Industry/Information-technology Promotion Agency, Japan, Cybersecurity Management Guidelines, Ver. 2.0, Tokyo 2017, aufrufbar unter <https://www.meti.go.jp/policy/netsecurity/downloadfiles/ CSM_Guideline_v2.0_en.pdf>

JNISC, 2016. National Center of Incident Readiness and Strategy for Cybersecurity of Japan, General Framework for Secure IoT Systems of 26 August 2016, Tokyo 2016, aufrufbar unter <https://www.nisc.go.jp/eng/pdf/iot_framework2016_eng.pdf>

JPPC, 2016. Personal Information Protection Commission, 個人情報の保護に関する法律についてのガイドライン (通則編) of 30 November 2016 (englisch: Guidelines for the Law Concerning the Protection of Personal Information [General Rules]), Tokyo 2016, aufrufbar unter <https://www.ppc.go.jp/personalinfo/legal/2009_guidelines_tsusoku/>

JPPC, 2017. Personal Information Protection Commission, 個人データの漏えい等の事案が発生した場合等の対応について (englisch: About measures in case of leakage of personal data, etc.), Tokyo 2017, aufrufbar unter <https://www.ppc.go.jp/files/pdf/iinkaikokuzi01.pdf>

JPPC/JFSA, 2017. Personal Information Protection Commission/Japanese Financial Services Agency, 金融分野における個人情報保護に関するガイドライン of February 2017 (englisch: Guidelines for the Protection of Personal Information in the Financial Sector), Tokyo 2017, aufrufbar unter <https://www.fsa.go.jp/common/law/kj-hogo-2/01.pdf>

Juniper Research, 2019. Juniper Research, Business Losses to Cybercrime Data Breaches to Exceed $5 trillion by 2024, Cybersecurity Breaches to Increase Nearly 70% Over the Next 5 years, Hampshire 2019

MAS, 2015. Monetary Authority of Singapore (MAS), Comprehensive Risk Assessment Framework and Techniques, Impact Assessment, CRAFT Risk Assessment, April 2007 (revised in September 2015), Singapore 2015

MAS, 2021. Monetary Authority of Singapore (MAS), Technology Risk Management Guidelines, Singapore 2021

McAfee Labs, 2016. McAfee Labs, 2016 Threat Predictions, Report, Santa Clara 2016

MeitY, 2014. Ministry of Electronics and Information Technology, Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013 (CERT-In Rules) of 16 January 2014, New Delhi 2014, aufrufbar unter <https://www.cert-in.org.in/PDF/G.S.R_20(E).pdf>

MIIT, 2021. Ministry of Industry and Information Technology, 关于开展工业互联网企业网络安全分类分级管理试点工作的通知 of 13 January 2021 (englisch: Notice on Launching the Pilot Multi-Level Protection Scheme for Cybersecurity of Industrial Internet Enterprises 2021), Beijing 2021, aufrufbar unter <https://www.miit.gov.cn/jgsj/waj/gzdt/art/2021/art_eb95e60794794fc29f768233e7d7739d.html%20>

MPS, 2018. Ministry of Public Security, 网络安全等级保护 测评机构管理办法 of 17 April 2018 (englisch: Administrative Measures on Cybersecurity Classification Evaluating Institutions 2018), Beijing 2018, aufrufbar unter <http://www.djbh.net/webdev/web/HomeWebAction.do?p=getGzjb&id=8a8182565fd8b6b90162d2415180022e>

MPS, 2020. Ministry of Public Security, 贯彻落实网络安全等级保护制度和关键信 息基础设施安全保护制度的指导意见 of 22 July 2020 (englisch: Guiding Opinions on Implementing the Multi-Level Protection System for Cybersecurity and the Security Protection System for Critical Information Infrastructure 2020), Beijing 2020, aufrufbar unter <https://www.mps.gov.cn/n6557558/c7369310/content.html%20>

NCIIPC, 2015. National Critical Information Infrastructure Protection Centre, Guidelines for Protection of Critical Information Infrastructure of 16 January 2015, New Delhi 2015, aufrufbar unter <https://www.asianlaws.org/gcld/cyberlawdb/IN/guidelines/NCIIPC_Guidelines_V2.pdf>

NCSC, 2018. Nationales Zentrum für Cybersicherheit, Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS) 2018–2022, Bern 2018

NIST, 2018. National Institute of Standards and Technology, Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1, aufrufbar unter <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf>

Norton Rose Fulbright, 2021. Norton Rose Fulbright, Cybersecurity: Not just an IT issue, but a regulatory one too, London 2021, aufrufbar unter <https://www.nortonrosefulbright.com/en/knowledge/publications/b8178be8/cybersecurity-not-just-an-it-issue-but-a-regulatory-one-too>

PCPD, 2021. Privacy Commissioner for Personal Data, Personal Information Protection Law of the Mainland, Highlights of the Mainland's Personal Information Protection Law, Hong Kong 2021, aufrufbar unter <https://www.pcpd.org.hk/english/data_privacy_law/mainland_law/ mainland_law.html>

PRA, 2017. Prudential Regulation Authority, Supervisory Statement | SS21/15 Internal governance, April 2017, London 2017, aufrufbar unter <https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/supervisory-statement/2017/ss2115update.pdf?la=en&hash=DDA2A6148C17D00A86858D1F5B5922989ED69043>

PRA, 2020. Prudential Regulation Authority, CBEST Threat Intelligence-Led Assessments, January 2021, London 2020, aufrufbar unter <https://www.bankofengland.co.uk/financial-stability/operational-resilience-of-the-financial-sector/cbest-threat-intelligence-led-assessments-implementation-guide>

Protiviti, 2018. Protiviti, China's Cybersecurity Law and Its Impacts Key requirements businesses need to understand to ensure compliance, Hong Kong 2018

PwC Schweiz, 2019. Prüfung einer Meldepflicht bei Sicherheitsvorfällen, Studie von PwC Schweiz im Auftrag des Informatiksteuerungsorgans des Bundes (ISB) vom Oktober 2019 (PwC-Studie)

RBI, 2016. Reserve Bank of India, Cyber Security Framework in Banks of 2 June 2016, Mumbai 2016, aufrufbar unter <https://rbidocs.rbi.org.in/rdocs/notification/PDFs/NT41893F697BC1D57443BB76AFC7AB56272EB.PDF>

ReBIT, 2017. Reserve Bank Information Technology Private Limited, Cybersecurity Maturity Model, Implementation Guide of 28 October 2017, Mumbai 2017, aufrufbar unter <https://pub.rebit.org.in/2018-09/CMM_Implementation_Guide.pdf>

Resilient, 2020. Resilient, Towards Resilient EU HPC Systems: A Blueprint, European HPC resilience initiative, 2020, aufrufbar unter <https://resilienthpc.eu/sites/default/files/pdf/Blueprint2020__Towards-Resilient-EU-HPC-Systems.pdf>

SBVg, 2013. Schweizerische Bankiervereinigung (SBVg), Empfehlungen für das Business Continuity Management (BCM), Basel 2013

SBVg, 2020. Schweizerische Bankiervereinigung (SBVg), Cloud-Leitfaden, Wegweiser für sicheres Cloud Banking, 2. Aufl. Basel 2020

SVV, 2015. Schweizerische Versicherungsverband (SVV), Business Continuity Management (BCM) für Versicherungsunternehmen in der Schweiz – Mindeststandards und Empfehlungen, Zürich 2015

TC260, 2020. The National Information Security Standardisation Technical Committee of China, 信息安全技术 个人信息安全规范 of 1 October 2020, GB/T 35273–2020 (englisch: Information security technology – Personal information security specification), Beijing 2020, aufrufbar unter <https://www.tc260.org.cn/upload/2020-09-18/1600432872689070371.pdf>

UK NCSC, 2021. National Cyber Security Centre, Financial sector cyber collaboration centre (FSCCC), London 2021, aufrufbar unter <https://www.ncsc.gov.uk/information/financial-sector-cyber-collaboration-centre-fsccc>

UN General Assembly, Dokument A/68/98. United Nations General Assembly, Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, Document A/68/98, 24 June 2013

UN General Assembly, Dokument A/70/174. United Nations General Assembly, Group of Governmental Experts on Developments in the Field of Information and Telecommunications in theContext of International Security, Document A/70/174, 22 July 2015

WKO, 2021. Wirtschaftskammer Österreich, die Finanzdienstleister, Digital Operational Resilience Act (DORA), Teil des EU-Rahmenwerks «Digital Finance Package», Wien 2021

World Bank Group, 2018. World Bank Group, Financial Sector's Cybersecurity: Regulation and Supervision, Washington D.C. 2018

Abkürzungsverzeichnis

a.M.	anderer Meinung
ABl.	Amtsblatt der Europäischen Union (Brüssel)
Abs.	Absatz
ACSC	Australian Cyber Security Center
aDSG	Bundesgesetz über den Datenschutz vom 19. Juni 1992 (SR 235.1, Stand am 1. März 2019)
AJP	Aktuelle Juristische Praxis (St. Gallen)
APPI	Act on the Protection of Personal Information (個人情報の保護に関する法律) vom 30. Mai 2003 (Act No. 57 of 2003, englische Übersetzung vom 21. Dezember 2016 aufrufbar unter <http://www.japaneselawtranslation.go.jp/law/detail/?id=2781&vm=2&re=02>)
Art.	Artikel
aVDSG	Verordnung zum Bundesgesetz über den Datenschutz vom 14. Juni 1993 (SR 235.11; Stand am 16. Oktober 2012)
B-OCI	Operationelle, Cyber- und IT-Risiken
BABS	Bundesamt für Bevölkerungsschutz
BAC	Basic Act on Cybersecurity (サイバーセキュリティ基本法) of 12 November 2014 (Act No. 104 of 2014, englische Übersetzung vom 30. September 2015 aufrufbar unter <http://www.japaneselawtranslation.go.jp/law/detail/?printID=&re=02&vm=02&id=2760&lvm=01>
BankG	Bundesgesetz über die Banken und Sparkassen vom 8. November 1934 (SR 952.0; Stand am 1. August 2021)
BankV	Verordnung über die Banken und Sparkassen vom 30. April 2014 (SR 952.02; Stand am 1. August 2021)
BBl	Bundesblatt der Schweizerischen Eidgenossenschaft
BCBS	Basel Committee on Banking Supervision
BFE	Bundesamt für Energie
BGBl.	Bundesgesetzblattes (Deutschland)
BGE	Entscheidungen des Schweizerischen Bundesgerichts
BIP	Bruttoinlandsprodukt
BIS	Bank for International Settlements
BK	Berner Kommentar
BSI	Bundesamt für Sicherheit in der Informationstechnik
BSIG	Gesetz über das Bundesamt für Sicherheit in der Informationstechnik, BSI-Gesetz vom 14. August 2009 (BGBl. I S. 2821), das zuletzt durch Artikel 12 des Gesetzes vom 23. Juni 2021 (BGBl. I S. 1982) geändert worden ist
BSK	Basler Kommentar
BWL	Bundesamt für wirtschaftliche Landesversorgung
bzgl.	bezüglich

bzw.	beziehungsweise
C-RAF	Cyber Resilience Assessment Framework
ca.	circa
CAC	Cybersecurity Administration of China
Cap.	Chapter of the Laws of Hong Kong
CBIRC	China Banking and Insurance Regulatory Commission
CBK	Common Body of Knowledge
CBRC	China Banking Regulatory Commission
CCMP	Cyber Crisis Management Plan
CCP	Central Counterparty
CEPS	Centre for European Policy Studies (Brüssel)
CERT-In	Indian Computer Emergency Response Team
CFI	Cybersecurity Fortification Initiative
CFPB	Consumer Financial Protection Bureau
CFTC	Commodity Futures Trading Commission
CHF	Schweizer Franken
CID	Costumer Identifying Data
CII	Critical Information Infrastructure
CII-Regulierung China	关键信息基础设施安全保护条例 of 17 August 2021 (National Order No. 745; englisch: Regulations on the Security and Protection of Critical Information Infrastructure, aufrufbar unter <http://www.gov.cn/zhengce/content/2021-08/17/content_5631671.htm?mc_cid=da5881cf31&mc_eid=a268621911>)
CIISI-EU	Cyber Information and Intelligence Sharing Initiative
CIRC	China Insurance Regulatory Commission
CISA	Cybersecurity Information Sharing Act of 2015, To improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes, enacted 17 March 2015 (Stand am 28. Oktober 2015, 29 Stat. 2936, kodifiziert unter 6 U.S.C. §§ 1501–1510)
CISP	Cyber Intelligence Sharing Platform
CISSP	Certified Information Systems Security Professional
CLSR	Computer Law & Security Review (Amsterdam/London)
CMM	Cyber Security Maturity Model
COBIT	Control Objectives for Information and Related Technology
CPC	State Council of the People's Republic of China
CR	Computer und Recht (Köln)
CRAFT	Comprehensive Risk Assessment Framework and Techniques
CRi	Computer Law Review International, Computer und Recht International (Köln)
CSA	Cyber Security Agency of Singapore
CSIRT	Computer Security Incident Response Team
CSIS	Center for Strategic and International Studies

CSL	Cybersecurity Law of the People's Republic of China (中华人民共和国网络安全法) of 7 November 2016 (Stand am 1. Juni 2017, englische Übersetzung aufrufbar unter <https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china/>)
CSS	Center for Security Studies
CTI	Cyber Threat Intelligence
Cybersecurity Act 2018	Republic of Singapore, Government Gazette, Act Supplement, Cybersecurity Act 2018, Published by Authority, No. 9, 16 March 2018, aufrufbar unter <https://sso.agc.gov.sg/Acts-Supp/9-2018/>
CyRV	Verordnung über den Schutz vor Cyberrisiken in der Bundesverwaltung vom 27. Mai 2020 (SR 120.73, Stand am 1. April 2021)
d.h.	das heisst
DBB	Deutsche Bundesbank
DeFi	Dezentralisierte Finanzmärkte
DLT	Distributed Ledger Technologie
DND	Department of National Defence (Canada)
DNS	Domain Name System
DNSSEC	Domain Name System Security Extensions
DORA	Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die Betriebsstabilität digitaler Systeme des Finanzsektors und zur Änderung der Verordnungen (EG) Nr. 1060/2009, (EU) Nr. 648/2012, (EU) Nr. 600/2014 und (EU) Nr. 909/2014 vom 24. September 2020 (Englisch: Digital Operational Resilience Act)
DPA 2018	Data Protection Act 2018 of 23 May 2018 (UK Public General Acts, 2018 c. 12; Stand am 19. August 2018)
DPP	Data Protection Principles
DSGVO	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 (Datenschutz-Grundverordnung) (Text von Bedeutung für den EWR), ABl. L 119 vom 4.5.2016, 1–88
DSL	Data Security Law of the People's Republic of China (中华人民共和国数据安全法) of 10 June 2021 (derzeit keine Übersetzung vorhanden; chinesisches Gesetz aufrufbar unter <http://www.npc.gov.cn/englishnpc/c23934/202112/1abd8829788946ecab270e469b13c39c.shtml>)
dt.	deutsch
Durchführungsbeschluss (EU) 2019/419	Commission Implementing Decision (EU) 2019/419 of 23 January 2019 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by Japan under the Act on the Protection of Personal Information (Text with EEA relevance), ABl. L 76, 19.3.2019, 1–58
DV	Direktion für Völkerrecht
EBA	Europäische Bankenaufsichtsbehörde
Ecol. Soc.	Ecology and Society – A journal for integrative science for resilience and sustainability (Ontario)

ECRB	The Euro Cyber Resilience Board for pan-European Financial Infrastructures
ed.	edition (= Auflage)
Ed./Eds.	Editor/Editors (= Herausgeber)
EDÖB	Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter
EFD	Eidgenössisches Finanzdepartement
EFK	Eidgenössische Finanzkontrolle
EIOPA	Europäische Aufsichtsbehörde für das Versicherungswesen und die betriebliche Altersversorgung
EJIR	European Journal of International Relations (London)
EJPD	Eidgenössisches Justiz- und Polizeidepartement
Empfehlung der Kommission für eine koordinierte Reaktion	Empfehlung (EU) 2017/1584 der Kommission vom 13. September 2017 für eine koordinierte Reaktion auf grosse Cybersicherheitsvorfälle und -krisen, ABl. L 239 vom 19.9.2017, 36–58
EnG	Energiegesetz vom 30. September 2016 (SR 730.0; Stand am 1. Januar 2021)
ENISA	Agentur der Europäischen Union für Cybersicherheit
Erw.	Erwägung
ESMA	Europäische Wertpapier- und Marktaufsichtsbehörde
ETH	Ether
EU	Europäische Union
EuCML	Journal of European Consumer and Market Law (München)
Eur. Foreign Aff. Rev.	European Foreign Affairs Review (Alphen aan den Rijn)
EY	Ernst & Young
EZB	Europäische Zentralbank
FCA	Financial Conduct Authority
FinfraG	Bundesgesetz über die Finanzmarktinfrastrukturen und das Marktverhalten im Effekten- und Derivatehandel vom 19. Juni 2015 (SR 958.1; Stand am 1. August 2021)
FINMA	Eidgenössische Finanzmarktaufsicht FINMA
FINMAG	Bundesgesetz über die Eidgenössische Finanzmarktaufsicht vom 22. Juni 2007 (SR 956.1; Stand am 1. Januar 2020)
FINRA	Financial Industry Regulatory Authority
FIRST	Forum of Incident Response and Security Teams
FMA	Finanzmarktaufsicht Liechtenstein
FMAG	Gesetz über die Finanzmarktaufsicht vom 18. Juni 2004, LGBl.-Nr. 2004.175 (LR-Nr. 952.3)
FMID	Financial Market Infrastructure Directorate
FSB	Financial Stability Board
FSCCC	Financial Sector Cyber Collaboration Centre
FSIC	Center for Financial Industry Information Systems
FTC	Federal Trade Commission (USA)

FTC Act	An Act to create a Federal Trade Commission, to define its powers and duties, and for other purposes of 26 September 1914 (Stand am 5. Januar 2021, 38 Stat. 717, Chapter 311, kodifiziert unter 15 U.S.C. §§ 41-58)
gl.M.	gleicher Meinung
GLBA	Gramm-Leach-Bliley Act, An Act to enhance competition in the financial services industry by providing a prudential framework for the affiliation of banks, securities firms, and other financial service providers, and for other purposes of 12 November 1999 (113 Stat. 1338, kodifiziert unter 12 U.S.C. § 24a, § 248b, § 1831v, § 1831w, § 1831x, § 1831y, § 1848a, § 2908, 15 U.S.C. § 80b–10a, 15 U.S.C. § 6801–6809, 15 U.S.C. § 6821–6827)
GLJ	German Law Journal (Stuttgart)
h.L.	herrschende Lehre
HAVE	Haftung und Versicherung (Zürich)
HKAB	Hong Kong Association of Banks
HKASTARI	Hong Kong Applied Science and Technology Research Institute
HKFSBCM	Hong Kong Financial Services Business Continuity Management Forum
HKMA	Hong Kong Monetary Authority
HKSFC	Hong Kong Securities and Futures Commission
Hong Kong Banking Ordinance	(Hong Kong) Banking Ordinance of 1 September 1986, T-2 Cap. 155, (Stand am 12. Dezember 2019), aufrufbar unter <https://www.elegislation.gov.hk/hk/cap155>
HPC	High-Performance Computing
Hrsg.	Herausgeber
ICJ	International Court of Justice
ICO	Information Commissioner's Office
IDS	Intrusion Detection System
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IGH	Internationaler Gerichtshof
IIS	Issues in Information Systems (Stillwater, OK)
IKT	Informations- und Kommunikationstechnik
IMF	International Monetary Fund
Informatik Spektrum	Informatik Spektrum. Organ der Gesellschaft für Informatik e.V. und mit ihr assoziierter Organisationen (Berlin)
inkl.	inklusive
IOSCO	International Organization of Securities Commissions
Iowa Law Rev.	Iowa Law Review (Iowa City)
IRDAI	Insurance Regulatory and Development Authority (Indien)
ISACA	Information Systems Audit and Control Association
ISF	Information Security Forum

ISO	International Organisation for Standardisation
ISSA	Information Systems Security Association
IT	Informationstechnik
ITA	Information Technology Act, 2000, of 9 June 2000 (No. 21 of 2000, aufrufbar unter <https://www.meity.gov.in/writereaddata/files/itbill2000.pdf>)
ITA Amendment	Information Technology (Amendment) Act, 2008, of 5 February 2009 (No. 10 of 2009, aufrufbar unter <https://www.meity.gov.in/writereaddata/files/it_amendment_act2008%20%281%29_0.pdf>)
ITA-Rules	The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, of 13 April 2011, aufrufbar unter <https://www.wipo.int/edocs/lexdocs/laws/en/in/in098en.pdf>
ITIL	Information Technology Infrastructure Library
ITU	International Telecommunication Union
IXP	Internet Exchange Point
J. Cybersecur.	Journal of Cybersecurity (Oxford)
J. Gov. Regul.	Journal of Governance and Regulation (Sumy)
J. Leg. Anal.	Journal of Legal Analysis (Cambridge, MA)
J. Risk Manag. Financ. Inst.	Journal of Risk Management in Financial Institutions (London)
JCSH	Cybersecurity Strategic Headquarters (Japan)
JFSA	Japanese Financial Services Agency
JIBFL	Journal of International Banking and Financial Law (London)
JIPA	Information-technology Promotion Agency (Japan)
JMETI	Ministry of Economy, Trade and Industry (Japan)
JNICT	National Institute of Information and Communications Technology (Japan)
JNISC	National Center of Incident Readiness and Strategy for Cybersecurity of Japan
JPPC	Personal Information Protection Commission (Japan)
Kap.	Kapitel
LGBl.	Liechtensteinisches Landesgesetzblatt
lit.	litera
LR	Systematische Sammlung der liechtensteinischen Rechtsvorschriften
LVG	Bundesgesetz über die wirtschaftliche Landesversorgung vom 17. Juni 2016 (SR 531; Stand am 1. Januar 2020)
m.w.H.	mit weiteren Hinweisen
MAS	Monetary Authority of Singapore
MeitY	Ministry of Electronics and Information Technology (Indien)
MELANI	Melde- und Analysestelle Informationssicherung
MIIT	Ministry of Industry and Information Technology (China)

Mio.	Million(en)
MLPS	Multi-Level Protection Scheme
MMR	Multimedia und Recht (München)
MPS	Ministry of Public Security (China)
Nat. Law Rev.	The National Law Review (Chicago)
NATO	North Atlantic Treaty Organization
NBG	Bundesgesetz über die Schweizerische Nationalbank vom 3. Oktober 2003 (SR 951.11; Stand am 1. August 2021)
NCA	National Crime Agency
NCIIPC	National Critical Information Infrastructure Protection Centre (Indien)
NCSC	Nationale Zentrum für Cybersicherheit
nDSG	Bundesgesetz über den Datenschutz vom 25. September 2020 (BBl 2020, 7639 ff.) (voraussichtliches Inkrafttreten: 1. September 2023)
NFA	National Futures Association
NIS Regulations	The Network and Information Systems Regulations 2018 of 19 April 2019 (UK Statutory Instruments, 2018 No. 506; Stand am 20. Januar 2021, aufrufbar unter <https://www.legislation.gov.uk/uksi/2018/506>
NIS-Richtlinie	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 194 vom 19.7.2016, 1–30
NISC	National Center of Incident Readiness and Strategy for Cybersecurity (Japan)
NIST	National Institute of Standards and Technology
Notice on Cyber Hygiene	MAS Notice No.: 655 Notice to banks in Singapore Banking Act (Cap. 19), Notice on Cyber Hygiene of 6 August 2019
Nr./No.	Nummer
NZZaS	Neue Zürcher Zeitung am Sonntag (Zürich)
OCIE	Office of Compliance Inspections and Examinations
OeNB	Oesterreichische Nationalbank AG
OR	Bundesgesetz betreffend die Ergänzung des Schweizerischen Zivilgesetzbuches (Fünfter Teil: Obligationenrecht) vom 30. März 1911 (SR 220; Stand am 1. Januar 2022)
PBoC	People's Bank of China
PCPD	Privacy Commissioner for Personal Data
PDP	Professional Development Program
PDPA	Republic of Singapore, Government Gazette, Act Supplement, Personal Data Protection Act 2012, Published by Authority, No. 25, of 7 December 2012, aufrufbar unter <https://sso.agc.gov.sg/Act/PDPA2012>
PDPC	Personal Data Protection Commission

PDPO	(Hong Kong) Personal Data (Privacy) Ordinance of 1 August 1996, E-2 Cap. 486 (Stand am 20. April 2018), aufrufbar unter <https://www.elegislation.gov.hk/hk/cap486!en-zh-Hant-HK.pdf?FROMCAPINDEX=Y>
PFMI	Principles for Financial Market Infrastructures
PfPC	Partnership for Peace Consortium of Defense Academies and Security Studies Institutes
PIPL	Personal Information Protection Law of China (中华人民共和国个人信息保护法) of 1 November 2021 (verabschiedet am 20. August 2021, englische Übersetzung aufrufbar unter <https://digichina.stanford.edu/work/translation-personal-information-protection-law-of-the-peoples-republic-of-china-effective-nov-1-2021/>)
PRA	Prudential Regulation Authority
PrHG	Bundesgesetz über die Produktehaftpflicht vom 18. Juni 1993 (SR 221.112.944; Stand am 1. Juli 2010)
PTSP	Penetration Test Service Provider
PwC	PricewaterhouseCoopers International
RBI	Reserve Bank of India
ReBIT	Reserve Bank Information Technology Private Limited (Indien)
recht	Zeitschrift für juristische Weiterbildung und Praxis (Bern)
Rechtsakt zur Cybersicherheit	Verordnung (EU) 2019/881 des Europäischen Parlaments und des Rates vom 17. April 2019 über die ENISA (Agentur der Europäischen Union für Cybersicherheit) und über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik und zur Aufhebung der Verordnung (EU) Nr. 526/2013 (Rechtsakt zur Cybersicherheit) (Text von Bedeutung für den EWR), ABl. L 151 vom 7.6.2019, 15–69
Richtlinie (EU) 2016/680	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 119, 4.5.2016, 89–131
Rn.	Randnote(n)
s.	siehe
SBVg	Schweizerische Bankiervereinigung
SC	Strategic Change (Chichester, West Sussex)
SEBI	Securities and Exchange Board of India
SEC	Securities and Exchange Commission
Seton Hall Const. Law J.	Seton Hall Constitutional Law Journal (Newark, N.J.)
SICAV	Société d'investissement à capital variable (Investmentgesellschaft mit variablem Kapital)
SIEM	Security Information and Event Management
SJZ	Schweizerische Juristen-Zeitung / Revue Suisse de Jurisprudence (Zürich)
SKI	Schutz kritischer Infrastrukturen

SNB	Schweizerische Nationalbank
sog.	sogenannt
StGB	Schweizerisches Strafgesetzbuch vom 21. Dezember 1937 (SR 311.0; Stand am 1. Januar 2022)
StromVG	Bundesgesetz über die Stromversorgung vom 23. März 2007 (SR 734.7; Stand am 1. Juni 2021)
StromVV	Stromversorgungsverordnung vom 14. März 2008 (SR 734.7; Stand am 1. Juni 2021)
SVV	Schweizerische Versicherungsverband
SYSC	Senior Management Arrangements, Systems and Controls
SZW	Schweizerische Zeitschrift für Wirtschafts- und Finanzmarktrecht (Zürich)
TC260	The National Information Security Standardisation Technical Committee of China
TIBER-EU	European framework for threat intelligence-based ethical red-teaming
Total Qual. Manag. Bus. Excell.	Total Quality Management & Business Excellence (Abingdon)
TRMG	Technology Risk Management Guidelines
TRS	Technology Risk Supervision
u.a.	unter anderem
UK	United Kingdom = Vereinigtes Königreich
UK DSGVO	Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (United Kingdom General Data Protection Regulation; Regulations originating from the EU, 2016 No. 679)
UK NCSC	National Cyber Security Centre (Vereinigtes Königreich)
UN	United Nations
UNGGE	United Nations Group of Governmental Experts
URL	Uniform Resource Locator
USA	Vereinigte Staaten von Amerika
USD	US-Dollar
VE-ISG	Vernehmlassungsentwurf des Eidgenössisches Finanzdepartement (EFD) zur Änderung des Bundesgesetzes über die Informationssicherheit beim Bund vom 12. Januar 2022
VE-VDSG	Vorentwurf der Verordnung zum Bundesgesetz über den Datenschutz vom 23. Juni 2021
Verordnung über restriktive Massnahmen gegen Cyberangriffe	Verordnung (EU) 2019/796 des Rates vom 17. Mai 2019 über restriktive Massnahmen gegen Cyberangriffe, die die Union oder ihre Mitgliedstaaten bedrohen, ABl. L 129 vom 17.5.2019, 1–12
WISE	Whole Industry Simulation Exercise
WKO	Wirtschaftskammer Österreich
WTO	World Trade Organization
z.B.	zum Beispiel

ZaöRV	Zeitschrift für ausländisches öffentliches Recht und Völkerrecht (München)
ZSR	Zeitschrift für Schweizerisches Recht / Revue de droit suisse (Basel)

I. Einleitung

Die Digitalisierung verändert die sozialen, kulturellen, ökonomischen und rechtlichen Aspekte des Lebens und befruchtet die Innovationsanreize der Gesellschaft; sie hat in verschiedener Hinsicht eine «neue Welt» geschaffen. Die Grundlagen und Leitprinzipien im Bereich des Cyberspace (dt. «Raum der Kybernetik») sind weiterhin im Begriff, sich zu entwickeln.

Wie schon vor knapp 30 Jahren lassen sich auch heute der «Cyberspace» und seine rechtliche Regulierung nicht abschliessend definieren.[1] Dennoch ist anerkannt, dass eine gewisse Strukturierung erforderlich ist; Diskussionen über die «*Governance*» des Cyberspace und des Internets sind seit den ersten Entwicklungen in den 90er Jahren aktuell geblieben.[2]

Der Begriff «*Governance*» geht auf das griechische Wort «*kybernetes*», den Steuermann, zurück; darauf stützt sich das lateinische Wort «*gubernator*», der Statthalter bzw. Gouverneur. Dementsprechend betrifft die IT-Governance diejenigen Massnahmen, welche den Schutz der Daten und Informationen sowie deren zugrundeliegenden Vermögenswerte und Infrastrukturen zum Ziel haben.[3]

Ursprünglich beschrieb die IT-Governance bloss die Verwaltung und Gestaltung der Technologien, welche das Internet funktionsfähig halten und Massnahmen in diesem Zusammenhang ermöglichen. Verschiedene Fachrichtungen versuchen seither, die Probleme rund um die «*Governance*» zu thematisieren; diese Überlegungen lassen sich zusammenfassen als Diskussion über die angemessene Zuweisung von Aufgaben und Zuständigkeiten sowie die richtige Strukturierung der betreffenden Organe im Cyberspace.[4]

---

1 Die Aussage, dass die Rechtsordnung im Cyberspace nicht zur Geltung komme (so *Ryga*, 1995, 223), geht hingegen zu weit; vgl. auch *Weber*, 2009, 26.

2 Vgl. *Weber/Grosz*, 2009, 119 ff.; ferner *Weber*, 2021a, 3 f.; *Weber*, 2021b, Rn. 1 f.

3 *Weber*, 2021c, 1.

4 Alternativ lässt sich der Begriff auch in den Worten von *Ruggie* umschreiben: «Governance, at whatever level of social organization it may take place, refers to conducting the public's business—to the constellation of authoritative rules, institutions and practices by means of which any collectivity manages its affairs» (*Ruggie*, 2004, 504).

Gleichzeitig mit den schnellen Entwicklungen im Bereich der Informationstechnologie sind aber auch Herausforderungen aufgetreten. Ein besonderes Risiko betrifft die Finanzinfrastrukturanbieter und die Finanzdienstleister, da sich im Zuge der Digitalisierung auch ihr operatives Tagesgeschäft änderte; nicht selten hängt der Geschäftsbetrieb von den digitalen Umgebungen und Dienstleistungen (intern oder durch Dritte erbracht) ab. Diese Abhängigkeit schafft zusätzliche technische Gefahren und Schwächen im System. Ein grosses Risiko stellen die Sicherheits- bzw. Cybervorfälle dar, also das Fehlschlagen von Massnahmen und der Schutz vor einem nicht autorisierten Zugriff bzw. Zugriffsversuch auf das System.

Die Zahl verschiedenartiger Cybervorfälle hat sich in letzter Zeit nicht nur vermehrt, sondern sie betreffen zudem bedeutendere Bereiche und sind ausgeklügelter;[5] sie vermögen ganze Ökosysteme, Staaten, Unternehmen oder auch Individuen lahmzulegen. Die Lehre versucht, die Cybergefahren in sich teils überschneidende Kategorien zu unterteilen: Cyberkrieg, Cyberspionage, Cyberterrorismus und -vandalismus sowie Cyberkriminalität.[6] Zur Cyberkriminalität, welche kriminelle Tätigkeiten an sich beschreibt, gehören Aktivitäten wie z.B. das «Phishing», der Internetbetrug, die Fälschung im Internet oder auch der Identitätsdiebstahl.[7] Die Cyberkriminalität nimmt nicht nur schnell zu, sondern hat auch erhebliche ökonomische Folgen: Im Jahre 2016 betrugen die durch Cyberkriminalität verursachten Kosten 0.8% des weltweiten BIP und im Jahre 2024 sollen sie sich insgesamt auf 5 Billionen USD belaufen.[8]

Mit Blick auf den Finanzmarkt wird die Bedeutung der Cybersicherheit und der Cyber-Resilienz schnell ersichtlich: *Cœuré* hält es für möglich, dass «the next financial crisis may well start as a cyber-incident»[9]; auch Finanzminister und Zentralbankpräsidenten hielten am G-20 Treffen fest, dass «the malicious use of information and communication technologies could disrupt financial services crucial to both national and international financial systems, undermine security and confidence, and endanger financial stability»[10].

5 *Cœuré*, 2018; zur Umschreibung der Cybervorfälle vgl. hinten Kap. II.A.4.

6 *Calliess/Baumgarten*, 2020, 1151 ff. m.w.H.

7 *Bendiek/Porter*, 2013, 158 f.; *Calliess/Baumgarten*, 2020, 1152.

8 *Lewis*, 2018, 6 f.; *Juniper Research*, 2019; *Calliess/Baumgarten*, 2020, 1152.

9 *Cœuré*, 2018.

10 *G-20*, 2017.

Um die Folgen dieser Risiken zu lindern, haben sich im Bereich der Cybersicherheit verschiedene Grundsätze herausgebildet, welche der Eindämmung und effizienten Bekämpfung der Cybervorfälle dienlich sein sollen. Dabei ist wichtig, sich vor Augen zu führen, dass jeweils das schwächste Glied den Massstab der Verteidigung darstellt, denn Angreifer wählen grundsätzlich den Weg des geringsten Widerstands, um ihre Ziele zu erreichen.[11]

Diese Situation führt insbesondere dann zu grossen Sicherheitsproblemen, wenn Akteure eines Sektors funktionsbedingt eng miteinander verknüpft sind. In den Finanzmärkten zeigt sich dies auf verschiedenen Ebenen: Aufgrund der Internationalisierung genügt es einerseits, dass ein beliebiger Finanzdienstleister weltweit betroffen ist und die Angreifer mit «falscher Identität» die Sicherheitsvorkehren weiterer Dienstleister aushebeln können. Andererseits ist eine vergleichbare Situation innerhalb eines Betriebs beobachtbar: Über verschiedene Ebenen gesicherte Kundendaten sind erst sicher, wenn überall im Betrieb Sicherheitsvorkehren getroffen wurden. Folglich bleiben die Beteiligten selbst bei schärfsten Sicherheitsvorkehren vulnerabel, sofern nicht das schwächste Glied verbessert wird.

Dass Cybervorfälle ein hohes Risiko bergen, sind sich gemäss Bankenbarometer von Ernst & Young auch die Banken längst bewusst, denn seit dem Jahr 2010 wird die Cybersicherheit als prioritäres Thema behandelt und hat jährlich an Bedeutung gewonnen.[12]

Zudem sind nicht nur die Finanzdienstleister erheblichen Risiken ausgesetzt, sondern auch die als resilient und sicher bzw. unveränderlich angesehenen Distributed Ledger Technologien (DLT). Im Zuge des sog. «DAO-Hacks» konnten nämlich Angreifer durch Ausnutzung eines «Loophole» im Jahre 2016 ca. 12 Millionen Ether (ETH) zum damaligen Wert von über CHF 55 Mio. entwen-

11 *Bendiek/Pander Maat*, 2020, 39.

12 EY, 2021.

den.[13] Im Jahre 2021 gelang es einem Hacker mit einem Angriff auf die DeFi-Plattform[14] «Poly Network», über CHF 550 Mio in Kryptowährungen zu stehlen.[15]

Diese Vorfälle zeigen, weshalb ein angemessener Schutz der Bankensysteme bzw. des gesamten Finanzmarktes nicht leicht zu erreichen ist: Für die Eidgenössische Finanzkontrolle (EFK) sind die Risiken der Interbanken-Zahlungssysteme «nach wie vor eine Blackbox».[16] Betreiber von kritischen Infrastrukturen können solche Angriffe melden, im Finanzwesen sind die Akteure sogar dazu verpflichtet; indessen hält die EFK fest, dass die Finanzdienstleister sich nicht immer an die Meldepflicht gehalten haben.[17]

Dieses Buch behandelt zunächst die allgemeinen Grundsätze der Cybersicherheit und der Cyber-Resilienz (II.). Basierend auf den erläuterten Grundsätzen wird die gegenwärtige Rechtslage in der Schweiz und auf weiteren, wichtigen Handelsplätzen dargestellt; der Fokus liegt auf der rechtlichen Umsetzung der Grundsätze in Liechtenstein, in der Europäischen Union, im Vereinigten Königreich, in den USA sowie in Singapur, Hong Kong, China, Japan und Indien (III.). In diesem Zusammenhang ist auch zu ermitteln, ob die verschiedenen Rechtsordnungen die Grundsätze der Cybersicherheit und der Cyber-Resilienz bereits sachgerecht umsetzen und ob sich neue, rechtliche Rahmenbedingungen für die Schweiz als erforderlich erweisen.

---

13 *Meier/Schuppli*, 2019, 32 ff.

14 Eine DeFi-Plattform ist eine sog. «cross-chain decentralized finance platform» (DeFi bedeutet dezentralisierte Finanzmärkte). Solche Plattformen basieren auf Smart Contracts und dezentralisierten autonomen Organisationen und kommen im Rahmen der Blockchain vor. Die «cross-chain» DeFi-Plattformen bieten eine «Cross-Chain»-Architektur (eine Architektur, die zwischen verschiedenen Blockchain funktionsfähig ist) an. Diese Architektur erleichtert die Interoperabilität, indem sie zwei oder mehr Blockchains in die Lage versetzt, ihre Dezentralisierung, ihren Funktionsumfang und ihre Sicherheit miteinander in Einklang zu bringen.

15 *Daniel Meier*, Keine Waffe, kein Sprengstoff, kein Fluchtauto: Wie ein Hacker über 610 Millionen Dollar stehlen konnte, NZZaS vom 29.08.2021, aufrufbar unter <https://nzzas.nzz.ch/hintergrund/ein-hacker-und-der-groesste-diebstahl-der-geschichte-ld.1642710>; *Gertrude Chavez-Dreyfuss/Michelle Price*, Explainer: How hackers stole and returned 0 mln in tokens from Poly Network, aufrufbar unter <https://www.reuters.com/technology/white-hat-hacker-has-returned-nearly-all-600-million-crypto-tokens-taken-tuesday-2021-08-12/>.

16 *EFK*, 2021, 19.

17 *EFK*, 2020, 18 f.

In einem nächsten Schritt sind Handlungsempfehlungen für Finanzunternehmen auszuarbeiten, welche insbesondere den Vorschlag der EU für einen Digital Operational Resilience Act (DORA) mitberücksichtigen (IV.). Dabei soll ein holistischer Ansatz den dynamischen Entwicklungen im Bereich der Digitalisierung Rechnung tragen. Schliesslich geht das Buch auf weitere Rechtsbereiche ein und macht Vorschläge zur Umsetzung von Sanktionsmechanismen (V.). Den Abschluss bildet eine Zusammenfassung mit einem Ausblick (VI.).

II. Übersicht zum Regelungsrahmen von Cybersicherheit und Cyber-Resilienz

Dieses Kapitel setzt sich zunächst mit den Begrifflichkeiten im Bereich der Cybersicherheit und Cyber-Resilienz auseinander (A.); hernach ist eine Einführung der IT-Sicherheit als Rahmenordnung erforderlich (B.). Überdies kommen die möglichen Vorkehren zur Gewährleistung der Cybersicherheit zur Sprache (C.); schliesslich erfolgt eine Beurteilung der verschiedenen Arten der Rechtsquellen, die im Bereich der Cybersicherheit von besonderer Bedeutung sind (D.).

A. Begriffe

1. Cybersicherheit

Der Begriff Cybersicherheit (bzw. «cybersecurity») hat weder im deutschen noch im englischen Sprachgebrauch eine einheitliche Definition gefunden. Cybersicherheit und «cybersecurity» werden – aufgrund der gegenwärtigen Aktualität der Begriffe – in der Literatur oft als Schlagwörter verwendet, um das Sicherheitsbedürfnis im Zeitalter des Internets aufzuzeigen.[18] Die Umschreibung der Cybersicherheit in Art. 3 lit. a CyRV als «anzustrebender Zustand, bei dem die Datenbearbeitung, insbesondere der Datenaustausch zwischen Personen und Organisationen, über Informations- und Kommunikationsinfrastrukturen wie beabsichtigt funktioniert», ist immerhin eine gute Orientierungshilfe, um sich der Thematik anzunähern.

Im weitesten Sinne umfasst die Cybersicherheit diejenigen Gefahren, die sich durch die Kopplung von gesellschaftlichen Vorgängen an die Digitalisierung ergeben. Die Cybersicherheit betrifft einerseits die Fähigkeit, Angriffen zu widerstehen, welche die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit digitaler Daten zu beeinträchtigen versuchen, d.h. die Sicherheit der Netzwerk- und Informationssysteme. Andererseits beschäftigt sie sich auch mit der Bekämpfung von Cyberangriffen sowie der Cyberverteidigung.[19] Die Cybersicherheit beinhaltet verschiedenste Bereiche, wie z.B. den Schutz von

---

18 *Weber*, 2020, 280; *Weber/Studer*, 2016, 716 f. m.w.H.

19 *Calliess/Baumgarten*, 2020, 1150; ferner *Kosseff*, 2018, 988 f.

persönlichen, finanziellen und kommerziellen Daten sowie die Sicherstellung der Betriebskontinuität oder der Dienstleistungen. Neben den «Online»-Gefahren sind auch der physische Zugang zu den Daten zu sichern, kritische Daten zu verschlüsseln oder der Schutz der Privatsphäre der Kunden zu gewährleisten.[20]

Das Konzept der Cybersicherheit steht in engem Zusammenhang mit ähnlichen Konzepten, wie z.B. der «Informationssicherheit» oder «IT-Sicherheit» (bzw. «IKT-Sicherheit»). Die ISO/IEC-27000-Reihe definiert die Informationssicherheit als «preservation of confidentiality, integrity, and availability of information». Die Ähnlichkeiten treten in der Definition der Cybersicherheit als «preservation of confidentiality, integrity, and availability of information in the Cyberspace» hervor; der Zusatz «Cyberspace» ist als «the complex environment resulting from the interaction of people, software and services on the Internet by means of technology devices and networks connected to it, which does not exist in any physical form» umschrieben.[21]

Zur Cybersicherheit gehört jedoch nicht bloss der Schutz von Informationen und Daten (also Datensicherheit), sondern auch der Schutz von nicht informationsbasierten «assets», die für IKT-Bedrohungen anfällig sind.[22] Die International Telecommunication Union (ITU) nimmt in ihrer Definition der Cybersicherheit den Schutz der «assets» auf:

> «Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets.»[23]

Die «organization and user's assets» umfassen u.a. «connected computing devices». Gemäss ITU soll die Cybersicherheit gewährleisten, dass die Sicherheitseigenschaften der «organization and user's assets» gegen relevante Sicherheitsrisiken in der Cyberumgebung erreicht und aufrechterhalten werden. Zu den allgemeinen Sicherheitszielen gehören die Vertraulichkeit («confi-

---

20 *Thakur/Khan Pathan*, 2020, 31.

21 Die Definition der Cybersicherheit und des Cyberspace befindet sich in ISO/IEC 27032:2012, Information technology – Security techniques – Guidelines for cybersecurity, Technologies de l'information – Techniques de sécurité – Lignes directrices pour la cybersécurité.

22 *Weber*, 2020, 281.

23 Vgl. für die Definition der ITU <https://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx>.

dentiality»), die Integrität («integrity»)[24] und die Verfügbarkeit («availability»); diese drei Aspekte werden oft als CIA-Triade bezeichnet.[25] Vertraulichkeit bedeutet, dass Informationen nicht unrechtmässig an unbefugte Personen, Prozesse oder Geräte weitergegeben werden. Zur Integrität gehört, dass die Informationen vor unbefugter Zerstörung oder Veränderung geschützt sind. Verfügbarkeit drückt aus, dass autorisierte Benutzer zeitnah und zuverlässig auf Daten und Informationen zugreifen können.[26]

2. Cyber-Resilienz

Die Cybersicherheit allein genügt aber nicht, um ein stabiles und zuverlässiges System anzubieten; von Bedeutung sind auch die Widerstandsfähigkeit von Systemen und das Können, belastende Situationen zu meistern (sog. Cyber-Resilienz). Unter Resilienz ist die Fähigkeit von technischen Systemen zu verstehen, bei Störungen bzw. Teilausfällen nicht vollständig zu versagen, sondern wesentliche Systemdienstleistungen aufrechtzuerhalten.[27] Theoretisch betrachtet geht es um die Möglichkeit eines komplexen Systems, trotz massiver Störungen wieder in den Ausgangszustand zurückzukehren und grössere Systemzusammenbrüche zu vermeiden.[28]

Der Begriff der Resilienz findet sich – nicht zuletzt mit Blick auf eine interdisziplinäre Offenheit und Verknüpfung der Systeme – in neuerer Zeit auch in den Sozialwissenschaften, z.B. (i) als Fähigkeit von Gesellschaften, externe Störungen zu verkraften, ohne dass sich ihre wesentlichen Systemfunktionen ändern, bzw. (ii) als Beschreibung dynamischer Stabilitätseigenschaften ökologischer Systeme.[29] In ähnlicher Weise umschreibt auch der Bundesrat in Art. 3 lit. d CyRV die Resilienz als «die Fähigkeit eines Systems, einer Organisation oder einer Gesellschaft, intern oder extern verursachten Störungen zu widerstehen und das ordnungsgemässe Funktionieren zu erhalten oder dieses möglichst rasch und vollständig wiederzuerlangen».

---

24 Gemäss ITU kann die Integrität auch die die Authentizität und Unverfälschbarkeit umfassen.

25 *Weber*, 2020, 281.

26 *Weber/Studer*, 2016, 717.

27 *Resilient*, 2020, 11.

28 *Nagel*, 2020, 151 f.; vgl. ferner *Walker et al.*, 2006, 2.

29 *Walker et al.*, 2006, 2 f.

3. Cyber-Systemstabilität

Im Finanzmarktrecht spielt der Begriff der Systemstabilität eine besondere Rolle. Risiken für die Systemstabilität können von verschiedensten Faktoren herrühren, v.a. von Gefahren für die Cybersicherheit und die Cyber-Resilienz. Technologische Risiken betreffen insbesondere die Infrastrukturen. Mit Bezug auf Netzwerke, über die sich Zahlungen abwickeln lassen, sieht Art. 19 NBG ausdrücklich vor, dass die Nationalbank, um die Stabilität des Finanzsystems zu schützen, systemisch bedeutsame zentrale Gegenparteien, Zentralverwahrer und Zahlungssysteme (d.h. systemisch bedeutsame Finanzmarktinfrastrukturen) überwacht.

Mit dem Bundesgesetz zur Anpassung des Bundesrechts an Entwicklungen der Technik verteilter elektronischer Register (Distributed Ledger Technology, DLT) sind die Anwendungsbereiche des NBG und des FinfraG zudem auf die Überwachung der DLT-Handelssysteme ausgeweitet worden. Die DLT-Handelssysteme können neben Handelsdienstleistungen für DLT-Effekten (kryptobasierte Vermögenswerte) auch Nachhandelsdienstleistungen anbieten; folglich ist ein Angebot von Dienstleistungen im Bereich der Zentralverwahrung, Abrechnung oder Abwicklung möglich (Art. 73*e* Abs. 2 FinfraG).[30] Der Vorteil der DLT-Netzwerke besteht darin, dass die Abwicklung der Transaktionen in einem Peer-to-Peer Netzwerk ohne Intermediäre erfolgt und somit der Ausfall eines Teilnehmers ohne Probleme durch die restlichen Teilnehmer kompensiert werden kann.[31]

Im Gegensatz zur Cyber-Resilienz bezieht sich die Systemstabilität auf die Fähigkeit, die Funktionen von Systemen auch in Anspannungsphasen oder Umbrüchen effizient abzuwickeln. Die Finanzsysteme müssen folglich in der Lage sein, Schocks zu absorbieren und dabei die essenziellen Funktionen des Systems zu gewährleisten. Insbesondere der Nationalbank obliegt die Aufgabe, die Solidität und Leistungsfähigkeit des schweizerischen Finanzsystems sicherzustellen.[32]

---

30 *Weber*, 2021d, Rn. 28; vgl. ferner *Komm. NBG-Häusermann*, 2021, Art. 19 Rn. 5.

31 Vgl. hierzu *Drescher*, 2017, 206 f.; *Glatz*, 2018, 62; vgl. im Einzelnen dazu *Rolf H. Weber*, Sicherheit und Resilienz in DLT-basierten Finanzinfrastrukturen, erscheint im Frühling 2022 in Weblaw (online).

32 *Nagel*, 2020, 149 f.; vgl. auch DBB, Glossar «Finanzstabilität», aufrufbar unter <https://www.bundesbank.de/action/de/723820/bbksearch?firstLetter=F>; OeNB, Finanzmarktstabilität, aufrufbar unter <https://www.oenb.at/finanzmarkt/finanzmarktstabilitaet.html>; EZB, Finanzstabilität und makroprudenzielle Politik, aufrufbar unter <https://www.ecb.europa.eu/ecb/tasks/stability/html/index.de.html>.

4. Cybervorfall

Ein Cybervorfall tritt im Fall der Störung des normalen Betriebs ein. Unterscheiden lässt sich zwischen passiven Angriffen (unautorisierte Informationsgewinnung, Verlust der Vertraulichkeit) und aktiven Angriffen (unautorisierte Modifikation von Daten, Verlust der Integrität oder Verfügbarkeit).[33] Gemäss Bundesrat ist ein Cybervorfall ein «unbeabsichtigtes oder von Unbefugten beabsichtigtes Ereignis, das dazu führt, dass die Vertraulichkeit, Integrität, Verfügbarkeit oder Nachvollziehbarkeit von Daten beeinträchtigt ist oder es zu Funktionsstörungen kommen kann» (Art. 3 lit. v CyRV). Ein Cybervorfall hat somit negative Auswirkungen auf die Cybersicherheit und/oder die Cyber-Resilienz.

In der Praxis wird zwischen «threat agents» (Bedrohungsakteuren), «threat tools» (Bedrohungsinstrumenten) und «threat types» (Bedrohungstypen) differenziert.[34] Eine solche Kategorisierung ist zwar für bestimmte rechtliche Qualifikationen nützlich, aber sie zielt nicht darauf ab, ein umfassendes Bild von der sehr komplexen Natur und den Merkmalen von Cyberbedrohungen zu zeichnen, da sie insbesondere das Ausmass vernachlässigt, in dem sich die Kategorien überschneiden und miteinander verwobene Auswirkungen haben.[35]

Die Cybersicherheit wird durch eine Vielzahl externer und interner Akteure bedroht. Zu den Bedrohungsakteuren gehören Nationalstaaten, profitorientierte Cyberkriminelle, kriminelle Organisationen, Hacker (Black, Grey oder White Hat), Extremisten und Insider; ein Akteur kann zu mehr als einer Kategorie gehören.[36]

Die Bedrohungsakteure haben sehr unterschiedliche Motivationen: Sie handeln aus politischen Gründen (z.B. um Ziele zu zerstören, Cyberspionage zu betreiben oder politisch zu protestieren); sie können aber auch finanzielle (z.B. Diebstahl wertvoller persönlicher oder finanzieller Daten) oder soziokulturelle Motive (z.B. Angriffe mit philosophischen Zielen oder aus Gründen der Öffentlichkeit, der Neugier oder des Egos) haben.[37]

Bedrohungsakteure setzen in der Regel ähnliche Bedrohungswerkzeuge ein. Zu den grundlegenden Werkzeugen für Sicherheitsverletzungen gehören Mal-

33 *PwC Schweiz*, 2019, 5, 29 und 67.

34 *Weber/Studer*, 2016, 717 f.

35 *Weber*, 2020, 282.

36 *Weber/Studer*, 2016, 717.

37 *Weber*, 2020, 282.

ware und ihre Varianten (Ransomware, Viren, Würmer, Trojanische Pferde usw.) sowie Botnetze. Malware ist eine allgemeine Kategorie, die sich auf jeden Code oder jede Software bezieht, die heimlich und ohne Genehmigung auf einem Gerät installiert wird. Botnetze bestehen in der Regel aus Befehls- und Kontrollservern sowie Netzwerken von Computern, die mit Malware infiziert sind und aus der Ferne verwaltet werden können. Bislang ist Malware die grösste Cyberbedrohung.[38]

Weiter gehören die Veränderung oder der Missbrauch von Informationen, die Zerstörung von Informationen, der unbefugte Zugriff, die Verletzung von Daten, der Datendiebstahl und die «distributed denial-of-service» (Nichtverfügbarkeit eines Dienstes, der eigentlich verfügbar sein sollte) zu den Bedrohungen der Cybersicherheit. Obwohl alle Facetten vom oben genannten CIA-Dreiklangs durch Cyberangriffe bedroht sind, hat McAfee Labs vorausgesagt, dass die Bedrohung der Integrität von Systemen und Daten einen sehr wichtigen neuen Angriffsvektor darstellt, da die heimliche Veränderung bestimmter Elemente innerhalb von Transaktionen, Kommunikationen oder Daten betroffen ist.[39]

B. IT-Sicherheit als Rahmenordnung

Die Themen der Cybersicherheit und Cyber-Resilienz fallen in den weiteren Bereich der IT-Sicherheit und damit auch der (unternehmerischen) IT-Governance. Diese Rahmenordnung wird nachfolgend kurz dargestellt, weil sie die Grundlage für die Diskussion der spezifischen Handlungsempfehlungen im Kontext der Cybersicherheit und der Cyber-Resilienz darstellt.

1. Begriff und Wesen der IT-Sicherheit

Die IT-Sicherheit ist als Zustand zu verstehen, der die Risiken von Bedrohungen und Schwachstellen bei der Einsetzung von Informationstechnik durch angemessene Massnahmen auf ein tragbares Mass reduziert.[40]

---

38 *Weber*, 2020, 282 f.

39 *Weber*, 2020, 283; *McAfee Labs*, 2016, 34.

40 *Bundesamt für Sicherheit in der Informationstechnik* (BSI), Glossar, IT-Sicherheit, aufrufbar unter <https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Glossar-der-Cyber-Sicherheit/Functions/glossar.html?nn=522504&cms_lv2=132764>.

Gemäss § 2 Abs. 2 des deutschen Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik (BSIG) bedeutet Sicherheit in der Informationstechnik «die Einhaltung bestimmter Sicherheitsstandards, die die Verfügbarkeit, Integrität oder Vertraulichkeit von Informationen betreffen, durch Sicherheitsvorkehrungen in informationstechnischen Systemen, Komponenten oder Prozessen oder bei der Anwendung von informationstechnischen Systemen, Komponenten oder Prozessen».

Nachfolgend wird der Begriff der IT-Sicherheit unabhängig von der Berücksichtigung allfälliger Sicherheitsstandards verwendet, und zwar als Zustand, der vorliegt, wenn alle technischen, personellen und organisatorischen Massnahmen zum Schutze der Verfügbarkeit, Vertraulichkeit und Integrität der Systeme, Ressourcen sowie der gespeicherten oder elektronisch bearbeiteten Informationen umgesetzt sind.[41]

a) Grundanforderungen der IT-Sicherheit

Aus den vorerwähnten Umschreibungen ist ersichtlich, dass es im Bereich der Informationstechnologie drei Grundanforderungen gibt, die als notwendige Eigenschaften von technisch sicheren IT-Systemen gelten und die konstituierenden Begriffe der IT-Sicherheit bilden.[42]

aa) Verfügbarkeit

Unter Verfügbarkeit ist die uneingeschränkte Funktionalität eines Systems zu verstehen; die Verfügbarkeit gewährleistet, dass die Systeme, Daten oder Informationen zu einem bestimmten Zeitpunkt, an einem bestimmten Ort nutzbar sind.[43] In der Definition der Verfügbarkeit ist auch die maximal zulässige Ausfalldauer der Schutzobjekte festzuhalten; sie gibt Aufschluss über die Abhängigkeit des Benutzers vom Schutzobjekt. Ferner haben sich die Verfügbarkeitskontrollen auf Menschen, Prozesse und Systeme zu beziehen.[44]

bb) Vertraulichkeit

Im Rahmen der Vertraulichkeit eines IT-Systems sind alle enthaltenen Informationen vor unbefugter Kenntnisnahme zu schützen, d.h. nur denjenigen

41 *Weber/Willi*, 2006, 6.

42 *Weber/Willi*, 2006, 12; vgl. auch *Dierstein*, 2004, 347.

43 *Weber/Willi*, 2006, 6; vgl. auch *Warsinkse et al.*, 2019, 4.

44 *Weber/Willi*, 2006, 6 f.; *Warsinkse et al.*, 2019, 4.

Personen, die ein Recht auf Zugang zu diesen Informationen haben, dürfen diese Informationen zur Verfügung gestellt werden; Vertraulichkeit bedeutet also, dass der Zugang beschränkt ist. Um eine adäquate Vertraulichkeit der Informationen gewährleisten zu können, braucht es Kontrollen, welche die befugten Personen von den nicht befugten Personen trennen. Zu den vertraulichen Schutzobjekten gehören neben Nachrichteninhalten auch Informationen über Übermittlungsvorgänge und weitere interne Daten.[45]

cc) Integrität

Die Integrität lässt sich als Schutz vor unbefugter Modifikation der IT-Systeme und vor unberechtigter bzw. unbeabsichtigter Veränderung der Informationen umschreiben. Die Integrität ist gewährleistet, wenn berechtigte Subjekte (z.B. Personen, Funktionen oder Systeme) das spezifische Objekt (z.B. Systeme, Funktionen oder Datenbestände) zu berechtigten Zwecken nachvollziehbar bearbeiten.[46] Die Integrität sagt aber nichts über den Wahrheitsgehalt der Daten und Informationen aus; dies ist Gegenstand der Authentizität.[47]

Die Erstellung, Übertragung, Darstellung und Speicherung der Informationen sind zu kontrollieren, um sicherzustellen, dass die Informationen nicht in unangemessener Weise verändert wurden. Ausdruck einer höheren IT-Sicherheit ist die Fähigkeit, unangemessene Änderungen der Datenbestände, Informationen, Systeme oder Funktionen zu erkennen.[48]

b) Massnahmen zur Erreichung der Schutzziele

Ziel der Sicherheitsprozesse ist die Schadensverhinderung und die Risikominderung; als Ausgangspunkt dieser Prozesse dienen verschiedene Schutzziele. Im Rahmen der Sicherung der IT-Systeme werden die Vertraulichkeit, die Integrität, die Anonymität, die Authentizität, die Autorisierung, die Vertrauenswürdigkeit sowie die Nichtbestreitbarkeit (Gewährleistung der Zure-

45 *Warsinkse et al.*, 2019, 3; *Weber/Willi*, 2006, 7.

46 *Weber/Willi*, 2006, 7.

47 Die Authentizität ist der Schutz vor gefälschter Identität des Benutzers oder Systeme; sie stellt sicher, dass die Informationen tatsächlich aus der angegebenen Quelle stammen und wahrheitsgetreu sind (*Weber/Willi*, 2006, 7 f.).

48 *Warsinkse et al.*, 2019, 4.

chenbarkeit) als Schutzziele betrachtet. Diese Schutzziele gilt es mit verschiedenen Massnahmen, die präventiv, detektiv oder reaktiv wirken, zu erreichen.[49]

aa) Präventive Massnahmen

Die präventiven Massnahmen beinhalten ein vorausschauendes Sicherheitsmanagement, das einen Eintritt von potenziellen zukünftigen Sicherheitsereignissen verhindern soll. Sie wirken proaktiv, indem sie an vorangehende Bedrohungen und Ereignisse anknüpfen und darauf basierend Sicherheitsanforderungen erlassen. Rechtlich kann die Unterlassung präventiver Massnahmen im Rahmen der IT-Sicherheit ein Verschulden bzw. eine Pflichtverletzung zur Folge haben.[50]

Mögliche technische Massnahmen sind die Implementierung eines Firewalls (erlaubt einen spezifischen Verkehr im Netzwerk), die Berechtigungsverwaltung (Sicherstellung, dass nur befugte Zugriffe oder Zutritte erfolgen durch Autorisierung und Authentifikation der Benutzer), die Datenverschlüsselung (kryptografische Massnahmen, welche die Informationen verschlüsseln und die Vertraulichkeit der übertragenen und gespeicherten Daten gewährleisten), die Anonymisierung (Löschung von Informationen des Absenders bzw. Verunmöglichen von Rückschlüssen über den Absender) sowie die Verifikation von Systemkomponenten (Überprüfung auf Wirksamkeit der Komponenten vor dem Einsatz bzw. Überprüfung auf Vertrauenswürdigkeit der Komponenten).[51]

Überdies sind als präventive administrative Massnahmen die Verantwortlichkeiten und Vorgehensweisen zu definieren, um mit klaren Prozessen die zu erreichenden Sicherheitsziele zu kommunizieren und adäquate Schutzmassnahmen zu implementieren. Zudem sind die Massnahmen zu dokumentieren und mit dem aktuellen Stand der Realisierung zu beschreiben. Dieses Vorgehen soll einerseits das Sicherheitsniveau überprüfen helfen und andererseits auch zur Weiterentwicklung der Sicherheitsprozesse beitragen. Ausserdem sind aufgrund der zunehmenden Vernetzung auch die Abhängigkeiten von externen Dienstleistern (insb. beim Outsourcing) in die unternehmenseigenen Sicher-

49 *Weber/Willi*, 2006, 18 und 30 f.

50 *Weber/Willi*, 2006, 31.

51 *Weber/Willi*, 2006, 31 f.

heitsstandards einzubeziehen. Die Einbindung dieser externen Dienstleister stellt sicher, dass das Unternehmen sein eigenes Sicherheitsniveau hochhalten kann.[52]

Ferner gibt es auch präventive personelle Massnahmen; dazu gehören insbesondere spezifische fachliche und persönliche Anforderungen an die Mitarbeitenden. Aus diesem Grund sind die Mitarbeitenden regelmässig aus- und weiterzubilden sowie ist die Fortführung ihrer Aufgaben bei Abwesenheit zu regeln. Die personellen Massnahmen haben darüber hinaus zum Ziel, eine Sicherheitskultur und ein Sicherheitsbewusstsein bei den Mitarbeitenden zu schaffen, welche zur Erreichung der entsprechenden Sicherheitsvorschriften beitragen soll.[53]

bb) Detektive Massnahmen

Die detektiven Massnahmen werden erst bei einem Schadenseintritt relevant; sie ergänzen den präventiven Schutz. In diesem Zusammenhang sind insbesondere die Entdeckung der Gefahren für das System sowie die Einleitung geeigneter Massnahmen von grosser Bedeutung.[54]

Mögliche technische Massnahmen sind die automatische Angriffserkennung (Überwachung des Netzverkehrs mit einem Alarmsystem), Firewalls (Erkennung von Viren, Trojaner etc. durch Filterung der Kommunikation zwischen gesicherten und ungesicherten Netzen) und die Installation von Audit Trails (Dokumentation und Nachvollziehbarkeit von Informationsflüssen). Ferner können personelle Massnahmen, also Überwachungsmassnahmen im weitesten Sinne, eine IT-Sicherheit mit detektiver Wirkung gewährleisten; hierzu gehören das Vier-Augen-Prinzip, die Regelung der Nutzungsberechtigung und Job-Rotation-Modelle.[55]

---

52 *Weber/Willi*, 2006, 33; vgl. auch hinten Kap. IV.B.4, IV.C.3.a) und IV.C.7.

53 *Weber/Willi*, 2006, 33 f.

54 *Weber/Willi*, 2006, 34; vgl. auch hinten Kap. IV.B.3, IV.B.5, IV.C.3 und IV.C.6.

55 *Weber/Willi*, 2006, 35.

cc) Reaktive Massnahmen

Reaktive Massnahmen greifen, wenn ein Ereignis bereits eingetreten und ein Schaden entstanden ist. Der Schaden kann im Rahmen des akzeptierten Risikos, eines nicht identifizierten Risikos oder aufgrund des Versagens der installierten Sicherheitssysteme eintreten.[56]

Zu den reaktiven Massnahmen gehören Intrusion-Prevention-Systeme und reaktive Firewalls. Sie regeln den Informationsfluss und sind allenfalls in der Lage, kritische Datenpakete abzuweisen. Darüber hinaus können technische Massnahmen zur Wiederherstellung der Daten und Systeme implementiert werden, um im Falle eines Datenverlusts oder einer Datenmanipulation den Schaden zu begrenzen. Als reaktive, administrative Massnahme ist zudem die Erstellung eines Notfallplans von grosser Bedeutung, damit das Vorgehen in ausserordentlichen Situationen geregelt ist (Festlegung von Funktionen und Zuständigkeiten sowie Ablaufplanung und Schaffung von Redundanzen).[57]

2. Funktionen, Policy und Richtlinien der IT-Sicherheit

a) Funktionen der IT-Sicherheit

Die IT-Sicherheit ist gemäss eingangs erwähnter Umschreibung ein Zustand, den es zu erreichen gilt; sie enthält keine Aussage zum Sicherheitsmass.[58] Mit einer funktionalen Betrachtung lässt sich das Sicherheitsmass konkretisieren, da grundsätzlich die Gewährleistungsfunktion, die Schutzfunktion sowie die Wertschöpfungsfunktion zu beachten sind. Überblicksartig geht es insbesondere um die folgenden Funktionen:[59]

Gewährleistungsfunktion:

- Verfügbarkeit der Infrastruktur
- Regulatorisches Umfeld
- Interdependenzen
- Disaster Recovery

---

56 *Ibid.*

57 *Weber/Willi*, 2006, 36; vgl. auch hinten Kap. IV.B.7, IV.C.3, IV.C.5.

58 Vgl. Definition der IT-Sicherheit in Kap. II.B.1.

59 *Weber*, 2017a, 39 f.; *Weber/Willi*, 2006, 180 ff.

Schutzfunktion:

- Schutz des Informationsflusses
- Qualität der Informationen
- Daten- und Informationssicherungspflichten

Wertschöpfungsfunktion:

- Strategische Planung
- Ausrichtung auf die Geschäftsaktivitäten
- Vertrauensbildung
- Wettbewerbsfähigkeit

Diese Funktionen sind sachgerecht in die IT-Management-Umgebung des betroffenen Unternehmens einzubetten.

b) IT-Sicherheits-Policy

Darüber hinaus ist auch die IT-Sicherheits-Policy von Bedeutung. Zur IT-Sicherheits-Policy gehören grundsätzlich keine technischen Formulierungen oder Anforderungen; sie macht bloss allgemeine und grundlegende Vorgaben zu den Sicherheitszielen, die im Rahmen des Schutzkonzepts auf technischer Ebene umzusetzen sind. Mit der Sicherheits-Policy wird auch die Zuweisung der Funktionen und Zuständigkeiten geregelt. Die Sicherheitsgrundsätze, die in der Sicherheits-Policy geregelt werden, enthalten Aussagen zu folgenden Themen:[60]

- Festlegung der Zuständigkeiten;
- Kontinuität der Geschäftsabläufe;
- Verfügbarkeit der Systeme;
- Integrität der Daten und Informationen.

c) Richtlinien der IT-Sicherheit

Die IT-Sicherheitsrichtlinien betreffen die Sicherheitsmassnahmen, die auf die identifizierten Risiken anwendbar sind. Die Richtlinien beziehen sich konkret jeweils auf den bestimmten Einsatzgebiet, weshalb spezifische Richtlinien für

[60] Vgl. auch *Weber/Willi*, 2006, 188 f. mit einer grösseren Liste; vgl. ferner *Weber*, 2017a, 40.

beispielsweise Datensicherung, Nutzung von Endgeräten (insb. mobile Endgeräte), Notfallmanagement, Umgang mit klassifizierten Dokumenten existieren.[61]

Besonders wichtig ist, sicherzustellen, dass die Richtlinien effektiv umgesetzt werden. Aus diesem Grund müssen die Richtlinien verbindlichen Charakter haben und mit Instrumenten ausgestattet sein, welche die Aufsicht und Durchsetzung der Massnahmen erlauben.[62]

3. Akteure im Bereich der IT-Sicherheit

Im Bereich der IT-Sicherheit gibt es verschiedenste (praktisch wichtige) Akteure, die nachfolgend kurz zu erwähnen sind:

- Information Systems Security Association (ISSA): Als Non-Profit-Organisation widmet sich die ISSA der Aus- und Weiterbildung im Bereich der IT-Sicherheit und fördert Managementpraktiken, welche die Vertraulichkeit, Integrität und Verfügbarkeit von Informationsressourcen gewährleisten.[63]
- Institute of Electrical and Electronics Engineers (IEEE): Die IEEE ist ein weltweiter Berufsverband von Ingenieuren, Wissenschaftlern und verwandten Berufsgruppen mit technischen Interessen in den Bereichen Elektro- und Computerwissenschaften, Ingenieurwesen und verwandten Disziplinen. Die IEEE gibt verschiedene Standards im Bereich der Telekommunikation, der Informationstechnologie und der Energieerzeugung heraus und veröffentlicht fast einen Drittel der weltweiten Fachliteratur in den Bereichen Elektrotechnik, Informatik und Elektronik.[64]
- Forum of Incident Response and Security Teams (FIRST): FIRST ist ein Zusammenschluss verschiedener Computer Emergency Response Teams (CERT), darunter insbesondere Teams für die Produktsicherheit aus dem staatlichen, kommerziellen und akademischen Sektor. Sie dient als Aus-

61 *Weber/Willi*, 2006, 192 f.

62 *Weber/Willi*, 2006, 193.

63 ISSA, Developing and Connecting Cybersecurity Leaders Globally, aufrufbar unter <https://www.issa.org/about-issa/>.

64 IEEE, IEEE at a Glance, aufrufbar unter <https://www.ieee.org/about/at-a-glance.html>.

tauschplattform dieser Teams und will als Plattform einzelne Mittel und Werkzeuge bereitstellen, die eine effiziente Zusammenarbeit ermöglichen.[65]

- Information Systems Audit and Control Association (ISACA): Als unabhängige internationale Verbindung von IT-Fachleuten bietet die ISACA die international anerkannten Leistungsausweise des Certified Information Security Manager (CISM) und des Certified Information Systems Auditor (CISA) an.[66]
- Agentur der Europäischen Union für Cybersicherheit (ENISA): ENISA setzt sich als Agentur der Europäischen Union für ein hohes gemeinsames Niveau der Cybersicherheit in Europa ein, deren Ziele, Aufgaben und organisatorischen Aspekte im Rechtsakt zur Cybersicherheit[67] geregelt sind.[68]
- International Organisation for Standardisation (ISO): Die ISO ist eine unabhängige, nichtstaatliche internationale Organisation, die internationale Standards in verschiedensten technologischen Bereichen ausgearbeitet und veröffentlicht hat.[69]
- International Electrotechnical Commission (IEC): Die IEC ist eine globale Non-Profit-Organisation; sie publiziert internationale Standards im Bereich der Elektrotechnik und Elektronik.[70] Für die Cybersicherheit ist die ISO/IEC 27000-Reihe von grosser Bedeutung.

---

65 FIRST, About FIRST, aufrufbar unter <https://www.first.org/about/>.

66 ISACA, Credentialing, aufrufbar unter <https://www.isaca.org/credentialing>.

67 Verordnung (EU) 2019/881 des Europäischen Parlaments und des Rates vom 17. April 2019 über die ENISA (Agentur der Europäischen Union für Cybersicherheit) und über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik und zur Aufhebung der Verordnung (EU) Nr. 526/2013 (Rechtsakt zur Cybersicherheit) (Text von Bedeutung für den EWR), ABl. L 151 vom 7.6.2019, 15–69.

68 ENISA, About ENISA - The European Union Agency for Cybersecurity, aufrufbar unter <https://www.enisa.europa.eu/about-enisa>; vgl. ferner Kap. III.D.3.b).

69 ISO, About Us, aufrufbar unter <https://www.iso.org/about-us.html>; ISO, Standards, aufrufbar unter <https://www.iso.org/standards.html>.

70 IEC, About us, aufrufbar unter <https://iec.ch/about-us>; IEC, What we do, aufrufbar unter <https://iec.ch/what-we-do>.

- National Institute of Standards and Technology (NIST): Das NIST ist eine Standardisierungsbehörde in den USA, welche mit dem NIST Framework für Cybersicherheit auch im internationalen Kontext eine wichtige Position für die IT-Sicherheit einnimmt.[71]
- Nationales Zentrum für Cybersicherheit (NCSC): Als Kompetenzzentrum des Bundes für Cybersicherheit ist das NCSC erste Anlaufstelle für die Wirtschaft, Verwaltung, Bildungseinrichtungen und die Bevölkerung bei Cyberfragen. Das NCSC ist zuständig für die koordinierte Umsetzung der Nationalen Strategie zum Schutz der Schweiz vor Cyber-Risiken.[72]
- Bundesamt für wirtschaftliche Landesversorgung (BWL): Das BWL ist für die wirtschaftliche Landesversorgung zuständig; in den Bereichen, in denen das Funktionieren kritischer Infrastrukturen betroffen ist, besteht eine staatliche Verantwortung. Das BWL drückt mit den IKT-Minimalstandards[73] diese Schutzverantwortung des Staates gegenüber den Bürgern aus.[74]

C. Vorkehren zur Sicherstellung der Cybersicherheit und Cyber-Resilienz

Um die Systeme und Daten vor Cybervorfällen zu schützen, braucht es strategische Leitlinien für die Sicherstellung der Cybersicherheit. Je nach Rahmenbedingungen sind unterschiedliche Grundsätze umzusetzen; als mögliche Kategorisierung lässt sich eine Aufteilung wie folgt vornehmen:

1. Leitlinien für Massnahmen vor einem Cybervorfall

Präventiv bedarf es derjenigen Vorgaben («*Governance*»), welche Zuständigkeiten regeln, überwachen und sicherstellen, die dazu beitragen, dass die rechtlichen, regulatorischen und organisatorischen Anforderungen des Geschäftsumfelds eingehalten werden. Bei der Erarbeitung der Grundsätze bzw.

71 NIST, Cybersecurity Framework, aufrufbar unter <https://www.nist.gov/cyberframework>; vgl. auch Kap. II.C.

72 NCSC, Über NCSC, aufrufbar unter <https://www.ncsc.admin.ch/ncsc/de/home/ueber-ncsc/das-ncsc.html>.

73 BWL, 2018. Bundesamt für wirtschaftliche Landesversorgung BWL, Minimalstandard zur Verbesserung der IKT-Resilienz, Bern 2018.

74 BWL, 2018, 2.

Leitlinien sind sowohl nationale als auch internationale sowie sektorspezifische Standards zu beachten.[75] Die «Cyberwelt» umfasst aber mehr als bloss die Informations- und Kommunikationstechnik;[76] bei der Governance sind auch die Menschen und Prozesse miteinzubeziehen.[77]

Die Organisationen müssen in der Lage sein, ihr Geschäftsumfeld korrekt zu *analysieren*. Zur Grundlage der Verantwortlichkeitszuweisung sind die Ziele, Aufgaben und Aktivitäten zu priorisieren und bewerten;[78] hierfür muss das Unternehmen seine Funktion im Geschäftsumfeld und die betriebsnotwendigen Prozesse ermitteln.[79] Im Rahmen der Risikoanalyse sind interne und externe Cyberbedrohungen und deren Auswirkungen auf die Geschäftstätigkeit, auf Betriebsmittel und Individuen sowie auf Reputationsrisiken zu analysieren.[80]

Die Systeme müssen zudem fähig sein, verschiedenste Faktoren und Risiken im Unternehmen zu *identifizieren*.[81] Hierzu gehören einerseits die Umschreibung, Kategorisierung und Bewertung des Inventar Management («Asset Management»), also der Daten, Personen, Geräte, Systeme und Anlagen der Organisation. Andererseits ist eine Risikoeinschätzung erforderlich, welche das Inventar nach seiner Kritikalität klassifiziert.[82]

Neben der Identifikation ist der *Schutz* an sich ein wichtiger Faktor. Die Schutzmassnahmen sollten grundsätzlich proportional zur systemischen Rolle der Unternehmen im jeweiligen Sektor ausgestaltet sein. Der physische und datenbasierte Zugriff auf IKT-Betriebsmittel und IKT-Anlagen darf nur für autorisierte Personen (z.B. Berechtigungsstufen mit Trennung nach Funktion), Prozesse sowie Geräte erlaubt sein; dieser Zugriff ist zudem auf zulässige Aktivitäten zu beschränken.[83] Zum Schutz gehört auch eine angemessene Ausbil-

75 FSB, 2020, 3 f.; G7 *Cyber Expert Group*, 2016, 1.

76 Vgl. im Detail Kap. II.A.1 und II.C.

77 Vgl. im Detail Kap. IV.

78 NIST, 2018, 25 f.; BWL, 2018, 16.

79 ACSC, 2021, 1; BIS/IOSCO, 2016, 11.

80 NIST, 2018, 26 f.; BWL, 2018, 18 f.

81 ACSC, 2021, 1; *Resilient*, 2020, 15; NIST, 2018, 6 f.; BWL, 2018, 15; BIS/IOSCO, 2016, 11; G7 *Cyber Expert Group*, 2016, 2.

82 NIST, 2018, 24; BWL, 2018, 15; BIS/IOSCO, 2016, 11.

83 ACSC, 2021, 1 f.; NIST, 2018, 29 f.; BWL, 2018, 21; BIS/IOSCO, 2016, 12 f.; G7 *Cyber Expert Group*, 2016, 2.

dung und Sensibilisierung der Mitarbeitenden und der externen Partner; den Führungskräften kommt dabei eine besondere Rolle mit mehr Verantwortung zu.[84]

Die Cybersicherheit muss überdies auf den Grundprinzipien der Datensicherheit[85] aufbauen, d.h. der Schutz hat der Vertraulichkeit, Integrität und Verfügbarkeit der Daten und Datenträger – nach dem Massstab der Risikostrategie – zu dienen.[86] Dieses Ziel lässt sich u.a. durch den Einsatz von Schutztechnologien (technische Security-Lösungen) anstreben;[87] um ein angemessenes Schutzniveau zu erreichen, sind zudem regelmässige Unterhalts- und Reparaturarbeiten an den IKT-Systemen unvermeidbar.[88] Solche Schutzmassnahmen helfen, die Auswirkungen eines möglichen Cyberangriffs auf identifizierte, kritische Geschäftsfunktionen, Informationswerte und Daten zu minimieren.

Auch die besten Identifikations- und Schutzeinrichtungen sind nicht zu 100% sicher; deshalb ist es wichtig, mögliche Gefahren im Voraus *erkennen* zu können.[89] Von Bedeutung ist also, dass Sicherheitsvorkehren anomales Verhalten frühzeitig entdecken und dessen potenzielle Auswirkungen verstehen; hierfür sind die Cybervorfälle nach ihren Zielen und Methoden zu analysieren.[90] Dies ist nur möglich, wenn die IKT-Systeme und die Effektivität der Schutzmassnahmen auf allen Stufen regelmässig überprüft und die Handlungsanweisungen zur Erkennung von Cybervorfällen eingehalten werden.[91]

2. Leitlinien für Massnahmen nach einem Cybervorfall

Ist ein Cybervorfall eingetreten, erweist sich eine angemessene *Reaktion* als erforderlich.[92] Jedes Unternehmen braucht einen Reaktionsplan, welcher nach einem Cybervorfall auszuführen ist, da in der Realität nicht alle Gefahren frühzeitig erkennbar und damit auch vermeidbar sind.[93]

---

84 ACSC, 2021, 2; NIST, 2018, 31 f.; BWL, 2018, 22.

85 Für eine detailliertere Auseinandersetzung mit dem DSG vgl. Kap. III.B.2.b).

86 NIST, 2018, 32 f.; BWL, 2018, 23.

87 NIST, 2018, 36 f.; BWL, 2018, 26.

88 NIST, 2018, 36; BWL, 2018, 25.

89 ACSC, 2021, 2; *Resilient*, 2020, 15.

90 NIST, 2018, 37 f.; BWL, 2018, 27.

91 NIST, 2018, 38 ff.; BWL, 2018, 28 f.

92 ACSC, 2021, 2; *Resilient*, 2020, 15.

93 *Resilient*, 2020, 18 f.; NIST, 2018, 41; BWL, 2018, 30; BIS/IOSCO, 2016, 16.

Das Ziel der Reaktion muss darin bestehen, die weitere Ausbreitung eines Cybervorfalls zu verhindern und den Schaden zu verringern; hierfür haben die Schutzeinrichtungen in der Lage zu sein, Gefahren einzugrenzen und ihre weitere Ausbreitung zu unterbrechen.[94] Die Sicherheit ist nur gewährleistet, wenn die Unternehmen regelmässige Analysen durchführen, welche auf adäquate Handlungsmöglichkeiten geprüft und stetig verbessert werden; mithilfe der weitreichenden (und bestmöglichen internationalen) Kommunikation sollen die Unternehmen aus vorangegangenen Vorfällen lernen.[95]

Ein anderer Teilaspekt der Reaktion ist die Fähigkeit, die Systeme funktionswürdig *wiederherzustellen*;[96] die Wiederaufnahme der betrieblichen Operationen innerhalb kürzester Zeit muss dabei das Ziel sein.[97] Jedoch sollten z.B. Finanzdienstleister auch für diejenigen Fälle planen, in denen die IKT-Systeme nicht bereits nach zwei Stunden wiederhergestellt sind. Zeichnet sich ein längerer Ausfall der Systeme ab, brauchen Finanzdienstleister einen Plan mit Priorisierungen (z.B. Prozessieren von kritischen Transaktionen), während die Wiederherstellungsversuche fortlaufen.[98] Auch bei der Wiederherstellung der Systeme ist den Unternehmen zu empfehlen, sich stets mit internen und externen Partnern auszutauschen.[99]

Eine gut funktionierende, interne und externe Kommunikation mit allfälligen Ansprechgruppen (z.B. externe IT-Unternehmen, Behörden, Systemintegratoren, Internet Service Providern) kann die möglichen Folgen eines Cybervorfalls stark eindämmen; deshalb ist gegebenenfalls eine Meldestelle für Cybervorfälle einzurichten und auch die grenzüberschreitende Kommunikation zu fördern.[100] Die Kommunikation ist aber nur hilfreich, wenn alle relevanten Stellen rechtzeitig auf den neuesten Stand gebracht werden.[101]

---

94 FSB, 2020, 10; *Resilient*, 2020, 19 ff.; NIST, 2018, 42 f.; BWL, 2018, 33.

95 NIST, 2018, 42 f.; BWL, 2018, 32 und 34.

96 ACSC, 2021, 2; FSB, 2020, 10 f.; NIST, 2018, 43 f.; BWL, 2018, 35 f.

97 Die BIS und IOSCO erwähnen in ihren Guidelines explizit, dass Finanzmarktinfrastrukturen innerhalb von zwei Stunden in der Lage sein müssen, die betrieblichen Operationen wieder aufzunehmen (sog. resumption within two hours bzw. two-hour RTO oder 2hRTO; vgl. BIS/IOSCO, 2016, 2).

98 BIS/IOSCO, 2016, 16.

99 NIST, 2018, 44; BWL, 2018, 36.

100 ACSC, 2021, 2; FSB, 2020, 13 f.; NIST, 2018, 41; BWL, 2018, 31; BIS/IOSCO, 2016, 17; G7 *Cyber Expert Group*, 2016, 3.

101 FSB, 2020, 14.

3. Cybersicherheit und Cyber-Resilienz als fortlaufender Lernprozess

Die Gewährleistung der Cybersicherheit und der Cyber-Resilienz beschränkt sich jedoch nicht nur auf den Schutz vor bekannten Gefahren. Die Unternehmen müssen auch ein *Lagebewusstsein* haben und einen *fortlaufenden Lernprozess* etablieren.[102] Hierfür bedarf es des Zugriffs auf Informationen bzgl. möglicher Gefahren, um entsprechende Schutzvorkehren bereitzustellen; die Informationen sind in branchen-, regierungs- und grenzübergreifenden Gruppen zu sammeln, zu verteilen und zu bewerten.[103]

Gestützt auf solche Informationen haben die Unternehmen die Möglichkeit, aus den Cybervorfällen fortlaufend zu lernen und die Cyber-Resilienz zu verbessern. Wichtig ist, dass die Akteure die technischen Entwicklungen aktiv überwachen, um effiziente Gegenmassnahmen einführen zu können. Neben neuen Reaktionsmöglichkeiten sind auch die vorausschauenden Fähigkeiten zu verbessern und ein proaktiver Schutz vor zukünftigen Cybervorfällen zu etablieren.[104]

4. Weitere Vorkehren zur Sicherstellung der Cybersicherheit

Die Cybersicherheit dient grundsätzlich dem Schutz der notwendigen kritischen Betriebsmittel. Damit die Unternehmen einen angemessenen Schutz erlangen können, ist eine Strategie mit einem mehrschichtigen Ansatz, international bekannt als Defense-In-Depth-Strategie, erforderlich. Auch das Bundesamt für wirtschaftliche Landesversorgung (BWL) befasst sich mit der Defense-In-Depth-Strategie und hebt verschiedene Elemente dieser Strategie hervor.[105]

Demnach gehört zur Defense-In-Depth-Strategie eine Cybersicherheits-Architektur, die mit den Vorgaben des NIST Framework im Einklang steht, d.h. die Vertraulichkeit, Verfügbarkeit und Integrität der Daten sowie die Systeme sind zu schützen. Zusätzlich zu diesem informationsbezogenen Schutz ist auch die physische Sicherheit, die insbesondere den physischen Zugang sowie

---

102 ACSC, 2021, 2; BIS/IOSCO, 2016, 22; G7 *Cyber Expert Group*, 2016, 3.

103 BIS/IOSCO, 2016, 20 f.

104 BIS/IOSCO, 2016, 22.

105 BWL, 2018, 8.

die physischen Veränderungen oder Manipulationen der Systeme (z.B. durch Einführung unerlaubter Geräte, wie z.B. einem USB-Stick) und Infrastrukturen betrifft, von Bedeutung.[106]

Ähnlich wie der physische Schutz ist auch der Faktor «Mensch» nicht zu unterschätzen, da der Mensch in der Regel als «weakest link» angesehen wird.[107] Der Mensch ist in der Lage, die technischen Massnahmen durch mutwillige oder unbedarfte Fehlmanipulationen zu untergraben. Aus diesem Grund sind die Unternehmen gehalten, ihre Mitarbeitenden während der kompletten Anstellungsdauer zu schulen und weiterzubilden sowie angemessene Weisungen zu geben bzw. sachgerechte Richtlinien zu erlassen.[108]

Darüber hinaus können die Unternehmen mit der Business-Impact-Analyse ermitteln, welche Risiken tragbar sind und welche Auswirkungen ein Cybervorfall potenziell haben kann.[109] Die Unternehmen vermögen ausserdem mit einem Überwachungssystem Anzeichen eines Angriffs oder andere anomale Verhaltensweisen frühzeitig zu erkennen und ihre Assets vor unbefugten Zugriffen zu schützen. Hierfür sind u.a. gründliche und unabhängige Audits durchzuführen und die Informationsrisiken zu überwachen.[110]

D. Umfangreiche Rechtsquellen

Im Bereich der Cybersicherheit gibt es nationale (formelle) Gesetze sowie regionale bzw. internationale Regelungen (z.B. multilaterale Staatsverträge), die unter den Begriff des Hard Law fallen. Daneben sind aber auch branchenspezifische oder branchenübergreifende sowie themenorientierte Standards und Vorgaben zu berücksichtigen, die sich als Soft Law qualifizieren lassen und ebenfalls eine wichtige Rolle spielen.[111] Die nachfolgende detaillierte Analyse der Rechtsgrundlagen im In- und Ausland erläutert beide Arten von Rechtsquellen.

Gesetze werden normalerweise in einem formellen Verfahren durch die zuständige Behörde erlassen. Diese Rechtsquellen stellen ein stabiles Regelungssystem dar, sind jedoch mit dem Problem behaftet, dass sich technologische

106 BWL, 2018, 9 f.

107 *Bissell/Lasalle/Dal Cin*, 2019, 9; *Camillo*, 2017, 199; *Webley/Hardy*, 2015, 353.

108 BWL, 2018, 12.

109 Vgl. zur Business-Impact-Analyse Kap. IV.C.3.

110 BWL, 2018, 11 f.

111 Vgl. zu Soft Law in Finanzmärkten insb. Kap. III.F.

Fortschritte und gesellschaftliche Veränderungen oft nicht innert kurzer Zeit berücksichtigen lassen, weil die Gesetzgebungsverfahren meist recht langsam sind, insbesondere wenn es an ausreichendem Verhandlungsspielraum auf internationaler Ebene mangelt.[112]

Demgegenüber lehrt die Erfahrung, vor allem in den sich technologisch schnell entwickelnden Wirtschaftssektoren, dass Soft Law zunehmend eine wichtige «ersetzende» Rolle einnimmt; solche Bestimmungen werden in der Regel von den involvierten Akteuren erlassen und erfüllen oft nicht die Verfahrensformalitäten, die erforderlich sind, um ihnen den Rechtsstatus eines formellen Gesetzes zu verleihen.[113]

Die Entwicklungen auf den Finanzmärkten und noch mehr auf den Märkten der Informationstechnologien sowie des Internets zeigen, dass formelle Gesetze oft nicht besser geeignet sind als Soft Law, das soziale Umfeld zu regulieren.[114] Soft Law kann nämlich mehrere Funktionen erfüllen, die früher mit formellen Gesetzen verbunden waren, wie z.B. die Koordinierung der betroffenen Akteure;[115] es ist deshalb nicht überraschend, dass neben den formellen Gesetzen der jeweiligen Länder auch internationale Standards mit «Soft Law»-Charakter für die Cybersicherheit von grosser Bedeutung sind.

Die Selbstregulierung durch Soft Law bringt verschiedene Vorteile mit sich: Die von den Teilnehmern einer bestimmten Gemeinschaft geschaffenen Regeln sind grundsätzlich effizient, da sie auf reale Bedürfnisse reagieren, die Technologie widerspiegeln und die Möglichkeit bieten, den rechtlichen Rahmen flexibel an das sich verändernde Umfeld anzupassen. Da die Selbstregulierung von den beteiligten Stakeholdern ausgehandelt wird, ist die Wahrscheinlichkeit gross, dass solche Regeln auf breite Akzeptanz stossen.[116] Für die betroffenen Personen und Einrichtungen besteht zudem ein Anreiz, ständige Konsultationsprozesse für die Entwicklung und Umsetzung dieser privaten Regeln durchzuführen.[117]

Ein weiterer Vorteil von Soft Law besteht darin, dass sich die Regeln unabhängig vom Territorialitätsprinzip entwickeln und festlegen lassen, d.h. die Selbstregulierung hat zumindest im Prinzip eine globale Reichweite. Darüber hinaus

112 *Weber*, 2012, 10 ff.

113 *Weber*, 2014, 22 ff.

114 *Weber*, 2021e, 26.

115 *Weber*, 2021e, 26; vgl. ferner *Weber*, 2012, 11; *Guzman/Meyer*, 2010, 188 ff.

116 *Weber*, 2014, 27.

117 *Guzman/Meyer*, 2010, 179 ff.

handelt es sich bei Soft Law um eine normative Ordnung, die von den beteiligten Organisationen geschaffen wird und die auf Veränderungen im betreffenden Umfeld reagiert.[118]

Die Qualität des Soft Law ermöglicht es den Regulierungsbehörden, Vereinbarungen mit unterschiedlichem Umfang und unterschiedlicher Spezifität zu treffen und dann die Erwartungen der beteiligten Akteure zu klären (oder zu ändern).[119]

Die Erfahrung hat jedoch auch gezeigt, dass Soft Law in Form von Selbstregulierung nicht immer den gesamten Bereich eines gesellschaftlich erwünschten Rechtsrahmens abdeckt. Unter solchen Umständen kann der Selbstregulierungsansatz durch ein staatliches «Regime» unterstützt werden, insbesondere wenn ein Staat der Meinung ist, dass einige grundlegende Regeln nicht den privaten Akteuren überlassen werden sollten. In diesem Fall bezeichnet die Rechtslehre den «legislativen» Ansatz als eine Form der «Co-Regulierung».[120]

Aufgrund des Bedürfnisses, transnationale Lösungen zu finden, stützen die Länder ihre Gesetze und Richtlinien zutreffend oft auf internationale Standards und «best practices» ab; diese lassen sich nicht selten als Soft Law klassifizieren. Dadurch sind die Regelungen in den verschiedenen Ländern im Kern zumindest teilweise einheitlich. Indessen erweitern die verschiedenen Staaten die internationalen Standards nicht selten mit eigenen Richtlinien, um den Besonderheiten der einheimischen Interessen gerecht zu werden; dieser co-regulative Ansatz ist im Bereich der Cybersicherheit oft anzutreffen.[121]

118 *Weber*, 2021e, 28.

119 *Weber*, 2012, 12.

120 *Weber*, 2021e, 29.

121 Vgl. hierzu Kap. III.E.1.b)aa), III.E.2.c), III.E.3.c), III.E.4.c), III.E.5.a), III.E.6.b) und III.E.7.b), insb. III.E.7.b)bb).

III. Geltende Rechtsgrundlagen zur Cybersicherheit

Um die Grundsätze der Cybersicherheit und Cyber-Resilienz flächendeckend sicherstellen zu können, ist deren konkrete, rechtliche Umsetzung erforderlich. Verschiedene Länder und Organisationen haben hierfür unterschiedliche Ansätze gewählt. Ein Überblick (A.) dient als Einleitung in diese Thematik, bevor die Umsetzung der Grundsätze in der Schweiz (B.), in Liechtenstein (C.), in der Europäischen Union (D.), in weiteren Rechtsordnungen (E.) sowie in Normen mit Soft-Law-Charakter (F.) dargestellt wird. Schliesslich sind die Erkenntnisse der rechtsvergleichenden Analyse zusammenzufassen (G.).

A. Überblick

Rechtliche Regelungen versuchen, mit den Entwicklungen der «Cyberwelt» angemessen Schritt zu halten und die neusten technologischen Gegebenheiten normativ abzubilden. Nicht selten erachten die Staaten die Cyberregulierung als ein wichtiges, innerstaatliches Ziel; dennoch erweisen sich nationale Bestrebungen – insbesondere im Bereich eines weltweit verflochtenen Sektors wie dem Finanzmarkt – oft als nicht ausreichend.

1. Beschränktes internationales Regelwerk

Die zahlreichen Akteure im Finanzmarkt sind eng miteinander verknüpft und hängen – mindestens im Bereich Cybersicherheit – oft voneinander ab; konsequenterweise braucht es für transnationale Gefahren auch transnationale Lösungen. Schon seit Jahrzehnten versuchen internationale (und regionale) Organisationen, eine normative Ordnung zu entwickeln, welche die Regulierungsstandards in der Cybersicherheit harmonisiert.[122] Einige dieser Bemühungen waren auch erfolgreich, insbesondere bei der Umsetzung von Sicherheitsausnahmen («security exceptions») in multilateralen Abkommen sektorspezifischer internationaler Organisationen (z.B. ITU, WTO).[123]

---

122 Für einen Überblick, s. *Weber*, 2020, 284 ff.

123 Z.B. enthalten die ITU- und WTO-Agreements spezifische Sicherheitsregelungen (vgl. dazu *Weber*, 2020, 288–290.

Auf internationaler Ebene ist insbesondere die Bekämpfung der Cyberkriminalität ein wichtiges Thema; bereits fünf Expertengruppe der Vereinten Nationen (United Nations Group of Governmental Experts, UNGGE) haben sich ausgetauscht und Berichte veröffentlicht, ohne jedoch verbindliche Grundsätze festzulegen.[124] Die dritte Expertengruppe der Vereinten Nationen (UNGGE [2012/13]) sprach sich für die Anwendung der Charta der Vereinten Nationen auf den Cyberspace aus, der offen, sicher, friedlich und zugänglich bleiben soll;[125] die vierte Expertengruppe erstellte einen umfassenden Bericht über Normen, Regeln und Grundsätze für das verantwortungsvolle Verhalten von Staaten im Cyberspace sowie über die internationale Zusammenarbeit, vertrauensbildende Massnahmen und den Aufbau von erforderlichen Kapazitäten.[126] Auch die fünfte Expertengruppe hat es indessen (u.a. aufgrund politischer Spannungen) nicht geschafft, die allgemein anerkannten Grundsätze als detaillierte, für die Staaten umsetzbare Verpflichtungen festzulegen.[127]

Gemäss Auffassung der vierten Expertengruppe haben die Staaten mit angemessenen Massnahmen ihre kritischen Infrastrukturen vor Cybergefahren zu schützen, indem sie die UN-Resolution 58/199[128] und UN-Resolution 64/211[129] umsetzen, die eine globale Kultur der Cybersicherheit und einen Schutz der kritischen Informationsinfrastrukturen zu schaffen versuchen. Diese beiden Resolutionen geben indessen nur, aber immerhin, einen groben Rahmen vor, wie die kritischen Infrastrukturen zu schützen sind, beispielsweise durch Verhaltenstrainings, Kommunikation zwischen den Stakeholdern sowie Koordination im Rahmen des Notfallmanagements (einschliesslich der Fähigkeit zur Überwachung, Warnung, Reaktion und Wiederherstellung).

Für die Cybersicherheit von geringerer Bedeutung, aber nicht gänzlich belanglos, ist die Budapest Convention on Cybercrime, die von mehr als 60 Staaten ratifiziert wurde (u.a. auch von Staaten ausserhalb von Europa, wie z.B. Argentinien, Australien, Kanada, Chile, Israel, Japan und die Vereinigten Staaten);[130]

---

124 Im Detail zu diesem Thema vgl. *Kulesza/Weber*, 2021, 5; *Henriksen*, 2019, 4 ff.

125 *UN General Assembly*, Dokument A/68/98.

126 *UN General Assembly*, Dokument A/70/174.

127 *Weber*, 2021f, Rn. 11; *Weber*, 2020, 287 f.; *Tikk*, 2017, 1 ff.; *Meyer*, 2017, 352 f. und 357.

128 UN-Resolution 58/199 vom 21. Dezemeber 2009, Creation of a global culture of cybersecurity and the protection of critical information infrastructures.

129 UN-Resolution 64/211 vom 23. Dezemeber 2003, Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructures.

130 Convention on Cybercrime (ETS No. 185) vom 23. November 2001, Budapest 2001.

die Budapest Convention on Cybercrime beschäftigt sich hauptsächlich mit der Cyberkriminalität und enthält keine ausdrücklichen Vorgaben zur Cybersicherheit.[131]

Ferner leitet die Schweiz in ihrem Positionspapier basierend auf der völkerrechtlichen Due Diligence staatliche Verpflichtungen im Cyberraum ab; die Due Diligence ist ein völkerrechtlicher Verhaltensstandard, der gemäss dem Internationalen Gerichtshof (IGH) als «every State's obligation not to allow knowingly its territory to be used for acts contrary to the rights of other States» umschrieben wird. Die Staaten sind verpflichtet, diese Due-Diligence-Sorgfaltspflichten mit Bezug auf Handlungen innerhalb des eigenen Hoheitsgebiets, welche die Rechte anderer Staaten verletzen könnte, zu beachten.[132]

Die Due Diligence als völkerrechtliches Prinzip, das völkergewohnheitsrechtlich anerkannt ist, gilt gemäss dem Positionspapier auch im Cyberraum.[133] Selbst wenn die Due Diligence keine detaillierte Regelung darstellt, sondern bloss ein Prinzip ist, kann ein völkerrechtlich verantwortlicher Staat immerhin verpflichtet werden, allfällige Schutzlücken zu schliessen und bei der Abwehr eines Cybervorfalls behilflich zu sein; dies gilt insbesondere in jenen Konstellationen, die eine Attribution an ein Staat nicht oder nicht eindeutig ermöglichen (insb. in Fällen von [privaten] Hackergruppen).[134]

2. Regionale und nationale Rechtsinstrumente

Eine erfolgreichere, regional flächendeckende Lösung wird in der Europäischen Union mit dem geplanten Digital Operational Resilience Act (DORA) angestrebt. Die Europäische Union ist im Begriff, mit dem DORA einen Rahmen für die Cyber-Resilienz zuhanden der Finanzunternehmen auf Gesetzesstufe zu schaffen.

Die vorhandenen nationalen Regelwerke verfolgen grundsätzlich einen risikobasierten Ansatz. Unterschiede gibt es in der Art der Umsetzung eines solchen Ansatzes. Während die Schweiz, Liechtenstein, das Vereinigte Königreich und Indien auf Gesetzesstufe kein umfassendes Cybersicherheitsgesetz ein-

131 Vgl. auch *Weber*, 2021f, Rn. 14 f.

132 IGH, Corfu Channel Case (UK v. Albania), Merits, Urteil vom 9. April 1949, ICJ Reports 1949, 22.

133 *DV*, 2021. Direktion für Völkerrecht (DV), Schweizer Positionspapier: Die Anwendung des Völkerrechts im Cyberraum, Annex UN GGE Cybersicherheit 2019/2021, Bern 2021, 7 f., auch Fn. 24.

134 Vgl. *DV*, 2021, 8; zur Attribution im Allgemeinen vgl. *DV*, 2021, 5 f.

geführt haben, ist in den weiteren asiatischen Rechtsordnungen das Gegenteil ersichtlich, denn Singapur, Hong Kong, China und Japan kennen ein umfassendes, sektorübergreifendes Cybersicherheitsgesetz.

In den USA ist die Lage unübersichtlicher, da im Rahmen der Cybersicherheit eine Mischung aus allgemein anwendbaren Bundesgesetzen, einzelstaatlichen Gesetzen, sektorspezifischen Bundesgesetzen, sektorspezifischen einzelstaatlichen Gesetzen, Gewohnheitsrecht sowie Selbstregulierungsvorgaben zur Anwendung kommt.

Bei der Aufsicht des Finanzsektors sind immerhin nicht zu unterschätzende Ähnlichkeiten festzustellen, da alle untersuchten Rechtsordnungen detaillierte, sektorspezifische Regelungen – in Form von Rundschreiben, Leitlinien, Richtlinien, Cybersicherheitsprogrammen oder übrigen Regeln – aufgestellt haben.

3. Selbstregulierung

Zur Transnationalität tragen weiter die Standardisierungsbemühungen privater internationaler Organisationen bei, denn neben den staatlichen Regelungsvorhaben bestehen auch Richtlinien und Standards, welche eine technisch-organisatorische Implementierung anstreben; erwähnenswert sind die Handlungsempfehlungen[135] sowie die Leitsätze für Finanzmarktinfrastrukturen der Bank for International Settlements (BIS) und der International Organization of Securities Commissions (IOSCO)[136] oder auch die verschiedenen Standards zur Informationssicherheit (z.B. die ISO/IEC-27000-Reihe) sowie zur Sicherung der Domain Name Systeme (z.B. die Domain Name System Security Extensions [DNSSEC]).

Die ISO/IEC-27000-Reihe – herausgegeben von der International Organisation for Standardisation (ISO) und der International Electrotechnical Commission (IEC) – bietet Best-Practice-Empfehlungen für die Informationssicherheit an. Inhaltlich sind sie absichtlich breit ausgestaltet und behandeln mehr als nur Cybersicherheitsthemen; die Reihe enthält für Unternehmen aller Grössen und aller Branchen anwendbare Leitlinien.

135 BIS/IOSCO, 2016.

136 BIS/IOSCO, 2012.

B. Schweiz

In der Schweiz gibt es verschiedene Modelle für die Regulierung der Cybersicherheit und der Cyber-Resilienz; diese reichen von Rundschreiben der FINMA[137] bis hin zu sektorspezifischen Regelungsversuchen[138] und sektorübergreifenden Bestrebungen.[139]

1. Dossier «Cyberrisiken» der FINMA

a) Aufgabenbereich der FINMA

Die FINMA kontrolliert und beaufsichtigt als Finanzmarktaufsichtsbehörde der Schweiz alle Bereiche des Finanzwesens (u.a. Banken, Versicherungen, Börsen, Wertpapierhäuser sowie kollektive Kapitalanlagen und Prüfgesellschaften). Im Rahmen der Revision des Rundschreibens 2008/21 von 2019 hat die FINMA verschiedene Ergänzungen im Bereich der Cyberrisiken aufgenommen. Nach den neuen Regeln ist die Vorgehensweise bei Cyberrisiken zu dokumentieren; die Dokumentation soll mindestens folgende Aspekte abdecken:[140]

- Identifikation der institutsspezifischen Bedrohungspotenziale durch Cyberattacken;
- Schutz der Geschäftsprozesse und der Technologieinfrastruktur vor Cyberattacken;
- Zeitnahe Erkennung und Aufzeichnung von Cyberattacken;
- Reaktion auf Cyberattacken mit zeitnahen und gezielten Massnahmen;
- Sicherstellung der zeitnahen Wiederherstellung des normalen Geschäftsbetriebs nach Cyberattacken.

Die Finanzdienstleister sind ausserdem verpflichtet, regelmässige Verwundbarkeitsanalysen und Penetrationstests durchzuführen; hierfür erweisen sich qualifiziertes Personal und angemessene Ressourcen als erforderlich.[141]

Aus dem FINMA-Risikomonitor 2021 ist ersichtlich, dass die Cyberrisiken ein zunehmend relevantes Risiko darstellen; gemäss Monitor steigt die Cyberkri-

137 FINMA, Rundschreiben 2008/21.
138 BFE, 2021.
139 EFD, 2020.
140 FINMA, Rundschreiben 2008/21, Rn. 135.6 ff.
141 FINMA, Rundschreiben 2008/21, Rn. 135.12.

minalität und es kann zu Cybersabotagen von kritischen Infrastrukturen kommen. Erfolgreiche Cyberangriffe vermögen gravierende Folgen für die Funktionsfähigkeit des Finanzplatzes Schweiz zu haben, indem beispielsweise Finanzdienstleistungen nur noch verzögert bzw. unter Umständen gar nicht mehr erbracht werden können.[142]

Im Jahresbericht 2020 stellt die FINMA ferner fest, dass die Abhängigkeit von den Informations- und Kommunikationstechnologien weiter ansteigt und somit die Verwundbarkeit der Finanzinstitute erhöht wird. Aus diesem Grund beabsichtigt die FINMA, die Finanzinstitute mittels Analyse der Bedrohungslage, laufender Aufsicht und Vorfallbewältigung bzw. Krisenmanagement zu überwachen. Bei der Umsetzung dieses Aufsichtskonzepts fokussiert sich die FINMA u.a. auf die Etablierung der Bedrohungslage sowie die Durchführung von Vor-Ort-Kontrollen bei den Finanzinstituten. Ziel der FINMA ist es, frühzeitig über kritische Cybervorfälle orientiert zu sein, um zeitnahe Unterstützung anbieten zu können; entsprechend sind wesentliche Cyberangriffe auf kritische Funktionen der Finanzinstitute der FINMA zu melden.[143] Die rechtliche Grundlage dieser Meldepflicht ergibt sich aus Art. 29 Abs. 2 FINMAG.

b) Umsetzung

Die FINMA kann Selbstbeurteilungen von den Beaufsichtigten verlangen und Vor-Ort-Kontrollen durchführen.

Im Jahre 2016 hat die FINMA bloss von «sehr bedeutenden, komplexen Marktteilnehmern» sowie «grossen und komplexen Marktteilnehmern» eine Selbstbeurteilung verlangt, nicht jedoch von «äusserst grossen, bedeutenden und komplexen Marktteilnehmern», «Marktteilnehmern mittlerer Grösse» oder «kleinen Marktteilnehmern».[144] Problematisch an diesem Vorgehen ist, dass auch die übrigen, nicht zur Selbstbeurteilung verpflichteten Adressaten aufgrund der Abhängigkeiten die Stabilität des Finanzplatzes Schweiz gefährden können. Folglich ist im Rahmen der Cybersicherheit die Kategorisierung der

142 FINMA, Risikomonitor 2021, 11 f.

143 FINMA, Jahresbericht 2020, 35.

144 EFK, 2020, 17 und 20; zur Kategorisierung der Banken vgl. FINMA, Kategorisierung von Banken und Wertpapierhäusern, aufrufbar unter <https://www.finma.ch/de/ueberwachung/banken-und-wertpapierhaeuser/kategorisierung/>.

Adressaten an sich und die damit zusammenhängenden Massnahmen nur bedingt sinnvoll, da für einen erfolgreichen Angriff bereits das Ausnutzen einzelner Schwachstellen genügt.[145]

Die FINMA führt bei den Adressaten seit 2018 Vor-Ort-Kontrollen durch. Auch bei dieser Massnahme ergibt sich dasselbe Bild: Die FINMA hat bisher in den Aufsichtskategorien «Marktteilnehmer mittlerer Grösse» sowie «kleine Marktteilnehmer» keine Vor-Ort-Kontrollen durchgeführt. Gesamthaft betrachtet werden zu wenige Vor-Ort-Kontrollen praktiziert; in den Jahren 2018 und 2019 waren es je fünf.[146]

Die Eidgenössische Finanzkontrolle (EFK) hat im Jahre 2020 eine Prüfung der Aufsicht über die Cybersicherheit bei Finanzdienstleistern durchgeführt. Aus dem Bericht der EFK geht hervor, dass die FINMA nur einen lückenhaften Überblick über die Cybersicherheit der beaufsichtigten Institute hat; insbesondere die allgemeine Meldepflicht nach Art. 29 Abs. 2 FINMAG funktioniert noch nicht ausreichend. Gemäss FINMA selbst wurden bisher nicht alle relevanten Vorfälle gemeldet; jedoch sind bei der Risikoanalyse genau solche Meldungen zu Cybervorfällen ein wichtiges Hilfsmittel, um die Cybersicherheit und Cyber-Resilienz grossflächig zu stärken. Um der Meldepflicht mehr Bedeutung zu geben, wäre erwünscht, Verletzungen der Meldepflicht mit verwaltungsrechtlichen Zwangsmitteln zu verfolgen.[147]

2. Nationale Strategie zum Schutz der Schweiz vor Cyberrisiken

a) Strategische Zielsetzung

Neben den sektorspezifischen Regelungen der FINMA versucht die Schweiz auch sektorübergreifend Cyberrisiken abzufangen. Die nationale Strategie zum Schutz der Schweiz vor Cyberrisiken baut auf der nationalen Strategie von 2012-2017 auf und beabsichtigt, die Verwundbarkeiten zu minimieren und die Schweiz vor der intensivierten Bedrohungslage im Bereich der Cybersicherheit zu schützen sowie Massnahmen für absehbare, zukünftige Entwicklungen aufzunehmen.[148]

145 EFK, 2020, 17 f.
146 EFK, 2020, 21.
147 EFK, 2020, 18 f.
148 NCSC, 2018, 2.

Zu den strategischen Zielen der nationalen Strategie zum Schutz der Schweiz vor Cyberrisiken 2018-2022 gehören:[149]

- Über Kompetenzen, Wissen und Fähigkeiten verfügen, um Cyberrisiken frühzeitig zu erkennen und einzuschätzen;
- Wirksame Massnahmen zur Reduktion der Cyberrisiken entwickeln und bei der Prävention umsetzen;
- Über Kapazitäten und Organisationsstrukturen verfügen, um Cybervorfälle rasch zu erkennen und zu bewältigen;
- Resilienz gegenüber Cybervorfällen schaffen;
- Schutz der Schweiz als gemeinschaftliche Aufgabe von Gesellschaft, Wirtschaft und Staat wahrnehmen;
- Engagement der Schweiz für die internationale Kooperation zur Erhöhung der Cybersicherheit und Förderung des Dialogs verstärken;
- Aus Cybervorfällen im In- und Ausland lernen.

Das NCSC geht von einem risikobasierten, umfassenden Ansatz aus. Es ist folglich weder ein umfassender Schutz vor Cyberrisiken möglich noch existiert ein allgemeingültiger Mindeststandard. Dieser Ansatz basiert also implizit darauf, dass kein vollständiger Schutz möglich ist, jedoch die Risiken in jenem Rahmen zu behandeln sind, der das verbleibende Risiko tragbar macht. Ferner werden mit diesem umfassenden Ansatz alle relevanten Verwundbarkeiten und Bedrohungen berücksichtigt.[150]

b) Meldepflicht für kritische Infrastrukturen bei Cyberangriffen

In der Schweiz sind die Betreiber der Systeme und die Fachämter für den Schutz der kritischen Infrastrukturen[151] verantwortlich; subsidiär bietet das nationale Zentrum für Cybersicherheit (NCSC) bei der Bewältigung von Ereignissen fachliche Unterstützung an.

149 NCSC, 2018, 9.

150 *Ibid.*

151 Kritische Infrastrukturen lassen sich definieren als Prozesse, Systeme und Einrichtungen, die essenziell für das Funktionieren der Wirtschaft bzw. das Wohlergehen der Bevölkerung sind (NCSC, 2018, 9; Art. 3 lit. g CyRV enthält dieselbe Definition); auch der Sektor Finanzen (mit Finanz- und Versicherungsdienstleistungen) gehört zu den kritischen Infrastrukturen (EFD, 2020, 4).

Gegenwärtig bestehen für Cybervorfälle noch keine Meldepflichten, jedoch können sie freiwillig an die Melde- und Analysestelle zur Informationssicherung (MELANI)[152] und/oder an sektorielle Cybermeldestellen (Sektoren-CERTs) mitgeteilt werden.[153] Derzeit steht ein Ausbau der Meldestellen und -pflichten zur Diskussion:[154]

Denkbar ist einerseits, eine zentrale Meldestelle zu errichten, welche als sektorübergreifende Meldestelle für alle Sicherheitsvorfälle von kritischen Infrastrukturen agieren könnte. Andererseits besteht auch die Möglichkeit, die dezentralen Meldestellen zu stärken und die Meldepflichten auszubauen. Diese zweite Variante hätte den Vorteil, dass sie vergleichsweise rasch umsetzbar wäre. Diskutiert wird auch eine Mischform, welche die dezentralen Meldestellen durch eine zentrale Meldestelle für Cybervorfälle ergänzen soll. Dabei blieben die sektorspezifischen Meldestellen der primäre Ansprechpartner für Sicherheitsvorfälle; ergänzend würde eine übergreifende, zentrale Meldestelle für alle Cybervorfälle festgelegt.

Darüber hinaus wurde zu Beginn des Jahres 2022 eine Vernehmlassung zur Einführung einer Meldepflicht für Cyberangriffe bei kritischen Infrastrukturen eröffnet. Mit der Meldepflicht ist eine verbesserte Übersicht über Cyberangriffe in der Schweiz sowie die Unterstützung der Betroffenen bei der Bewältigung von Cyberangriffen anvisiert. Die Vorlage schafft die gesetzlichen Grundlagen für die Meldepflicht und definiert die Aufgaben des NCSC, welches als zentrale Meldestelle für Cyberangriffe vorgesehen ist.[155]

Das Eidgenössische Finanzdepartement (EFD) sieht in Art. 74*a* ff. des Vernehmlassungsentwurfs zur Änderung des Informationssicherheitsgesetzes (ISG)[156] eine Meldepflicht für Cyberangriffe vor. Demnach sind die Betreiber von kritischen Infrastrukturen gehalten, im Falle eines Cyberangriffs so rasch wie möglich eine Meldung zu erstatten.[157] In Art. 74*b* des Vernehmlassungsentwurfs ist der persönliche Geltungsbereich geregelt; meldepflichtig sein sollen u.a. Banken, Versicherungen und Finanzmarktinfrastrukturen (Art. 74*b* lit. e

152 Am 1. Juli 2020 erfolgte die Integration von MELANI in das NCSC.

153 *EFD*, 2020, 3; vgl. auch *Mathys/Hösli*, 2019, 54.

154 *EFD*, 2020, 3.

155 *Bundesrat*, 2022, Vernehmlassung 2021/70, Meldepflicht von Betreiberinnen kritischer Infrastrukturen für Cyberangriffe.

156 Vernehmlassungsentwurf des Eidgenössisches Finanzdepartement (EFD) zur Änderung des Bundesgesetzes über die Informationssicherheit beim Bund vom 12. Januar 2022.

157 *EFD*, 2022, 17.

des Vernehmlassungsentwurfs). Da gemäss Art. 74*d* des Vernehmlassungsentwurfs nur *Cyberangriffe* meldepflichtig sind, lassen sich *Cybervorfälle* bloss freiwillig melden.[158]

3. Datenschutzregelungen

a) Datenschutzgesetz (DSG)

Das DSG stellt sektorübergreifende Regelungen auf, welche u.a. die Cybersicherheit betreffen. Die relevanten Bestimmungen sind im voraussichtlich am 1. September 2023 in Kraft tretenden nDSG und im VE-VDSG (sowie im aDSG und in der aVDSG) zu finden.

Gemäss Art. 8 Abs. 1 nDSG hat der Auftragsbearbeiter durch geeignete technische und organisatorische Massnahmen eine dem Risiko angemessene Datensicherheit zu gewährleisten (Art. 7 Abs. 1 aDSG); es obliegt dem Bundesrat, die Mindestanforderungen festzulegen (Art. 8 Abs. 3 nDSG und Art. 7 Abs. 2 aDSG). Die Regelungen im VE-VDSG knüpfen an die Standards von Art. 8 ff. aVDSG an und ergänzen diese mit dem neusten Stand der Technik sowie den Vorgaben der Schengen-relevanten Richtlinie (EU) 2016/680[159]. Darüber hinaus beabsichtigt der VE-VDSG auch die Kompatibilität mit der DSGVO zu gewährleisten. Hingegen legt der VE-VDSG keine starren Mindestanforderungen fest, sondern verfolgt einen risikobasierten Ansatz: Die Verantwortlichen haben angemessene Massnahmen anhand der jeweiligen Risiken zu treffen (Art. 1 und 2 VE-VDSG; sinngemäss Art. 8 und 9 aVDSG).[160]

Ferner sieht das DSG neu eine Pflicht zur Meldung von Verletzungen der Datensicherheit vor. Die Regelung ist zwar vergleichbar mit den Art. 33 und 34 DSGVO («Data Breach Notification»), aber die beiden Gesetze verwenden verschiedene Schwellenwerte. Gemäss Art. 24 Abs. 1 nDSG (keine entsprechende Regelung im aDSG) muss der Verantwortliche bloss Verletzungen der Datensi-

158 Vgl. im Detail den Gesetzestext in Vernehmlassung 2021/70, Vernehmlassung aufrufbar unter <https://fedlex.data.admin.ch/eli/dl/proj/2021/70/cons_1>; EFD, 2022, 21.

159 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 119, 4.5.2016, 89–131.

160 EJPD, 2021, 10.

cherheit, die voraussichtlich zu einem *hohen Risiko* für die Persönlichkeit oder die Grundrechte der betroffenen Person führen, dem EDÖB melden, während Art. 33 DSGVO die Schwelle des «hohen Risikos» nicht kennt.

Bei der Benachrichtigung der betroffenen Person ergibt sich das gegenteilige Bild: Art. 34 DSGVO verlangt eine Benachrichtigung nur, falls die Verletzung «voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen zur Folge» hat; gemäss Art. 24 Abs. 4 nDSG (keine entsprechende Regelung im aDSG) hat der Verantwortliche die betroffene Person zu informieren, wenn es zu ihrem Schutz erforderlich ist oder der EDÖB es verlangt.

b) Bankkundengeheimnis (Art. 47 BankG)

Weitere Datenschutzanforderungen sind im Rahmen des Bankkundengeheimnisses gemäss Art. 47 BankG zu berücksichtigen. Art. 47 BankG dient demselben Zweck wie das DSG und schützt die Daten vor dem Zugriff von Dritten, ist aber im Teilbereich des Persönlichkeitsschutzes mit Bezug auf das Bankkundengeheimnis als *lex specialis* zu den Regelungen im DSG und in der VDSG einzustufen.[161] In diesem Zusammenhang stellt sich insbesondere die Frage, inwieweit die Bekanntgabe der Bankkundendaten an potenzielle Cloud-Anbieter mit dem Bankkundengeheimnis vereinbar ist. Die Schweizerische Bankiervereinigung (SBVg) hat hierfür zwei Rechtsgutachten eingeholt, welche die Rahmenbedingungen einer Datenbekanntgabe analysieren:[162]

Isler/Kunz/Müller/Schneider/Vasella sind der Ansicht, dass die Banken Hilfspersonen (Erfüllungsgehilfen) beiziehen dürfen und die Bekanntgabe von CID («Costumer Identifying Data») an diese Personen zulässig ist, falls die Hilfspersonen die Geschäftstätigkeit der Bank unterstützen und ihrer Weisungsbefugnis unterstehen, die Bank die mit dem Bankkunden vereinbarten Leistungen überwiegend selbst erbringt, die Unzulässigkeit des Beizugs nicht aus einer ausdrücklich oder stillschweigend getroffenen Abrede mit dem Bankkunden folgt und die Bank ein vernünftiges Interesse am Outsourcing hat.[163]

Gemäss dem Gutachten ist Art. 47 BankG eine strafrechtliche Verstärkung der zivilrechtlich begründeten Geheimhaltungspflichten; insofern ist die Bekanntgabe von Bankkundendaten strafrechtlich zulässig, falls sie vertragsrechtlich

---

161 *Schulthess Komm. BankG-Kleiner/Schwob/Winzeler*, Art. 47 Rn. 14 und 403 ff.

162 *Weber/Henseler*, 2020, 612 f.; *SBVg*, 2020, 12 ff. und 32 f.

163 *Isler/Kunz/Müller/Schneider/Vasella*, 2019, Rn. 5.

ebenfalls zulässig ist.[164] Die Autoren führen weiter aus, dass die Bank bei einer solchen Auslagerung unter strafrechtlichen Gesichtspunkten die nach den Umständen gebotene Sorgfalt einzuhalten hat, damit sie sich nicht dem Vorwurf der Fahrlässigkeit aussetzen muss. Die gebotene Sorgfalt ergibt sich demnach aus dem geltenden Datenschutzrecht, aus den Anforderungen der FINMA[165] und dem Leitfaden des EDÖB zu den technischen und organisatorischen Massnahmen zum Datenschutz.[166]

Laux/Hofmann/Schieweck/Hess gehen davon aus, dass die Cloud-Lösungen auch den Banken zur Verfügung stehen, sofern die Banken das Erfordernis der sorgfältigen Auswahl des Anbieters erfüllen und – um strafrechtlich relevante Offenbarungen im Normalbetrieb zu verhindern – geeignete Massnahmen veranlassen, sodass die migrierten Daten in den IT-Infrastrukturen des Cloud-Anbieters geschützt sind.[167] Demnach verletzt die Bank weder ihre Garantenstellung noch laufen die Organe der Bank Gefahr, aufgrund fahrlässiger Tatbegehung bestraft zu werden, falls sie bei sorgfältiger Prüfung zum Ergebnis gelangen, dass ihre Massnahmen nach dem voraussehbaren Lauf der Dinge im Normalbetrieb allfällige Offenbarungen ausschliessen würden. Diese Ausführungen gelten laut den Autoren insbesondere, wenn die Banken den Cloud-Anbieter auf dieser Grundlage vertraglich als Beauftragten im Sinne von Art. 47 BankG in ihre Risikosphäre einbinden.[168]

Rosenthal hat die Rechtslage auf der Basis der beiden Gutachten erneut analysiert.[169] Gemäss *Rosenthal* dient die Pflicht zur angemessenen Datensicherheit und Verwendungskontrolle – die auf einem normativen Konsens fundiert – als genügende Basis für den Beizug von Cloud-Anbietern, weshalb dieser als datenschutzrechtlich zulässig erscheint.[170] Ferner geht er davon aus, dass im Rahmen des «Lawful Access» oder wegen fehlender Durchsetzbarkeit des Art. 47 BankG im Ausland neue Probleme im Zusammenhang mit der Auswahl

164 *Isler/Kunz/Müller/Schneider/Vasella*, 2019, Rn. 7, 14 ff., 59. Gemäss dem Gutachten gilt dies auch für das Ausland, vgl. *Isler/Kunz/Müller/Schneider/Vasella*, 2019, Rn. 9 und 62 f.

165 Eidgenössische Finanzmarktaufsicht FINMA, Rundschreiben 2008/21 Operationelle Risiken – Banken, Eigenmittelanforderungen und qualitative Anforderungen für operationelle Risiken bei Banken.

166 Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter EDÖB, Leitfaden zu den technischen und organisatorischen Massnahmen des Datenschutzes; *Isler/Kunz/Müller/Schneider/Vasella*, 2019, Rn. 11 und 65 ff., insb. Rn. 71 mit Fn. 57.

167 *Laux/Hofmann/Schieweck/Hess*, 2019, Management Summary und Rn. 56 ff.

168 *Laux/Hofmann/Schieweck/Hess*, 2019, Rn. 56.

169 Vgl. *Rosenthal*, 2020a, insb. Rn. 30 ff.

170 *Rosenthal*, 2020a, Rn. 43 f.

und Nutzung der Cloud-Dienstleister im Ausland resultieren könnten, welche die Banken im Rahmen der Risikobeurteilung zu berücksichtigen haben. Sofern sich das Restrisiko in einem akzeptablen Rahmen hält, ist gemäss *Rosenthal* die Nutzung von Cloud-Anbietern im Ausland zulässig.[171]

4. Anhang: Cybersicherheit und Cyber-Resilienz für die Schweizer Stromversorgung

Obwohl die Cybersicherheit und die Cyber-Resilienz der Schweizer Stromversorgung nicht unmittelbar den Bereich der Finanzinstitute betreffen, geben sie einerseits einen wichtigen Einblick in vergleichbar systemische und kritische Infrastrukturen, andererseits bildet die Stromversorgung die Grundlage für das Funktionieren der IKT-Dienste bzw. IKT-Systeme. Aus diesen Gründen erscheint eine kurze Zusammenfassung der Rahmenordnung für die Cybersicherheit und Cyber-Resilienz in der Schweizer Stromversorgung als angebracht.[172]

Die Cybersicherheit im Bereich der Stromversorgung ist nicht vollständig reguliert; die wenigen vorhandenen und rechtlich verbindlichen Dokumente enthalten ausserdem keine detaillierten Vorgaben bezüglich der Cybersicherheit und der Cyber-Resilienz.[173]

Gemäss Landesversorgungsgesetz (LVG) hat das Bundesamt für wirtschaftliche Landesversorgung (BWL) die Kompetenz, subsidiär präventive Massnahmen zur Sicherstellung der Energieversorgung umzusetzen; das BWL hat hierfür Cyberstandards zuhanden der Wirtschaft und der Stromversorgung festgelegt, um für unmittelbar drohende Mangellagen vorbereitet zu sein.[174]

In Art. 7 Abs. 1 Energiegesetz (EnG) ist als Leitlinie festgehalten, dass für eine sichere Energieversorgung jederzeit ausreichend Energie und ein breit gefächertes Angebot sowie technisch sichere und leistungsfähige Versorgungs- und Speichersysteme verfügbar sein müssen. Diese Vorgabe umfasst implizit auch den Schutz der kritischen Infrastrukturen einschliesslich der zugehörigen IKT.[175]

171 *Rosenthal*, 2020a, Rn. 53 ff.

172 *Bundesrat*, 2019, 11 ff.; vgl. ferner *EFD*, 2020, 3.

173 *BFE*, 2021, 41; vgl. ferner zur Bedeutung des Soft Law Kap. II.D und III.F.

174 *BFE*, 2021, 42.

175 *Ibid.*

Schliesslich finden sich im Stromversorgungsgesetz (StromVG) und in der Stromversorgungsverordnung (StromVV) Bestimmungen, die einen Bezug zur Cybersicherheit und zur Cyber-Resilienz herstellen. Art. 8 Abs. 1 lit. a StromVG schreibt vor, dass Netzbetreiber ein sicheres, leistungsfähiges und effizientes Netz zu gewährleisten haben; ferner müssen die Betreiber der Verteilnetze erforderliche Massnahmen treffen, um jederzeit die gewünschte Menge an Elektrizität mit der erforderlichen Qualität verfügbar zu halten und zu angemessenen Tarifen liefern zu können (Art. 6 Abs. 1 StromVG). Ähnlich dem EnG implizieren auch diese Vorgaben, dass angemessene Massnahmen für die Cybersicherheit zu treffen sind, ohne sie aber zu konkretisieren; folglich bestehen keine ausdrücklichen Vorgaben mit Bezug auf die Vorgehensweise bei Cyberrisiken.[176] Immerhin halten Art. 8a und 8b StromVV einzelne Massnahmen fest, welche im Bereich der Datensicherheit auf die Einhaltung eines Branchenstandards verweisen.[177]

C. Liechtenstein

1. Grundsätze

In Liechtenstein ist am 1. Januar 2022 die Richtlinie IKT-Sicherheiten der Finanzmarktaufsicht Liechtenstein (FMA) in Kraft getreten. Sie regelt gestützt auf Art. 4 und Art. 25 Abs. 1 FMAG die Überwachung der IKT-Risiken der Finanzintermediäre nach dem Prinzip der Proportionalität, d.h. die Richtlinie ist nach Risikostruktur, Komplexität, Grösse, Umfang sowie Art des Geschäfts umzusetzen. Die jeweiligen Finanzintermediäre haben die angemessene Umsetzung sicherzustellen. Gemäss den Definitionen der Richtlinie beinhalten die IKT- und Sicherheitsrisiken auch die Cyberrisiken.[178]

2. Richtlinie IKT-Sicherheiten

Verschiedenste Finanzintermediäre sind Adressaten (u.a. Banken, Wertpapierfirmen, Zahlungsinstitute, Versicherungsunternehmen, Vorsorgeeinrichtungen, Vermögensverwalter) der FMA-Richtlinie.

176 *Komm. StromVG-Kaiser*, 2016, Art. 8 N 4 und 9 m.w.H.; vgl. ferner *Komm. StromVG-Weber*, 2016, Art. 1 N 22.

177 *BFE*, 2021, 42 f.

178 FMA, Richtlinie 2021/3, 4; vgl. ferner zur Bedeutung des Soft Law Kap. II.D und III.F.

a) IKT-Strategie und -Sicherheitsmanagement

Gemäss der Richtlinie sind die Leitungsorgane verpflichtet, eine IKT-Strategie festzulegen und deren Wirksamkeit regelmässig zu überprüfen. Durch die IKT-Governance stellen die Finanzintermediäre sicher, dass ein angemessener interner Kontrollrahmen besteht (u.a. ausreichende Qualifikation des Personals sowie ausreichende Ressourcen).[179]

Mithilfe eines wirksamen IKT- und Informationssicherheitsrisikomanagements sind die Finanzintermediäre gehalten, ihre IKT-, Sicherheits- und Cyberrisiken zu identifizieren, zu bewerten und zu steuern. Entsprechend den Grundsätzen der Cybersicherheit sind geeignete Prozesse und Kontrollen erforderlich, um sicherstellen zu können, dass alle Risiken identifiziert, analysiert, gemessen, überwacht, gesteuert, gemeldet und innerhalb der Grenzen der Risikobereitschaft des Finanzintermediärs gehalten werden können. Diese Aufgaben sind an die für das Risikomanagement zuständige Stelle zu übertragen, welche durch eine angemessene Trennung der IKT-Betriebsprozesse unabhängig ist und objektiv agiert.[180]

Das IKT- und Informationssicherheitsrisikomanagement umfasst folgende Prozesse:[181]

- Ermittlung der Risikobereitschaft für IKT-, Sicherheits- und Cyberrisiken des Finanzdienstleisters;
- Identifikation und Bewertung der IKT-, Sicherheits- und Cyberrisiken;
- Festlegung von Massnahmen zur Minderung von IKT-, Sicherheits- und Cyberrisiken;
- Überwachung der Wirksamkeit dieser Massnahmen und Erfassung der Anzahl gemeldeter Vorfälle;
- Berichterstattung über die IKT-, Sicherheits- und Cyberrisiken;
- Identifikation und Beurteilung, ob IKT-, Sicherheits- und Cyberrisiken bestehen, die sich aus einer wesentlichen Änderung des IKT-Systems oder der IKT-Dienste ergeben.

Identifizierte Geschäftsfunktionen, Unterstützungsprozesse und IKT-Assets sind nach ihrer Kritikalität einzustufen; die Betroffenen haben hierfür Vertrau-

179 FMA, Richtlinie 2021/3, 6 f.
180 FMA, Richtlinie 2021/3, 7.
181 FMA, Richtlinie 2021/3, 8.

lichkeits-, Integritäts- und Verfügbarkeitsanforderungen zu berücksichtigen. Mögliche IKT-, Sicherheits- und Cyberrisiken sind ferner auf ein akzeptables Mass zu begrenzen und die Ergebnisse der Risikobewertung dem Leitungsorgan klar und rechtzeitig mitzuteilen.[182]

b) Prävention und Reaktion

Die Finanzintermediäre sind ausserdem verpflichtet, mittels Good-Practice-Ansätzen (z.B. Schwachstellenmanagement mit regelmässigen Verwundbarkeitsanalysen, Penetrationstests, Red-Team-Übungen und weiteren geeigneten Massnahmen) mögliche Sicherheitslücken zu überprüfen. Für Informationssicherheitstests müssen die Finanzintermediäre ein Rahmenwerk, welches die Robustheit und Wirksamkeit der Massnahmen betreffend Informationssicherheit bewertet und gewährleistet, einrichten und umsetzen. Das Rahmenwerk stellt sicher, dass die Tests von unabhängigen Prüfern durchgeführt werden und umfassende Schwachstellen- und Penetrationstests enthalten;[183] mit dem Threat-Led-Penetrationstest beispielsweise wird in einem kontrollierten Rahmen durch Simulation von Verfahren und Techniken realer Bedrohungsakteure die Cyber-Resilienz des Unternehmens gefährdet, um anhand realer Bedrohungsinformationen die Mitarbeitenden auszubilden sowie die Prozesse und Technologien zu verbessern.[184]

Neben der digitalen Sicherheit regelt die Richtlinie auch die physische Sicherheit. Die Finanzintermediäre sind verpflichtet, einen physischen Sicherheitsrahmen zu definieren, um Räumlichkeiten, Rechenzentren und sensible Bereiche vor unbefugtem Zugang zu schützen; entsprechend der Wichtigkeit der Gebäude und der Kritikalität der in diesen Gebäuden befindlichen IKT-Systeme sind angemessene Massnahmen erforderlich.[185]

Als Teil des IKT-Betriebsmanagement definieren und implementieren die Finanzintermediäre periodische Sicherungs- und Wiederherstellungsverfahren für Daten und IKT-Systeme, um diese bei Bedarf wiederherstellen zu können; die Systeme müssen auch Cyberangriffen standhalten können. Die Häufigkeit der Sicherungen ist anhand der durchgeführten Risikobewertung und Kritikalität der Daten bzw. der IKT-Systeme zu bestimmen.[186]

182 FMA, Richtlinie 2021/3, 8 f.
183 FMA, Richtlinie 2021/3, 10 f.
184 FMA, Richtlinie 2021/3, 5.
185 FMA, Richtlinie 2021/3, 13.
186 FMA, Richtlinie 2021/3, 13 f.

Darüber hinaus haben die Finanzdienstleister konkrete Verfahren zu implementieren, die das Auftreten von Sicherheitsproblemen in IKT-Systemen und IKT-Diensten verhindern. Diese Verfahren müssen u.a. die potenziellen Schwachstellen ermitteln, Netzwerkkomponenten überwachen, den Schutz von Endpunkten (Server, Arbeitsplatz, Mobilgerät) gewährleisten und die Integrität von Software, Firmware und Daten überprüfen.[187]

Weiter bleiben die Finanzdienstleister auch bei der Auslagerung ihrer IKT-Dienste «in vollem Masse für die Erfüllung ihrer regulatorischen Pflichten verantwortlich und rechenschaftspflichtig». Die Risikobewertung und Due-Diligence-Prüfung im Rahmen der Auslagerung sind im Verhältnis zu Art, Umfang und Komplexität der Risiken durchzuführen.[188] Allfällige Auslagerungsvereinbarungen mit Dienstleistern müssen u.a. Mindestanforderungen an die Cybersicherheit erfüllen, damit die Vertraulichkeit, Verfügbarkeit und Integrität der Daten von den ausgelagerten IKT-Diensten und IKT-Systemen gewährleistet sind.[189]

Die FMA-Richtlinie verpflichtet Finanzintermediäre zudem, unter Berücksichtigung von möglichen Cyberangriffen ein Notfallkonzept sowie Reaktions- und Wiederherstellungspläne zu entwickeln. Im Rahmen des Business-Continuity-Planing sind regelmässige Tests durchzuführen und wirksame Massnahmen zur Krisenkommunikation einzuführen.[190]

D. Europäische Union

1. Behördenorganisation

Die gegenwärtige europäische Regulierungslandschaft im Finanzsektor für IKT- und Cyberrisiken ist vielschichtig. Es gibt nicht *eine* europäische Cybersicherheitsgesetzgebung für den Finanzdienstleistungssektor, sondern eine Vielzahl unterschiedlicher europäischer und nationaler Vorschriften und sektorspezifischer Standards. Die Finanzinstitute sind verpflichtet, sich an die Vorschriften für kritische Infrastrukturen, an allgemeine europäische Rechtsvorschriften und an spezifische Vorschriften und Standards für den Finanzsektor zu halten. Die Zuständigkeiten variieren in der EU je nach Vorschrift

187 FMA, Richtlinie 2021/3, 14.

188 FMA, Richtlinie 2021/3, 18; vgl. ferner FMA, Richtlinie 2021/3, 19 ff.

189 FMA, Richtlinie 2021/3, 22.

190 FMA, Richtlinie 2021/3, 26 f.

bzw. Rechtsakt; für Richtlinien der Europäischen Union, welche die Mitgliedstaaten umzusetzen haben, sind grundsätzlich deren gesetzgeberische Behörden zuständig; für die Umsetzung der DSGVO hingegen sind die Datenschutzaufsichtsbehörden der Mitgliedstaaten zuständig.

Sektorspezifisch für die Finanzmärkte steht der Digital Operational Resilience Act (DORA) im Vordergrund (2.). Darüber hinaus regeln weitere Verordnungen sektorübergreifende Fragen im Rahmen der Cybersicherheit und der Cyberangriffe (3.). Die wichtigsten und weitreichendsten sektorübergreifenden Rechtsvorschriften für Finanzinstitute sind die Richtlinie über die Sicherheit von Netz- und Informationssystemen (NIS-Richtlinie, 4.),[191] ergänzt durch verschiedene, zum Teil sektorspezifische Empfehlungen und Leitlinien (5.), sowie die allgemeine Datenschutzverordnung (DSGVO, 6.).

2. Digital Operational Resilience Act (DORA)

a) Hintergrund

Die Verflechtungen zwischen den Finanzmärkten, Finanzdienstleistern und Finanzmarktinfrastrukturen sowie insbesondere zwischen den IKT-Systemen können zu Systemanfälligkeiten führen, weil auch lokalisierte Cyberangriffe schnell auf das gesamte Finanzsystem übergreifen. Solche Angriffe vermögen die Stabilität des Finanzsystems der Europäischen Union zu beeinträchtigen und zum Verlust des Vertrauens in die Finanzmärkte zu führen (Erw. 3 DORA); um solche Systemausfälle zu verhindern, ist ein einheitliches, harmonisiertes Gesetz erforderlich.

Aktuell sind die Regulierungen des Finanzsektors zusätzlich in Teilsektoren (Banken, Versicherungen, Finanzmarktinfrastrukturen) unterteilt; die Cybersicherheit und Cyber-Resilienz in den Teilsektoren des europäischen Finanzsektors sind nicht einheitlich geregelt. Das bestehende europäische Recht konzentriert sich insbesondere auf Kredit-, Gegenparteiausfall-, Markt-, und Liquiditätsrisiken und geht nur beschränkt auf die IKT-Risiken ein (Erw. 12 DORA).

Eine harmonisierte Regelung der Cybersicherheit ist jedoch unabdingbar, um operationelle Resilienz gegenüber Cyberrisiken zu erreichen. Um diese Situa-

[191] 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 194 vom 19.7.2016, 1–30.

tion zu verbessern, hat die Europäische Kommission im September 2020 als Teil der «Strategie für ein digitales Finanzwesen in der EU» den Digital Operational Resilience Act (DORA)[192] für den europäischen Finanzsektor vorgeschlagen. Diese Strategie soll als gemeinsamer und einheitlicher Rechtsrahmen für die meisten europäischen Teilsektoren des Finanzsektors eine Harmonisierung bzgl. IKT-Risiken und Cyberrisiken herbeiführen.

Mit DORA wird ein umfassender Rahmen für die digitale operationelle Widerstandsfähigkeit der europäischen Finanzinstitute geschaffen, der ausdrückliche Anforderungen für den Umgang mit und die Minderung von IKT- und Cyberrisiken festlegt. Um eine erfolgreiche Umsetzung von DORA gewährleisten zu können, sind gemäss Begründungstext zu DORA 18 Vollzeitbeschäftigte erforderlich; je sechs Vollzeitbeschäftigte sind für die Europäische Bankenaufsichtsbehörde (EBA), die Europäische Wertpapier- und Marktaufsichtsbehörde (ESMA) und Europäische Aufsichtsbehörde für das Versicherungswesen und die betriebliche Altersversorgung (EIOPA) vorgesehen.[193]

b) Gegenstand und Geltungsbereich

DORA will ein hohes gemeinsames Niveau digitaler Betriebsstabilität erreichen (Art. 1 Abs. 1 DORA), für das insbesondere Folgendes erforderlich ist:

- Anforderungen an Finanzunternehmen in Bezug auf u.a. Risikomanagement im Bereich der IKT, Prüfung der digitalen Betriebsstabilität, Austausch von Informationen und Erkenntnissen in Bezug auf Cyberbedrohungen und Schwachstellen sowie Massnahmen für die wirtschaftliche Steuerung des Risikos durch IKT- Drittanbieter (lit. a);
- Anforderungen in Bezug auf vertragliche Vereinbarungen zwischen IKT-Drittanbietern und Finanzunternehmen (lit. b);
- Ein Aufsichtsrahmen für kritische IKT-Drittanbieter bei der Erbringung von Dienstleistungen für Finanzunternehmen (lit. c);

192 Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die Betriebsstabilität digitaler Systeme des Finanzsektors und zur Änderung der Verordnungen (EG) Nr. 1060/2009, (EU) Nr. 648/2012, (EU) Nr. 600/2014 und (EU) Nr. 909/2014 vom 24. September 2020 (Englisch: Digital Operational Resilience Act); vgl. ferner WKO, 2021, 2.

193 DORA, «Auswirkungen auf den Haushalt», 7 f.

– Vorschriften über die Zusammenarbeit zwischen zuständigen Behörden und Vorschriften über die Beaufsichtigung und Durchsetzung aller von dieser Verordnung erfassten Sachverhalte durch zuständige Behörden (lit. d).

DORA gilt für Unternehmen, die in Art. 2 Abs. 2 lit. a–u DORA aufgeführt sind; als Finanzunternehmen sind die in lit. a–t erwähnten Unternehmen zu bezeichnen (Art. 2 Abs. 2 DORA). Zu diesen Unternehmen gehören u.a. Kredit- und Zahlungsinstitute, Wertpapierfirmen, Anbieter von Krypto-Dienstleistungen, Zentralverwahrer oder Handelsplätze. Kleinstunternehmen[194] sind von einigen Vorgaben in Art. 4–13 DORA (IKT-Risikomanagement) befreit.

Ferner definiert DORA den Cyberangriff als «böswilligen IKT-bezogenen Vorfall, in dessen Rahmen ein Angriffsvektor versucht, einen Vermögenswert zu zerstören, freizulegen, zu verändern, zu deaktivieren, zu entwenden oder auf unberechtigte Weise auf diesen Vermögenswert zuzugreifen oder ihn auf unberechtigte Weise zu nutzen» (Art. 3 Ziff. 9 DORA).

c) IKT-Risikomanagement

Art. 4 Abs. 1 DORA verpflichtet Finanzunternehmen, einen internen Governance- und Kontrollrahmen einzurichten. Weiter wird vorgesehen, ein Leitungsorgan einzusetzen, das Vorkehrungen im Rahmen des IKT-Risikomanagement definiert, genehmigt und überwacht sowie für deren Umsetzung rechenschaftspflichtig ist (Art. 4 Abs. 2 DORA).

Darüber hinaus haben die Finanzunternehmen «über einen soliden, umfassenden und gut dokumentierten IKT-Risikomanagementrahmen» zu verfügen, welcher IKT-Risiken schnell, effizient und umfassend angeht sowie ein hohes Mass an Betriebsstabilität zu gewährleisten vermag; diese Vorkehrungen müssen den geschäftlichen Bedürfnissen, der Grösse der Unternehmen und ihrer Komplexität entsprechen (Art. 5 Abs. 1 DORA). Der IKT-Risikomanagementrahmen hat auch alle für einen ordnungsgemässen und wirksamen Schutz erforderlichen Strategien, Verfahren, IKT-Protokolle und IKT-Instrumente zu um-

194 Kleinstunternehmen beschäftigen weniger als 10 Personen und haben einen Jahresumsatz bzw. eine Jahresbilanz von weniger als 2 Mio. Euro; sie sind Finanzunternehmen im Sinne von Art. 2 Abs. 3 des Anhangs der Empfehlung der Kommission vom 6. Mai 2003 betreffend die Definition der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen (Text von Bedeutung für den EWR) (Bekannt gegeben unter Aktenzeichen K(2003) 1422), OJ L 124, 20.5.2003, 36–41.

fassen (Art. 5 Abs. 2 DORA). Der IKT-Risikomanagementrahmen soll «jährlich sowie bei Auftreten schwerwiegender IKT-bezogener Vorfälle und nach aufsichtsrechtlichen Anweisungen oder Schlussfolgerungen» dokumentiert und überprüft werden (Art. 5 Abs. 6 DORA).

Als Teil des IKT-Risikomanagementrahmens müssen die Finanzunternehmen neueste IKT-Systeme, IKT-Protokolle und IKT-Instrumente verwenden (Art. 6 DORA) und sie sind verpflichtet, alle IKT-bezogenen Unternehmensfunktionen angemessen zu identifizieren, zu klassifizieren und zu dokumentieren (Art. 7 DORA). Darüber hinaus haben sie auch kontinuierlich die Funktionsweise der IKT-Systeme und IKT-Instrumente zu überwachen und zu kontrollieren sowie die Auswirkungen einschlägiger Risiken durch den Einsatz geeigneter IKT-Sicherheitsinstrumente, IKT-Strategien und IKT-Verfahren zu minimieren (Art. 8 DORA).

Die Finanzunternehmen sind weiter verpflichtet, Mechanismen einzuführen, die anomale Aktivitäten (u.a. Probleme bei der Leistung von IKT-Netzen und IKT-bezogene Vorfälle) umgehend erkennen und alle potenziellen Schwachstellen ermitteln können (Art. 9 DORA). Sie müssen auch in der Lage sein, die Fortführung des Geschäftsbetriebs zu gewährleisten; hierzu implementieren sie Pläne, Verfahren und Mechanismen, die alle IKT-bezogenen Vorfälle aufzeichnen, die Kontinuität der kritischen Funktionen des Finanzunternehmens sicherstellen sowie auf alle IKT-bezogenen Vorfälle (insb. Cyberangriffe) schnell, angemessen und wirksam reagieren (Art. 10 DORA).

Ferner haben die Finanzunternehmen eine Strategie für die Datensicherung und für Wiederherstellungsverfahren zu entwickeln, um den Ausfall von IKT-Systemen mit minimaler Ausfallzeit und begrenzter Störung sicherstellen zu können (Art. 11 DORA). Zudem hält Art. 13 DORA fest, dass das IKT-Risikomanagement ein fortlaufender Lernprozess ist und dass Informationen zu Anfälligkeiten, Cyberbedrohungen, IKT-bezogenen Vorfällen und Cyberangriffen zu sammeln und die Auswirkungen auf die digitale Betriebsstabilität zu untersuchen sind. Teil des IKT-Risikomanagementrahmens ist auch die Verpflichtung der Finanzunternehmen, Kommunikationspläne zu erstellen und eine verantwortungsbewusste Offenlegung IKT-bezogener Vorfälle zu ermöglichen (Art. 14 DORA).

d) IKT-bezogene Vorfälle

Art. 15 ff. DORA gibt vor, wie bei IKT-bezogenen Vorfällen vorzugehen ist; die Finanzunternehmen müssen zu deren Bewältigung konkrete Vorgehensweisen festlegen (Art. 15 DORA); sie sind verpflichtet, die Vorfälle nach folgenden Kriterien zu klassifizieren (Art. 16 Abs. 1 DORA):

- Zahl der Nutzer oder anderer Akteure im Finanzbereich (lit. a);
- Dauer des IKT-bezogenen Vorfalls (lit. b);
- Geografische Ausbreitung (lit. c);
- Mit dem IKT-bezogenen Vorfall verbundene Datenverluste (lit. d);
- Schwere der Auswirkungen (lit. e);
- Kritikalität der betroffenen Dienste (lit. f);
- Wirtschaftliche Auswirkungen auf absoluter und relativer Basis (lit. g).

Die schwerwiegenden Vorfälle haben die Finanzunternehmen anschliessend der zuständigen Behörde zu melden (Art. 17 DORA).

e) Prüfung der digitalen Betriebsstabilität

DORA verpflichtet die Finanzunternehmen, unter Berücksichtigung ihrer Grösse, ihrer Geschäfts- und Risikoprofile ein solides und umfassendes Programm zur Prüfung der digitalen Betriebsstabilität zu erarbeiten, damit sie ihre Abwehrbereitschaft einzuschätzen und Schwachstellen, Mängel oder Lücken zu erkennen vermögen (Art. 17 DORA). Hierfür müssen die Finanzunternehmen verschiedene Tests (u.a. Bewertungen und Überprüfungen der Anfälligkeit, Bewertungen der Netzsicherheit, Lückenanalysen, Fragebögen, Quellcodeprüfungen, Leistungstests, End-to-End-Tests oder Penetrationstests) durchführen (Art. 22 DORA); alle drei Jahre haben die Finanzunternehmen eine erweiterte Prüfung zu machen (Art. 23 DORA). Schliesslich regelt Art. 24 DORA die Anforderungen an die Prüfer.

f) Risiken durch IKT-Drittanbieter

Kapitel V (Art. 25 ff. DORA) verpflichtet die Finanzunternehmen, die durch IKT-Drittanbieter verursachte Risiken im Einklang mit verschiedenen Grundsätzen zu steuern:

Zunächst bleiben die Finanzunternehmen, die IKT-Dienste in Anspruch nehmen, für die Einhaltung von DORA verantwortlich und sind haftbar (Art. 25 Abs. 1 DORA); sie haben bei der Steuerung des Risikos dem Grundsatz der Verhältnismässigkeit – unter Berücksichtigung des Ausmasses, der Komplexität und der Relevanz von IKT-bezogenen Abhängigkeiten sowie der Risiken durch vertragliche Vereinbarungen über die Nutzung der IKT-Dienste – Rechnung zu tragen (Art. 25 Abs. 2 DORA).

Die Finanzinstitute sind darüber hinaus verpflichtet, eine Strategie für das Risiko durch IKT-Drittanbieter zu erstellen und diese regelmässig zu überprüfen (Art. 25 Abs. 3 DORA). Im Bereich ihres IKT-Risikomanagementrahmens müssen die Finanzunternehmen ein Informationsregister mit vertraglichen Vereinbarungen über die Nutzung von IKT-Diensten der Drittanbieter führen (Art. 25 Abs. 4 DORA). Zudem dürfen die Finanzunternehmen nur vertragliche Vereinbarungen, die hohe, angemessene und aktuelle Standards für die Informationssicherheit einhalten, mit Drittanbietern abschliessen (Art. 25 Abs. 6 DORA) und die sich mindestens unter den Umständen von Art. 25 Abs. 8 kündigen (u.a. Kündigung aufgrund Verstosses gegen geltende Gesetze, Verordnungen oder Vertragsbedingungen).

Ferner schafft DORA einen Aufsichtsrahmen für kritische IKT-Drittanbieter (Art. 28 ff. DORA). Für die Bestimmung als kritischer IKT-Drittanbieter sind u.a. folgende Kriterien heranzuziehen (Art. 28 Abs. 2 DORA):

- Systemische Auswirkungen auf die Stabilität, Kontinuität oder Qualität der Erbringung von Finanzdienstleistungen (lit. a);
- Grad der Substituierbarkeit des IKT-Drittanbieters (lit. d);
- Zahl der Mitgliedstaaten, in denen der betreffende IKT-Drittanbieter Dienstleistungen erbringt (lit. e);
- Zahl der Mitgliedstaaten, in denen Finanzunternehmen tätig sind, die den betreffenden IKT-Drittanbieter in Anspruch nehmen (lit. f).

3. Weitere Verordnungen

a) Verordnung über restriktive Massnahmen gegen Cyberangriffe

Die Verordnung über restriktive Massnahmen gegen Cyberangriffe[195] «gilt für Cyberangriffe mit erheblichen Auswirkungen, einschliesslich versuchter Cyberangriffe mit potenziell erheblichen Auswirkungen, die eine äussere Bedrohung für die Union oder ihre Mitgliedstaaten darstellen» (Art. 1 Abs. 1 der Verordnung); sie kann u.a. dazu beitragen, dass die Attribution von Cyberangriffen leichter erfolgt.

Nach Art. 1 Abs. 2 der Verordnung stellt ein Cyberangriff eine äussere Bedrohung dar, wenn er seinen Ausgang ausserhalb der Europäischen Union hat oder von ausserhalb der Europäischen Union durchgeführt wird (lit. a) oder wenn er ausserhalb der Europäischen Union befindliche Infrastrukturen nutzt (lit. b).

Gemäss Art. 1 Abs. 3 der Verordnung gelten alle Handlungen, die den Zugang zu Informationssystemen (lit. a), den Eingriff in Informationssysteme (lit. b), den Eingriff in Daten (lit. c) oder das Abfangen von Daten (lit. d) umfassen, als Cyberangriff, wenn diese Handlungen «vom Eigentümer oder einem anderen Rechtsinhaber des Systems oder der Daten oder eines Teils des Systems oder der Daten nicht ordnungsgemäss gestattet wurden oder nach dem Recht der Union oder des betreffenden Mitgliedstaats nicht zulässig sind».

In Art. 1 Abs. 4 regelt die Verordnung, welche Cyberangriffe eine Bedrohung für die Mitgliedstaaten darstellt; hierzu zählen u.a. Cyberangriffe auf Informationssysteme im Bereich kritischer Infrastrukturen (lit. a) oder «Dienstleistungen, die für die Aufrechterhaltung wesentlicher sozialer und/oder wirtschaftlicher Tätigkeiten erforderlich sind, insbesondere in den Sektoren: […] Bankenwesen, Finanzmarktinfrastrukturen […] und in anderen Sektoren, die für den betreffenden Mitgliedstaat von wesentlicher Bedeutung sind» (lit. b).

[195] Verordnung (EU) 2019/796 des Rates vom 17. Mai 2019 über restriktive Massnahmen gegen Cyberangriffe, die die Union oder ihre Mitgliedstaaten bedrohen, ABl. L 129I vom 17.5.2019, 1–12.

b) Rechtsakt zur Cybersicherheit

Mit dem Rechtsakt zur Cybersicherheit[196] hat die Europäische Union ein Rahmenwerk für die IT-Sicherheitszertifizierung von Produkten, Dienstleistungen und Prozessen geschaffen.

Der Rechtsakt zur Cybersicherheit regelt einerseits die Ziele, Aufgaben und organisatorischen Aspekte der Agentur der Europäischen Union für Cybersicherheit (ENISA), andererseits schafft er einen Rahmen für die Festlegung europäischer Schemata für die Cybersicherheitszertifizierung, mit dem Ziel, für IKT- Produkte und IKT-Dienste sowie IKT-Prozesse in der Union ein angemessenes Mass an Cybersicherheit zu gewährleisten (Art. 1 Rechtsakt zur Cybersicherheit).

Darüber hinaus enthält der Rechtsakt auch Begriffsbestimmungen: Die Cybersicherheit umfasst «alle Tätigkeiten, die notwendig sind, um Netz- und Informationssysteme, die Nutzer solcher Systeme und andere von Cyberbedrohungen betroffene Personen zu schützen» (Art. 2 Ziff. 1 Rechtsakt zur Cybersicherheit). Ferner ist die Cyberbedrohung ein «mögliche[r] Umstand, ein mögliches Ereignis oder eine mögliche Handlung, der/das/die Netz- und Informationssysteme, die Nutzer dieser Systeme und andere Personen schädigen, stören oder anderweitig beeinträchtigen könnte» (Art. 2 Ziff. 8 Rechtsakt zur Cybersicherheit).

4. NIS-Richtlinie

Als erste europaweite Rechtsvorschrift zur Cybersicherheit zielt die NIS-Richtlinie[197] darauf ab, ein gleich hohes Sicherheitsniveau für die Netz- und Informationssysteme in der Europäischen Union zu erreichen und somit eine grenzüberschreitende Lösung zu bieten. Gemäss Art. 1 Abs. 2 lit. a NIS-Richtlinie sind alle Mitgliedstaaten verpflichtet, «eine nationale Strategie für die Sicherheit von Netz- und Informationssystemen festzulegen». Zudem sind sie gehalten, «nationale zuständige Behörden, zentrale Anlaufstellen und Computer Security Incident Response Teams (CSIRTs) mit Aufgaben im Zusammen-

196 Verordnung (EU) 2019/881 des Europäischen Parlaments und des Rates vom 17. April 2019 über die ENISA (Agentur der Europäischen Union für Cybersicherheit) und über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik und zur Aufhebung der Verordnung (EU) Nr. 526/2013 (Rechtsakt zur Cybersicherheit) (Text von Bedeutung für den EWR), ABl. L 151 vom 7.6.2019, 15–69.

197 Weitere Details zur nationalen Strategie sind in Art. 7 NIS-Richtlinie aufgeführt.

hang mit der Sicherheit von Netz- und Informationssystemen zu benennen» (Art. 1 Abs. 2 lit. e NIS-Richtlinie); die Details zu den nationalen zuständigen Behörden und zentralen Anlaufstellen sind in Art. 8 NIS-Richtlinie geregelt.

Mit einem Netzwerk von nationalen Computer Security Incident Response Teams (CSIRTs) sollen die Mitgliedstaaten eine wirksame und effiziente Zusammenarbeit gewährleisten (Art. 12 Abs. 1 NIS-Richtlinie). Das CSIRT-Netzwerk zielt u.a. darauf ab, den Informationsaustausch zu fördern, Informationen zu einzelnen Sicherheitsvorfällen auszutauschen und die aus den Übungen zur Sicherheit von Netz- und Informationssystemen gezogenen Lehren zu erörtern (Art. 12 Abs. 3 NIS-Richtlinie).

Im Anhang II der Richtlinie sind die «Betreiber wesentlicher Dienste» gemäss Art. 4 Ziff. 4 NIS-Richtlinie aufgelistet: Das Bankwesen und die Finanzmarktinfrastrukturen gelten demnach auch als Betreiber wesentlicher Dienste und fallen unter die Regelungen in Kapitel IV der Richtlinie (Art. 14 f. NIS-Richtlinie).

Gemäss Art. 14 Abs. 1 NIS-Richtlinie haben die Mitgliedstaaten sicherzustellen, dass «die Betreiber wesentlicher Dienste geeignete und verhältnismässige technische und organisatorische Massnahmen ergreifen, um die Risiken für die Sicherheit der Netz- und Informationssysteme, die sie für ihre Tätigkeiten nutzen, zu bewältigen». Die Mitgliedstaaten müssen auch Massnahmen ergreifen, welche die Auswirkungen von Sicherheitsvorfällen begrenzen und sicherstellen, dass die Betreiber wesentlicher Dienste solche Sicherheitsvorfälle unverzüglich den zuständigen Behörden melden (Art. 14 Abs. 2 und 3 NIS-Richtlinie).

Um das Ausmass der Auswirkungen eines Sicherheitsvorfalls abschätzen zu können, sind gemäss Art. 14 Abs. 4 NIS-Richtlinie folgende Kriterien zu beachten:

- Zahl der von der Unterbrechung der Erbringung des wesentlichen Dienstes betroffenen Nutzer (lit. a);
- Dauer des Sicherheitsvorfalls (lit. b);
- Geografische Ausbreitung in Bezug auf das von dem Sicherheitsvorfall betroffene Gebiet (lit. c).

Zurzeit wird die NIS-Richtlinie überarbeitet und auf eine grössere Anzahl Sektoren ausgeweitet, welche sich an deren strategischer Bedeutung für Wirtschaft und Gesellschaft messen. Der Entwurf will zudem die Unterscheidung zwischen den Betreibern wesentlicher Dienste und den Anbietern digitaler

Dienste aufgeben; stattdessen sollen die Betreiber bzw. Anbieter nach ihrer Bedeutung als «wesentlich» oder «wichtig» qualifiziert werden. Weiter will der Entwurf die Sicherheitsanforderungen und die Voraussetzungen für Meldungen verschärfen und ein Risikomanagementkonzept vorschreiben.[198]

Darüber hinaus schlägt die Kommission vor, die Sicherheit von Lieferketten und Lieferbeziehungen stärker zu berücksichtigen, indem einzelne Unternehmen zu verpflichten sind, sich mit Cybersicherheitsrisiken in Lieferketten und Lieferbeziehungen zu befassen. Ferner sieht der Entwurf strengere Aufsichtsmassnahmen für die zentralen nationalen Behörden sowie strengere Durchsetzungsanforderungen vor und möchte die Sanktionsregelungen in den Mitgliedstaaten harmonisieren.[199]

5. Empfehlungen und Leitlinien

a) Empfehlung der Kommission für eine koordinierte Reaktion

Die Empfehlung der Kommission für eine koordinierte Reaktion auf grosse Cybersicherheitsvorfälle und -krisen[200] hält in den Erwägungen fest, dass eine wirksame Reaktion auf grosse Cybersicherheitsvorfälle und -krisen eine rasche und konstruktive Zusammenarbeit erfordert. Hierfür sind bereits im Voraus mögliche Massnahmen zu treffen, die Rollen und Zuständigkeiten zu definieren und eine gewisse Koordination einzuüben (Erw. 5).

Gemäss der Empfehlung sind Mitgliedstaaten und EU-Institutionen gehalten, einen EU-Rahmen für die Reaktion auf Cybersicherheitsvorfälle zu schaffen (Empfehlung 1), welcher die einschlägigen Akteure bestimmt und Standardarbeitsanweisungen abgibt; dabei sollte der Schwerpunkt auf dem unverzüglichen Austausch von Informationen und der Koordinierung der Reaktion liegen (Empfehlung 2).

Weiter empfiehlt die Kommission, dass die Mitgliedstaaten mit der ENISA zusammenarbeiten sollten, um eine gemeinsame Systematik zu erarbeiten und gestützt auf gemeinsame Muster für Lageberichte die Zusammenarbeit in Krisenzeiten zu erleichtern (Empfehlung 7).

198 Europäische Kommission, Revision of the Network and Information Security Directive: Questions and Answers, aufrufbar unter <https://digital-strategy.ec.europa.eu/en/revision-network-and-information-security-directive-questions-and-answers>.

199 *Ibid.*

200 Empfehlung (EU) 2017/1584 der Kommission vom 13. September 2017 für eine koordinierte Reaktion auf grosse Cybersicherheitsvorfälle und -krisen, ABl. L 239 vom 19.9.2017, 36–58.

Um die Wirksamkeit der im Bereich des Krisenreaktionsrahmens festgelegten Verfahren zu gewährleisten, empfiehlt die Kommission, diese Verfahren zu erproben und gegebenenfalls zu überarbeiten; wichtig ist, dass dabei auch Erfahrungen aus Übungen zur Cybersicherheit auf nationaler, regionaler, Unions- und NATO-Ebene sowie im Rahmen der Cyberdiplomatie zu berücksichtigen sind (Empfehlung 8).

Schliesslich sollen die Mitgliedstaaten und EU-Institutionen ihre Reaktionen auf grosse Cybersicherheitsvorfälle und -krisen regelmässig erproben und bei Möglichkeit auch den privaten Sektor einbeziehen (Empfehlung 9).

b) Leitlinien der EBA

Die EBA-Leitlinien für das Management von IKT- und Sicherheitsrisiken[201] legen für Finanzinstitute Massnahmen für das Management von Risiken fest; die Anforderungen der Leitlinien beziehen sich auf die Informationssicherheit, einschliesslich der Cybersicherheit.[202]

Die Leitlinien basieren auf dem Prinzip der Proportionalität, d.h. die Leitlinien sind nach Grösse, interner Organisation sowie der Art und dem Umfang der Finanzinstitute, der Komplexität und dem Risikogehalt ihrer Dienstleistungen und Produkte umzusetzen.[203]

Die EBA-Leitlinien verlangen von den Finanzinstituten eine angemessene interne Governance mit einem internen Kontrollrahmen für ihre IKT- und Sicherheitsrisiken; zudem erwarten die Leitlinien die Festlegung einer angemessenen Strategie, welche auch die Entwicklung der Finanzinstitute in Betracht zieht.[204]

Darüber hinaus fordern die EBA-Leitlinien, dass die Finanzinstitute ihre IKT- und Sicherheitsrisiken identifizieren und steuern können; sie sollen mit geeigneten Verfahren und Kontrollen sicherstellen, dass eine angemessene Ermittlung, Analyse, Messung, Überwachung, Verwaltung und Meldung der Risiken innerhalb der Grenzen der Risikobereitschaft des Finanzinstituts stattfindet.[205]

---

201 Europäische Bankenaufsichtsbehörde, EBA-Leitlinien für das Management von IKT- und Sicherheitsrisiken, EBA/GL/2019/04, November 2019.

202 EBA, 2021, 4.

203 EBA, 2021, 7.

204 EBA, 2021, 7 f.

205 EBA, 2021, 9.

Um die Sicherheit der Finanzinstitute aufrechterhalten zu können, verlangen die EBA-Leitlinien, dass die Finanzinstitute Überprüfungen, Bewertungen und Tests bzgl. der Informationssicherheit durchführen. Dies ermöglicht den Finanzinstituten, einerseits mögliche Schwachstellen zu ermitteln und andererseits die Robustheit und Wirksamkeit ihrer Informationssicherheitsmassnahmen zu prüfen. Darüber hinaus sind die Finanzinstitute gehalten, diese Tests regelmässig durchzuführen.[206]

c) Leitlinien der EIOPA

Die EIOPA kann gemäss Art. 16 Verordnung (EU) Nr. 1094/2010[207] Leitlinien und Empfehlungen für die zuständigen Behörden und die Finanzinstitute erlassen. Mit ihren Leitlinien[208] versucht die EIOPA, den «Marktteilnehmern Klarheit und Transparenz hinsichtlich der erwarteten Mindestanforderungen an Informations- und Cybersicherheit, d.h. eine Sicherheits-Baseline, bereitzustellen».[209]

Auch die EIOPA-Leitlinien basieren auf dem Prinzip der Proportionalität, d.h. die Leitlinien sind der Wesensart, dem Umfang und der Komplexität der Risiken angemessen anzuwenden.[210]

Die Leitlinien verlangen von den Unternehmen, dass sie ein Governance-System einführen, mit dem die Unternehmen ihre IKT- und (Cyber-)Sicherheitsrisiken angemessen beherrschen können (Leitlinie 2).[211]

Gemäss den Leitlinien sind die Unternehmen gehalten, Verfahren zur Gewährleistung der Vertraulichkeit, Integrität und Verfügbarkeit von IKT-Systemen und IKT-Diensten einzuführen; diese Massnahmen zielen darauf ab, Auswir-

206 EBA, 2021, 9 und 16.

207 Verordnung (EU) Nr. 1094/2010 des Europäischen Parlaments und des Rates vom 24. November 2010 zur Errichtung einer Europäischen Aufsichtsbehörde (Europäische Aufsichtsbehörde für das Versicherungswesen und die betriebliche Altersversorgung), zur Änderung des Beschlusses Nr. 716/2009/EG und zur Aufhebung des Beschlusses 2009/79/EG der Kommission, ABl. L 331 vom 15.12.2010, 48–83.

208 EIOPA, 2021. Europäische Aufsichtsbehörde für das Versicherungswesen und die betriebliche Altersversorgung, Leitlinien zu Sicherheit und Governance im Bereich der Informations- und Kommunikationstechnologie, EIOPA-BoS-20/600, Frankfurt 2021.

209 EIOPA, 2021, 4.

210 EIOPA, 2021, 9.

211 *Ibid.*

kungen von Sicherheitsproblemen zu minimieren. Die Verfahren sollen u.a. potenzielle Anfälligkeiten identifizieren und Daten im Ruhezustand und bei der Übertragung verschlüsseln (Leitlinie 10).[212]

Darüber hinaus wird den Unternehmen empfohlen, Prozesse zur kontinuierlichen Überwachung von Aktivitäten, welche Auswirkungen auf ihre Informationssicherheit haben, festzulegen und umzusetzen (Leitlinie 11). Ähnlich wie die EBA-Leitlinien schreiben auch die EIOPA-Leitlinien vor, «eine Vielzahl unterschiedlicher Überprüfungen, Bewertungen und Tests in Bezug auf die Informationssicherheit durch[zu]führen, um die wirksame Ermittlung von Anfälligkeiten ihrer IKT-Systeme und IKT-Dienste sicherzustellen». Diese regelmässigen Tests sind – gemäss dem Grundsatz der Proportionalität – dem ermittelten Risikoniveau entsprechend häufig durchzuführen (Leitlinie 12).[213]

Die EIOPA-Leitlinien verlangen von den Unternehmen, eine Strategie für die Betriebskontinuität einzuführen und diese innerhalb des Unternehmens angemessen zu kommunizieren (Leitlinie 19). Leitlinie 20 erwähnt, dass im Rahmen der Betriebskontinuität die Unternehmen eine Business-Impact-Analyse durchführen sollten, damit sie bewerten können, inwiefern sie Betriebsausfällen ausgesetzt sind; gleichzeitig sollten sie ihre Systeme und Dienste so auslegen, dass sie Störungen und Ausfälle von kritischen Komponenten zu minimieren vermögen. In der Betriebskontinuitätsplanung ist zudem auch sicherzustellen, dass die Unternehmen innerhalb einer bestimmten Wiederherstellungszeit reagieren können (Leitlinie 21).

Schliesslich ist innerhalb der Business-Impact-Analysen ein Reaktions- und Wiederherstellungsplan auszuarbeiten, welcher die Integrität, Verfügbarkeit, Kontinuität und Wiederherstellung der kritischen Systeme, Dienste und Daten gewährleistet (Leitlinie 22); ferner sind diese Pläne auch regelmässig zu testen und die Tests zu dokumentieren (Leitlinie 23).

6. Datenschutz-Grundverordnung (DSGVO)

Die im Mai 2016 in Kraft getretene und seit Mai 2018 anwendbare Datenschutz-Grundverordnung (DSGVO) zielt darauf ab, das Datenschutzrecht im gesamten Binnenmarkt zu vereinheitlichen und den Einzelpersonen mehr Kontrolle über die Verwendung der personenbezogenen Daten zu geben. Alle

212 EIOPA, 2021, 14.

213 EIOPA, 2021, 15.

Organisationen, die personenbezogene Daten kontrollieren oder verarbeiten und innerhalb der EU tätig sind oder Waren in die EU verkaufen, unterstehen der DSGVO.

Die DSGVO ist auf die Verarbeitung der personenbezogenen Daten anwendbar, womit praktisch jede Art der Datennutzung abgedeckt ist (u.a. die Erhebung, der Abruf, die Veränderung, die Speicherung und die Vernichtung von Daten).

Als allgemeiner Rechtsakt ist die DSGVO auch für Finanzinstitute bindend, zumal diese eine grosse Menge an Daten kontrollieren und verarbeiten.[214] Gemäss Art. 7 DSGVO ist für die Verarbeitung der personenbezogenen Daten eine Einwilligung der betroffenen Person erforderlich. Gemäss Art. 12 ff. DSGVO müssen die Finanzinstitute alle Mitteilungen, die sich auf die Verarbeitung beziehen, in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache übermitteln.

Darüber hinaus enthält die DSGVO auch Anforderungen an die Datensicherheit und den Umgang mit Datenschutzverletzungen. Vorgesehen ist eine sog. «Data Breach Notification»: Gemäss Art. 33 DSGVO sind die Finanzinstitute verpflichtet, die Verletzung des Schutzes personenbezogener Daten unverzüglich der Aufsichtsbehörde zu melden. Zudem haben sie die betroffene Person unverzüglich von der Verletzung zu benachrichtigen, falls die Verletzung des Schutzes personenbezogener Daten voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen zur Folge hat (Art. 34 DSGVO).[215] Ausserdem ist der Verantwortliche verpflichtet, vorab eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durchzuführen, falls die Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat (Datenschutz-Folgenabschätzung gemäss Art. 35 DSGVO).

Die Finanzinstitute sind überdies verpflichtet, interne Strategien festzulegen und Massnahmen zu ergreifen, um insbesondere den Grundsätzen des Datenschutzes durch Technik («data protection by design») und den datenschutzfreundlichen Voreinstellungen («data protection by default») Genüge zu tun (Art. 25 DSGVO).[216]

214 Vgl. ferner *Krüger/Brauchle*, 2021, 11.

215 Vgl. ferner Kap. III.B.2.b).

216 Vgl. hierzu auch DSGVO, Erw. 78.

E. Weitere Rechtsordnungen

1. Vereinigtes Königreich (UK)

a) Behördenorganisation

Im Vereinigten Königreich regulieren verschiedene Behörden die Aspekte der Cybersicherheit im Finanzwesen. Für die Banken und Finanzinstitute gilt zu beachten, dass sie nicht unter die Network and Information Systems Regulations (NIS Regulations)[217] fallen, sondern anderen Regelungen (z.B. dem FCA Handbook) unterstehen.[218]

Das National Cyber Security Centre (UK NCSC) ist eine wichtige Anlaufstelle für Unternehmen, um zu gewährleisten, dass sie ihren Verpflichtungen im Bereich der Cybersicherheit nachkommen. In Zusammenarbeit mit den Finanzbehörden, der Industrie, der National Crime Agency (NCA) und UK Finance hat die UK NCSC spezifisch für den Finanzsektor das Financial Sector Cyber Collaboration Centre (FSCCC), einen Zusammenschluss von über 40 Unternehmen, ins Leben gerufen. Die FSCCC untersucht und koordiniert die Reaktion auf Cybervorfälle, die potenzielle Auswirkungen auf den Finanzsektor haben können.[219]

Darüber hinaus reguliert und beaufsichtigt die Bank of England als Zentralbank des Vereinigten Königreichs die Finanzdienstleistungsunternehmen über die Prudential Regulation Authority (PRA); sie bemüht sich zudem, die operative Resilienz des Finanzsektors zu stärken.[220] Die Financial Conduct Authority (FCA) ist für die Aufsicht der Finanzinstitute zuständig, auferlegt ihnen regulatorische Anforderungen und verfügt folglich über mehr Einfluss über die Finanzinstitute als z.B. das Information Commissioner's Office (ICO). Trotzdem haben die Finanzinstitute auch die Vorgaben des ICO zu befolgen, welches für die allgemeinen Datenschutzregulierungen im Vereinigten Königreich zuständig ist.[221]

---

217 The Network and Information Systems Regulations 2018 vom 19. April 2019 (UK Statutory Instruments, 2018 No. 506; Stand am 20. Januar 2021, aufrufbar unter <https://www.legislation.gov.uk/uksi/2018/506>).

218 *Burnett*, 2021, 9; *Parker/Charnock*, 2020, 70; *Long/Scali*, 2019, 14.

219 UK NCSC, 2021.

220 *Bank of England*, 2021.

221 *Long/Shankar*, 2021, 1 f.; *Parker/Charnock*, 2020, 70; *Long/Blythe*, 2020, 444.

b) FCA Handbook

aa) FCA-Prinzipien und FCA-Rules

Weder England noch Wales haben ein umfassendes Cybersicherheitsgesetz;[222] die Cybersicherheit ist vielmehr auf verschiedene Arten reguliert. Die FCA setzt bei der Regulierung des Finanzsektors auf FCA-Prinzipien und FCA-Rules im FCA Handbook.[223] Im Bereich der Cybersicherheit und Cyber-Resilienz sind insbesondere folgende Prinzipien und Regelungen zu beachten:[224]

- Principle 3 der Principles for Business: Das Unternehmen muss mit angemessener Sorgfalt dafür sorgen, dass es seine Geschäfte verantwortungsbewusst und wirksam organisiert sowie kontrolliert; gleichzeitig haben die Unternehmen über angemessene Risikomanagementsysteme zu verfügen;
- Principle 11 der Principles for Business: Das Unternehmen muss mit seinen Aufsichtsbehörden offen und kooperativ sein sowie der zuständigen Aufsichtsbehörde in angemessener Weise alles mitteilen, was das Unternehmen betrifft und wovon die Aufsichtsbehörde vernünftigerweise Kenntnis erwarten würde;
- Senior Management Arrangements, Systems and Controls (SYSC) 3.1.1: Das Unternehmen muss mit angemessener Sorgfalt für die Einrichtung und Aufrechterhaltung von Systemen und Kontrollen sorgen, die seiner Geschäftstätigkeit entsprechen; diese Anforderungen erstrecken sich auch auf Fragen der Cybersicherheit;
- SYSC 3.2.6: Das Unternehmen muss angemessene Sorgfalt walten lassen, um wirksame Systeme und Kontrollen einzurichten und aufrechtzuerhalten, welche die Einhaltung der geltenden Anforderungen und Standards im Rahmen des Regulierungssystems gewährleisten und dem Risiko entgegenwirken, dass das Unternehmen zur Förderung der Finanzkriminalität missbraucht wird;

---

222 *Parker/Charnock*, 2020, 69.

223 Das FCA Handbook ist aufrufbar unter <https://www.handbook.fca.org.uk/handbook>.

224 FCA Handbook; vgl. ferner *Norton Rose Fulbright*, 2021; *Wright/Dunphy-Moriel*, 2021; *Long/Shankar*, 2021, 8; *Parker/Charnock*, 2020, 69 und 71; *Long/Blythe*, 2020, 444.

- SYSC 13.7: Das Unternehmen muss Verfahren und Kontrollen für das Management operationeller Risiken einrichten und aufrechterhalten, um die Sicherheit der Informationssicherheitssysteme und IT-Systeme zu gewährleisten;
- SUP 15.3.1: Das Unternehmen muss die FCA sofort benachrichtigen, wenn es feststellt oder über Informationen verfügt, die vernünftigerweise vermuten lassen, dass eine der folgenden Situationen eingetreten ist, eingetreten sein könnte oder in absehbarer Zukunft eintreten könnte:
  - Situation, in welcher das Unternehmen eine oder mehrere der «threshold conditions» nicht erfüllt;
  - Angelegenheit, die erhebliche negative Auswirkungen auf den Ruf des Unternehmens haben könnte;
  - Angelegenheit, welche die Fähigkeit des Unternehmens beeinträchtigen könnte, weiterhin angemessene Dienstleistungen für ihre Kunden zu erbringen, und die einen schwerwiegenden Schaden für einen Kunden des Unternehmens verursachen könnte;
  - Angelegenheit bzgl. des Unternehmens, die zu schwerwiegenden finanziellen Folgen für das Finanzsystem des Vereinigten Königreichs oder für andere Firmen führen könnte.

Zudem empfiehlt die FCA, dass die Unternehmen bei der Ausarbeitung ihrer Cybersicherheitsstrategie auf die Erfahrungen der bewährten Praxis und das Wissen bereits bestehender Standards, wie z.B. das NIST Framework, die 10 Steps to Cyber Security[225] bzw. Cyber Essentials der UK NCSC[226] oder die NIS Directive der UK NCSC,[227] zurückgreifen.[228]

225 UK NCSC, 10 Steps to Cyber Security, aufrufbar unter <https://www.ncsc.gov.uk/collection/10-steps>.

226 UK NCSC, About Cyber Essentials, aufrufbar unter <https://www.ncsc.gov.uk/cyberessentials/overview>.

227 UK NCSC, NCSC CAF guidance, aufrufbar unter <https://www.ncsc.gov.uk/collection/caf>.

228 FCA, 2019, 6; vgl. ferner Soft Law Kap. II.D und III.F.

Darüber hinaus hat die FCA auf ihrer Website Principle 11 der Principles for Business im Zusammenhang mit Cybervorfällen näher erläutert. Die FCA legt fest, dass ein Unternehmen wesentliche Cybervorfälle melden muss; gemäss der FCA ist ein Vorfall wesentlich, wenn er:[229]

- Zu einem erheblichen Verlust von Daten oder der Verfügbarkeit oder Kontrolle seiner IT-Systeme führt;
- Eine grosse Anzahl von Opfern betrifft;
- Zu einem unbefugten Zugriff auf die Informations- und Kommunikationssysteme des Unternehmens oder zum Vorhandensein von Schadsoftware auf diesen Systemen führt.

bb) Herangehensweise der FCA

Mit der Umsetzung dieser Prinzipien und Regeln zielt die FCA (zusammen mit der PRA) darauf ab, dass alle Unternehmen eine Sicherheitskultur entwickeln, die vom Vorstand bis hin zu jedem Mitarbeitenden reicht. Die Unternehmen sollten in der Lage sein, ihre Informationswerte (Hardware, Software und Mitarbeitende) zu identifizieren und zu priorisieren, diese Werte zu schützen, Verstösse aufzudecken, auf Vorfälle zu reagieren und sich ständig weiterzuentwickeln, um neuen Bedrohungen entgegnen zu können.[230]

Neben den FCA-Principles und FCA-Rules veröffentlicht die FCA auch «weiche» Leitlinien («soft guidance») in Form von FCA-Reden oder dem Austausch von Ratschlägen («adivce-sharing»),[231] wie z.B. die Rede von Nausicaa Delfas,[232] in welcher darauf hingewiesen wird, dass die richtigen Cybergrundlagen für die Aufsichtsbehörde von entscheidender Bedeutung sind. Delfas hält auch fest, dass die Unternehmen bei ordnungsgemässer Umsetzung der *Cyber Essentials* oder der 10 *Steps to Cyber Security* etwa 80 Prozent der Cyberbedrohungen beseitigen könnten.

---

229 FCA, Operational Resilience, aufrufbar unter <https://www.fca.org.uk/firms/operational-resilience>.

230 *Norton Rose Fulbright*, 2021.

231 Vgl. *Norton Rose Fulbright*, 2021; *Hayes/Drury*, 2020.

232 Vgl. die im Materialienverzeichnis erwähnte Ansprache von *Delfas*, 2017.

Im Jahre 2018 hat die FCA zudem das Paper «Cyber and Technology Resilience: Themes from cross-sector survey 2017/2018»[233] veröffentlicht, welches in einigen grösseren Unternehmen einen Mangel an Cyber- und Technologiekenntnissen auf Geschäftsführungsebene feststellte. Bei einem Drittel der untersuchten Unternehmen ergab sich, dass sie keine regelmässigen Cyberbewertungen durchführen.[234]

c) PRA Rulebook

Als Teil der Bank of England kann auch die PRA die Finanzinstitute regulieren. Die PRA (bzw. auch die Bank of England) können ihre Reden, ähnlich wie die FCA, als «weiche» Leitlinien im Bereich der Cybersicherheit und Cyber-Resilienz veröffentlichen. Darüber hinaus hat die PRA im PRA Rulebook[235] acht Fundamental Rules[236], welche mit den Principles for Business der FCA vergleichbar sind, festgehalten:[237]

- Fundamental Rule 2: Das Unternehmen muss seine Geschäfte mit der gebotenen Sachkenntnis, Sorgfalt und Gewissenhaftigkeit ausführen;
- Fundamental Rule 5: Das Unternehmen muss über wirksame Risikostrategien und Risikomanagementsysteme verfügen;
- Fundamental Rule 6: Ein Unternehmen muss seine Aktivitäten verantwortungsbewusst organisieren und kontrollieren;
- Fundamental Rule 7: Das Unternehmen muss mit seinen Aufsichtsbehörden offen und kooperativ umgehen und der PRA in angemessener Weise alles mitteilen, was das Unternehmen betrifft und wovon die PRA vernünftigerweise Kenntnis erwarten würde.

Im Zusammenhang mit der Cyber-Resilienz werden die Fundamental Rules durch den Abschnitt Risk Control[238] des PRA Rulebook weiter ergänzt. Die

---

233 *Financial Conduct Authority* (FCA), Cyber and Technology Resilience: Themes from cross-sector survey 2017/2018, London 2018, aufrufbar unter <https://www.fca.org.uk/publication/research/technology-cyber-resilience-questionnaire-cross-sector-report.pdf>.

234 FCA, 2018.

235 Das PRA Rulebook ist aufrufbar unter <https://www.prarulebook.co.uk/rulebook/Home/Rulebook/21-02-2022>.

236 Die Fundamental Rules sind aufrufbar unter <https://www.prarulebook.co.uk/rulebook/Content/Part/211136/21-02-2022>.

237 Vgl. *Norton Rose Fulbright*, 2021.

238 Der Abschnitt Risk Control ist aufrufbar unter <https://www.prarulebook.co.uk/rulebook/Content/Part/214146/21-02-2022>.

Vorschriften in diesem Teil des PRA-Regelwerks betreffen die Risikokontrolle, den Risikoausschuss und Gruppenvereinbarungen. Sie werden durch Leitlinien in Form einer Reihe von PRA-Aufsichtserklärungen ergänzt (u.a. das Supervisory Statement 21/15: Internal Governance[239]). In dieser Aufsichtserklärung ist u.a. festgehalten, dass die PRA erwartet, dass die Geschäftskontinuitätspolitik eines Unternehmens die folgenden Punkte behandelt:

- Prioritäten für die Wiederherstellung der Geschäftstätigkeit des Unternehmens;
- Kommunikationsvorkehren für interne und externe Beteiligte (einschliesslich der zuständigen Aufsichtsbehörde, Kunden und Medien);
- Eskalations- und Einberufungspläne, welche die Verfahren zur Umsetzung der Pläne zur Aufrechterhaltung des Geschäftsbetriebs zusammen mit den entsprechenden Kontaktinformationen darlegen;
- Verfahren zur Validierung der Integrität der von der Störung betroffenen Informationen;
- Regelmässiges Testen der Geschäftskontinuitätspolitik in angemessener und verhältnismässiger Weise gemäss Rule 2.8 im Abschnitt General Organisational Requirements des PRA-Regelwerks.

d) CBEST und CQUEST

aa) *CBEST*

Für die Banken und Finanzmarktinfrastrukturen, die als Kernbestandteile des britischen Finanzsystems gelten, haben die britischen Behörden im Mai 2014 das freiwilliges Programm CBEST aufgelegt. Ziel des CBEST-Programms ist es, die Cyber-Resilienz zu verbessern und zu testen. Das Sector Cyber Team der Bank of England hat einen CBEST-Implementierungsleitfaden für CBEST-Teilnehmer und CBEST-Dienstleister entwickelt. Da dieser Implementierungsleitfaden bloss ein «guiding framework» darstellt, wird den Teilnehmern empfohlen, auch andere Leitfäden von CBEST, wie z.B. den Leitfaden für die Bewertung von Dienstleistungen und den Leitfaden zur Aufklärung von Cyberbedrohungen, zu konsultieren.[240]

239 PRA, 2017.

240 PRA, 2020, 2; *Bank of England*, 2021.

CBEST unterscheidet sich durch den «Intelligence-Led»-Ansatz von anderen Sicherheitstests, die derzeit im Finanzdienstleistungssektor durchgeführt werden. CBEST basiert auf «threat intelligence», ist weniger eingeschränkt und konzentriert sich auf die stärker ausgefeilten und hartnäckigeren Angriffe auf kritische Systeme und wesentliche Dienste. Der «Intelligence-Led»-Penetrationstestansatz ahmt die Handlungen von Cyberangreifern nach, die darauf abzielen, die wichtigen Unternehmensdienste einer Organisation zu beschädigen sowie die technologischen Anlagen und Prozesse zu stören.[241] Die Finanzinstitute beauftragen die Dienstleister von Penetrationstests (Penetration Test Service Provider, PTSP), welche unabhängige Unternehmen sind, ihre Tests zu planen und durchzuführen.[242]

Da CBEST ein von den Aufsichtsbehörden geleitetes Assessment ist, geben die Aufsichtsbehörden während der gesamten Beurteilung Leitlinien und Anweisungen vor und stellen sicher, dass das Assessment im Einklang mit dem CBEST-Framework durchgeführt wird; entweder die PRA, das Financial Market Infrastructure Directorate (FMID) der Bank of England oder die FCA leiten die CBEST-Bewertung. Bei doppelt regulierten Finanzmarktinstituten stellen sowohl die PRA als auch die FCA ein Team mit Cyber-Fachwissen und Projektmanagement auf.[243]

bb) CQUEST

Für Situationen, in denen die britischen Aufsichtsbehörden die Cyber-Resilienz eines «high-level» Unternehmens bewerten wollen, haben die PRA und die FCA einen Fragebogen entwickelt (CQUEST). CQUEST besteht aus Multiple-Choice-Fragen, die verschiedene Aspekte der Cyber-Resilienz abdecken.[244] Die Antworten liefern eine nützliche Momentaufnahme der Cyber-Resilienz eines Unternehmens und zeigen Bereiche auf, die weiterzuentwickeln sind.[245]

---

241 PRA, 2020, 3; CREST, 2019, 6; CREST, 2014, 1.

242 PRA, 2020, 8.

243 PRA, 2020, 7.

244 Mögliche Fragen des Multiple-Choice sind: Verfügt das Unternehmen über eine vom Vorstand genehmigte Cybersicherheitsstrategie? Wie identifiziert und schützt es seine kritischen Vermögenswerte? Wie wird ein Vorfall erkannt, wie wird darauf reagiert, wie wird der Geschäftsbetrieb wiederhergestellt und wie lernt das Unternehmen aus der Erfahrung?; vgl. *Bank of England*, 2021.

245 *Bank of England*, 2021.

e) Datenschutzregelungen

Die wichtigsten Gesetze im Rahmen des Datenschutzes im Vereinigten Königreich sind die sektorübergreifend (und somit auch für den Finanzsektor) anwendbare DSGVO des Vereinigten Königreichs (UK DSGVO)[246] und der Data Protection Act 2018 (DPA 2018).[247] Das Vereinigte Königreich hat den Inhalt der DSGVO der EU – mit wenigen technischen Änderungen – nach dem Austritt aus der EU mit dem DPA 2018 in nationales Recht umgesetzt. Weil der DPA 2018 nicht sektorspezifische Regelungen aufstellt, muss jeder, der personenbezogene Daten verarbeitet, die Datenschutzbestimmungen einhalten; dies trifft auf die meisten Unternehmen und Organisationen, unabhängig von ihrer Grösse, zu.[248]

Der DPA 2018 gilt neben der UK DSGVO und ergänzt deren Anwendung im Land; diese nationale Umsetzung war erforderlich, damit die DSGVO im britischen Kontext effektiv funktioniert (u.a. Befugnisse und Pflichten des Information Commissioner's Office [ICO]).[249] Die Regelung bzgl. der Meldung von Verletzungen der Datensicherheit («Data Breach Notification») richten sich weiterhin nach der DSGVO.[250]

Das ICO ist für die Überwachung der Anwendung der UK DSGVO und des DPA 2018 zuständig und ergreift Durchsetzungsmassnahmen gegen Organisationen, welche diese Rechtsvorschriften nicht einhalten.[251]

---

246 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (United Kingdom General Data Protection Regulation; Regulations originating from the EU, 2016 No. 679).

247 Data Protection Act 2018 vom 23. Mai 2018 (UK Public General Acts, 2018 c. 12, Stand am 19. August 2018).

248 *Blair/Lloyd/Sussman/Nonninger*, 2021, 2.

249 *Long/Shankar*, 2021, 1; *Blair/Lloyd/Sussman/Nonninger*, 2021, 2; *Parker/Charnock*, 2020, 68 f.; *Long/Blythe*, 2020, 426.

250 Vgl. hierzu Kap. III.B.2.b).

251 *Blair/Lloyd/Sussman/Nonninger*, 2021, 2; *Parker/Charnock*, 2020, 68 f.; *Long/Blythe*, 2020, 426.

2. Vereinigte Staaten von Amerika (USA)

a) Behördenorganisation

Die Cybersicherheit ist in den USA durch eine Mischung aus allgemein anwendbaren Bundesgesetzen, sektorspezifischen Bundesgesetzen, allgemein anwendbaren einzelstaatlichen Gesetzen und sektorspezifischen einzelstaatlichen Gesetzen sowie durch Normen des Gewohnheitsrechts, die sich aus Gerichtsentscheidungen ergeben haben, geregelt. Allgemein geltende Bundesgesetze legen den Informationsaustausch mit der Regierung und bestimmte Handlungen wie Hacking oder das unrechtmässige Abfangen elektronischer Kommunikationen fest; andere Bundesgesetze schreiben spezifische Regeln vor, die nur für bestimmte Unternehmen in kritischen Infrastruktursektoren (z.B. im Finanzsektor) gelten.[252]

Da in den USA weder ein umfassendes Gesetz für die Cybersicherheit noch ein umfassendes Gesetz für Finanzinstitute existiert, beaufsichtigen zahlreiche Aufsichtsbehörden den Finanzdienstleistungssektor je nach Art des beaufsichtigten Unternehmens und des Finanzprodukts bzw. der Finanzdienstleistung. Als Aufsichtsbehörde agieren die Commodity Futures Trading Commission (CFTC), das Consumer Financial Protection Bureau (CFPB) und die Federal Trade Commission (FTC);[253] die FTC kommt der Rolle einer Aufsichtsbehörde für den Verbraucherschutz in den USA am nächsten.[254]

In den USA hat die Securities and Exchange Commission (SEC) – und insbesondere ihr Office of Compliance Inspections and Examinations (OCIE), das für bestimmte registrierte Berater, Broker-Dealer und Fonds zuständig ist – eine führende Rolle bei der Förderung von Cybersicherheitsmassnahmen im Finanzdienstleistungssektor übernommen.[255]

Selbstregulierungsagenturen wie die Financial Industry Regulatory Authority (FINRA) und die National Futures Association (NFA) haben ebenfalls Vorschriften für die Cybersicherheit erlassen.[256]

---

252 *McNicholas/Angle/Faircloth*, 2021, 1; *Sussman/Tabatabai/Downey/Boyle*, 2021, 2; *McNicholas/Angle*, 2020, 221; *Raul/Tapia*, 2020, 456 ff.

253 *McNicholas/Angle/Faircloth*, 2021, 4 f.; *Raul/Tapia*, 2020, 459 und 472.

254 *Raul/Tapia*, 2020, 456.

255 *McNicholas/Angle/Faircloth*, 2021, 4 f.; *Raul/Tapia*, 2020, 471 f.

256 *McNicholas/Angle/Faircloth*, 2021, 4 f.; *McNicholas/Angle*, 2020, 223; *Raul/Tapia*, 2020, 471 ff.

b) Bundesgesetze

Vorliegend lässt sich nicht auf die verschiedenen bundesstaatlichen Gesetze in den USA eingehen. Immerhin ist zu erwähnen, dass alle 50 Bundesstaaten der USA sowohl eigene Datenschutzregelungen als auch eigene Cybersicherheitsregelungen erlassen haben.[257]

Auf Bundesebene gibt es in den USA den Federal Trade Commission Act (FTC Act)[258] und den Cybersecurity Information Sharing Act (CISA)[259], welche im Grundsatz die Cybersicherheit regeln. Darüber hinaus haben Präsident Obama und Präsident Trump verschiedene Executive Orders im Bereich der Cybersicherheit erlassen, welche u.a. das Department of Homeland Security und eine Reihe anderer Behörden angewiesen haben, konkrete Massnahmen zur Cybersicherheit und zum Schutz kritischer Infrastrukturen zu ergreifen. Diese Executive Orders haben zusätzlich das National Institute of Standards and Technology (NIST) verpflichtet, ein Framework für Cybersicherheit[260] zu entwickeln.[261]

Der FTC Act überträgt der FTC die Zuständigkeit für grundsätzlich alle geschäftlichen Handlungen in den USA, die den zwischenstaatlichen (oder internationalen) Handel und einzelne Verbraucher betreffen.[262] Obwohl der FTC Act nicht ausdrücklich den Datenschutz oder die Informationssicherheit regelt, legt die FTC den § 5(a) des FTC Act so aus, dass sie befugt ist, u.a. Vorgaben zum Datenschutz, zur Datensicherheit und zur Online-Werbung zu machen und Unternehmen zur Einführung von Sicherheitsmassnahmen zu verpflichten. Die FTC hat seit 2002 gegen mehr als 80 Unternehmen Durchset-

257 Vgl. *McNicholas/Angle/Faircloth*, 2021, 3; *Raul/Tapia*, 2020, 462 f.

258 An Act to create a Federal Trade Commission, to define its powers and duties, and for other purposes vom 26. September 1914 (Stand am 5. Januar 2021, 38 Stat. 717, Chapter 311, kodifiziert unter 15 U.S.C. §§ 41-58).

259 Cybersecurity Information Sharing Act of 2015, To improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes, vom 17. März 2015 (Stand am 28. Oktober 2015, 29 Stat. 2936, kodifiziert unter 6 U.S.C. §§ 1501–1510).

260 National Institute of Standards and Technology, Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1, aufrufbar unter <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf>.

261 Exec. Order No. 13873,84 F.R. 22689 (2019); Exec. Order No. 13800, 82 F.R. 22391 (2017); Exec. Order No. 13718, 81 F.R. 7441 (2016); Exec. Order No. 13636, 78 F.R. 11737 (2013).

262 Vgl. hierfür FTC, What We Do, aufrufbar unter <https://www.ftc.gov/about-ftc/what-we-do>.

zungsmassnahmen aufgrund des Versäumnisses, angemessene Sicherheitsmassnahmen zu treffen, ergriffen.[263] Diese Auslegung der FTC kommt einer allgemeinen nationalen Regelung der Cybersicherheit in den USA recht nahe.

Der CISA hat zwei Schwerpunkte: Erstens erlaubt der Rechtsakt den Unternehmen, den Netzwerkverkehr zu überwachen und auch Abwehrmassnahmen für ihre eigenen Systeme zu ergreifen. Zweitens fördert er den Austausch von Informationen über Cyberbedrohungen im privaten Sektor zwischen Unternehmen und der Regierung.[264]

Ferner regelt der Gramm-Leach-Bliley Act (GLBA)[265] den Datenschutz und die Sicherheit von Finanzdaten durch Standards, die festlegen, dass Finanzinstitute nicht öffentliche personenbezogene Informationen («nonpublic personal information») der Kunden schützen müssen (§ 501 GLBA). Die Finanzinstitute sind gemäss § 503 GLBA verpflichtet, die Verbraucher über ihre Grundsätze und Praktiken in Bezug auf die Offenlegung persönlicher Daten zu informieren; ohne diesen Hinweis dürfen sie weder direkt noch über ein verbundenes Unternehmen nicht öffentliche personenbezogene Daten an einen nicht verbundenen Dritten weitergeben (§ 502 GLBA).

c) Selbstregulierungen der Industrie

Verschiedene Interessenvertreter der Branche haben gemeinsam mit der Regierung, Wissenschaftlern und Vertretern des Datenschutzes eine Reihe von Co-Regulierungen[266] entwickelt, welche bereichsspezifische, solide Datenschutzmassnahmen vorsehen, die von der FTC nach § 5 FTC Act durchgesetzt werden können.[267] Dabei werden Rahmenwerke zur Cybersicherheit, wie z.B. das NIST Framework[268] und die ISO-27001-Standards, von US-Organisationen in Betracht gezogen und als massgebend angesehen.[269]

---

263 *McNicholas/Angle*, 2020, 221; *Raul/Tapia*, 2020, 456.

264 Vgl. auch *McNicholas/Angle*, 2020, 221; *Raul/Tapia*, 2020, 458.

265 Gramm-Leach-Bliley Act, An Act to enhance competition in the financial services industry by providing a prudential framework for the affiliation of banks, securities firms, and other financial service providers, and for other purposes vom 12. November 1999 (113 Stat. 1338, kodifiziert unter 12 U.S.C. § 24a, § 248b, § 1831v, § 1831w, § 1831x, § 1831y, § 1848a, § 2908, 15 U.S.C. § 80b–10a, 15 U.S.C. § 6801–6809, 15 U.S.C. § 6821–6827).

266 Vgl. hierzu Kap. II.D.

267 *Raul/Tapia*, 2020, 465.

268 Für einen detaillierteren Einblick in den Inhalt des NIST Framework vgl. Kap. II.C, welches sich näher mit den Empfehlungen des NIST Framework auseinandersetzt.

269 *McNicholas/Angle/Faircloth*, 2021, 10.

3. Singapur

a) Behördenorganisation

Drei verschiedene Behörden regulieren die Cybersicherheitsaspekte der Finanzinstitute in Singapur: Die Monetary Authority of Singapore (MAS), die Personal Data Protection Commission (PDPC) und die Cyber Security Agency of Singapore (CSA). Die MAS ist gleichzeitig Singapurs Zentralbank und Behörde für Finanzmarktregulierung; sie führt auch Untersuchungen und Kontrollen im Bereich der Cybersicherheit und deren Regulierung durch.[270] Gemäss dem Cybersecurity Act 2018[271] ist die CSA für den Schutz der kritischen Informationsinfrastrukturen – einschliesslich der Infrastrukturen im Bank- und Finanzwesen[272] – zuständig; deshalb entwickelt sie für die Infrastrukturbetreiber Strategien (Art. 5 lit. b Cybersecurity Act 2018) sowie Verhaltensvorschriften und Standards (Art. 5 lit. f und Art. 11 Cybersecurity Act 2018). Die PDPC ist zuständig für die Durchsetzung des Personal Data Protection Act 2012, der festlegt, dass die Übermittlung der Daten ins Ausland verboten (Art. 10 Abs. 3 Personal Data Protection Act 2012) sowie die Einwilligung zur Sammlung und Verarbeitung der Daten erforderlich ist (Art. 13 ff. Personal Data Protection Act 2012).

b) Cybersecurity Act 2018

Der Cybersecurity Act als allgemeine Cybersicherheitsregulierung ist am 5. Februar 2018 in Kraft getreten und strebt verschiedene Ziele an: Einerseits soll der Schutz für kritische Informationsinfrastrukturen («Critical Information Infrastructure», auch CII) gegen Cybervorfälle verstärkt werden, andererseits ist die CSA autorisiert, Cybersicherheitsgefahren zu verhindern bzw. darauf zu antworten. Das Gesetz beinhaltet auch Rahmenbedingungen für die CSA, um Informationen anfordern sowie den Schutz und Austausch solcher Informationen regeln zu können. Im fünften Teil regelt das Gesetz die Lizenzierung der Cybersicherheitsdienstleister.

---

270 *Carter/Crumpler*, 2019, 5.

271 Republic of Singapore, Government Gazette, Act Supplement, Cybersecurity Act 2018, Published by Authority, No. 9, 16. März 2018, aufrufbar unter <https://sso.agc.gov.sg/Acts-Supp/9-2018/>.

272 CSA, 2018. Cybersecurity Act, aufrufbar unter <https://www.csa.gov.sg/Legislation/Cybersecurity-Act>.

Mit dem Cybersecurity Act 2018 wurde auch die Position des Commissioner of Cybersecurity geschaffen, der die Cybersicherheit für CII überwacht (Art. 4 Abs. 1 und 2 Cybersecurity Act 2018). Der Commissioner kann nach Art. 7 Cybersecurity Act 2018 bestimmen, welche Computer bzw. Computersysteme als CII gelten und die Betreiber dieser Systeme den Bestimmungen des Cybersecurity Act 2018 unterwerfen. Die Betreiber – inklusive der Finanzinstitute – sind gehalten, im Rahmen der Cybersicherheit jährlich eine Risikoeinschätzung (Art. 15 Abs. 1 lit. b Cybersecurity Act 2018) und jedes zweite Jahr Cybersicherheits-Überprüfungen («audits») durchzuführen (Art. 15 Abs. 1 lit. a Cybersecurity Act 2018), alle erheblichen Cybersicherheitsvorfälle zu melden (Art. 14 Cybersecurity Act 2018) sowie alle weiteren Weisungen zu befolgen.

Bei der Erarbeitung des Cybersecurity Act 2018 hat sich die CSA bemüht, die internationalen Standards und Empfehlungen in das Gesetz einzuarbeiten und die Vorgaben mit nationalen, sektorspezifischen Regelungen (u.a. den Regelungen der MAS im Finanzsektor) zu harmonisieren.[273]

c) Technology Risk Management Guidelines (TRMG)

Das wichtigste Regelwerk im Bereich der Cybersicherheit für die Finanzinstitute in Singapur sind die von der MAS herausgegebenen Technology Risk Management Guidelines (TRMG)[274] mit den zugehörigen Rundschreiben. Die Technology Risk Supervision (TRS) ist mit der Aufsicht der Cybersicherheitskontrollen von über tausend Finanzinstituten beauftragt und überwacht die Einhaltung der Vorschriften. Das 14-köpfige TRS-Team setzt auf einen risikobasierten Ansatz, d.h. die Einhaltung der TRMG durch Finanzinstitute mit geringem Risiko erfolgt über ein Selbsteinschätzungsverfahren («self-report»); diese sind gehalten, eine Reihe von Fragen zu beantworten und die Ergebnisse einem externen IT-Prüfunternehmen zu übermitteln. Bei Finanzinstituten mit hohem Risiko führt das TRS-Team jährliche Besuche und vierteljährliche Inter-

273 *Ang*, 2021, 99 ff.; *Carter/Crumpler*, 2019, 8; vgl. ferner *Mohit Sagar*, Singapore's Cybersecurity Bill passed into law, Minister addresses concerns, aufrufbar unter <https://opengovasia.com/singapores-cybersecurity-bill-passed-into-law-minister-addresses-concerns/>.

274 Monetary Authority of Singapore (MAS), Technology Risk Management Guidelines, Singapur 2021.

views durch. Die Einteilung in Finanzinstitute mit geringem bzw. hohem Risiko erfolgt nach den Comprehensive Risk Assessment Framework and Techniques (CRAFT)[275] der MAS.[276]

Die Finanzinstitute sind – im Einklang mit den Grundsätzen der Cybersicherheit und Cyber-Resilienz – auch verpflichtet, eine Rahmenverordnung für das Risikomanagement mit angemessenen Governance-Strukturen zu erlassen. Die Rahmenverordnung soll die Themen Risikoidentifizierung («risk identification»), Risikoeinschätzung («risk assemsment»), Risikobehandlung («risk treatment») sowie Risikoüberwachung, -bewertung und -berichterstattung («risk monitoring, review and reporting») beinhalten und die Eignung der Regeln stetig überprüfen, da sich die Cybersicherheit in einem schnell ändernden Umfeld befindet (Art. 4 TMRG).[277]

Damit bei einem allfälligen Cybervorfall die Systeme trotzdem verfügbar bleiben, machen die TMRG auch Vorgaben zur Cyber-Resilienz. Die Finanzinstitute sind gehalten, ihre Systeme und Netzwerkarchitektur periodisch zu überprüfen und interne sowie externe Abhängigkeiten zu analysieren, um die «single point of failure» bestimmen zu können (Art. 8.1 TRMG). Da Cybervorfälle auch einen «disaster recovery plan» erfordern, sind die Finanzdienstleister verpflichtet, diesen mindestens einmal jährlich zu überprüfen und zu aktualisieren (Art. 8.2 TRMG); darüber hinaus ist der «disaster recovery plan» regelmässig zu testen, um seine Wirksamkeit einschätzen zu können (Art. 8.3 TRMG). Hierfür sind häufige Backups erforderlich, auf die man bei einem Cybervorfall allenfalls zurückgreifen kann und so keinen Komplettverlust des Systems erleidet (Art. 8.4 TRMG). Die Datenzentren selbst müssen Naturereignisse sowie physische Gefahren ausstehen können (Art. 8.5 TRMG).

Die Finanzinstitutionen sollen gemäss Art. 3.1.7 lit. g und Art. 15 TRMG unabhängige Überprüfungsprozesse («audit procedures») für alle kritischen IT-Betriebe einführen; die Häufigkeit der Kontrollen ist nach der Kritikalität des IT-Betriebs und der IT-Informationen zu bestimmen (Art. 15.1.3 TRMG). Darüber hinaus sind die Finanzinstitute auch verpflichtet, jährliche Penetrati-

275 MAS, 2015. Monetary Authority of Singapore (MAS), Comprehensive Risk Assessment Framework and Techniques, Impact Assessment, CRAFT Risk Assessment, April 2007 (revised in September 2015), Singapore 2015.

276 *Carter/Crumpler*, 2019, 5; vgl. ferner *Kin/Alfred/Pichlmaier*, 2020, 177 f.

277 Vgl. hierzu auch Kap. I und ferner II.D.

onstests als Kombination von Blackbox-[278] und Greybox-Tests[279] durchzuführen (Art. 13.2 TRMG). Sowohl «White Hat Hacker» als auch automatisierte Bug-Bounty-Programme sollen Schwachstellen des Systems ausfindig machen (Art. 13.2.2 TRMG). Obwohl die MAS im Rahmen des Enforcement auch Strafen für die Nichtbeachtung der Regeln aussprechen kann, greift sie darauf fast nur bei grösseren Datenpannen zurück. Die Durchsetzung erfolgt in der Regel durch Mahnschreiben oder Kommentare in den verbesserungswürdigen Bereichen.[280]

d) Notice on Cyber Hygiene

Neben den TRMG hat die MAS im Jahre 2019 die Notice on Cyber Hygiene[281] erlassen, welche ein rechtlich verbindliches Fundament für alle Finanzinstitute darstellt. Die Notice on Cyber Hygiene beinhaltet folgende Elemente (Art. 4 Notice on Cyber Hygiene):

- Einführung und Umsetzung solider Sicherheitsmassnahmen für IT-Systeme;
- Rechtzeitige Durchführung von Sicherheitsupdates;
- Einführung von Sicherheitsmassnahmen zur Verhinderung von nicht autorisiertem Zugang;
- Einführung von Massnahmen zur Verringerung der Risiken durch Malware;
- Besondere Sicherung der Systemkonten mit privilegiertem Zugang;
- Verstärkung der Benutzerauthentifizierung für kritische Systeme und Systeme mit Zugang zu Kundeninformationen.

278 Bei Blackbox-Tests kennt der Tester die Umgebung nicht, mit Ausnahme der IP-Adressen und der URLs.

279 Bei Greybox-Tests sind Tests mit Anmeldedaten betroffen, d.h. der Tester hat dieselben Rechte wie ein normaler Kunde.

280 *Jacob/Loh*, 2021, 11; *Carter/Crumpler*, 2019, 5; vgl. ferner zur Bedeutung des Soft Law Kap. II.D und III.F.

281 MAS Notice No.: 655, Notice to banks in Singapore Banking Act (Cap. 19), Notice on Cyber Hygiene vom 6. August 2019.

e) Personal Data Protection Act (PDPA)

Neben dem Cybersecurity Act 2018 hat der Gesetzgeber in Singapur sektorübergreifend Angelegenheiten im Bereich des Datenschutzes im Personal Data Protection Act (PDPA)[282] reguliert.[283] Der PDPA ist nicht spezifisch auf Cybersicherheitsfragen zugeschnitten, aber regelt Fragen zur Cybersicherheit im weiteren Sinne. Die Unternehmen sind gehalten, Personendaten zu schützen, um unbefugten Zugriff, Verwendung, Änderung und ähnliche Risiken sowie den Verlust der Daten zu vermeiden (Art. 24 PDPA).

4. Hong Kong

a) Behördenorganisation

Die Hong Kong Monetary Authority (HKMA) und Hong Kong Securities and Futures Commission (HKSFC) sind für die Cybersicherheit im Finanzsektor zuständig. Die HKMA reguliert alle Finanzinstitute in Hong Kong und überwacht die Einhaltung der Hong Kong Banking Ordinance[284]; als Aufsichtsbehörde kann die HKMA auch an Finanzdienstleister gerichtete Richtlinien erlassen.[285] Als Regulator der Handelsdienstleister stellt die HKSFC Sicherheitsanforderungen an die lizenzierten Makler.[286]

Im Jahre 2015 hat das Hong Kong Financial Services Business-Continuity-Management Forum (HKFSBCM) in einer umfassenden Übung (Whole Industry Simulation Exercise [WISE]) einen systemischen Cybervorfall im Bankensektor in Hong Kong simuliert. Diese Übung hat erhebliche Defizite in den von der HKMA im Jahre 2003 erlassenen General Principles for Technology Risk Management[287] offenbart. Als Reaktion auf die WISE 2015 hat die HKMA ein Rundschreiben zum Risikomanagement im Kontext der Cybersicherheit veröffentlicht, das die Leitungspersonen der Finanzinstitute verpflichtet hat, die

---

282 Republic of Singapore, Government Gazette, Act Supplement, Personal Data Protection Act 2012, Published by Authority, No. 25, 7. Dezember 2012, aufrufbar unter <https://sso.agc.gov.sg/Act/PDPA2012>.

283 *Didenko*, 2020, 4; *Kin/Alfred/Pichlmaier*, 2020, 174 f.

284 (Hong Kong) Banking Ordinance vom 1. September 1986, T-2 Cap. 155, (Stand am 12. Dezember 2019), aufrufbar unter <https://www.elegislation.gov.hk/hk/cap155>.

285 *Crompton/Northcott/Buttoo* 2021, 9; *Tham*, 2020, 208 f.; *Carter/Crumpler*, 2019, 11.

286 *Crompton/Northcott/Buttoo* 2021, 9; *Carter/Crumpler*, 2019, 13 f.

287 HKMA, 2003.

Aufsicht mit Bezug auf die Cybersicherheit zu verstärken und die Auswertungen der Cybersicherheitskontrollen an einer vorgegebenen Benchmark zu messen.[288]

b) Cybersecurity Fortification Initiative der HKMA

Gestützt auf die Erkenntnisse aus WISE 2015 hat die HKMA im Mai 2016 die Cybersecurity Fortification Initiative (CFI) angestossen. Die CFI soll die Cyber-Resilienz der Finanzinstitute in Hong Kong verstärken und besteht aus drei Teilen: Cyber Resilience Assessment Framework (C-RAF), Professional Development Program (PDP) und Cyber Intelligence Sharing Platform (CISP).[289]

Das C-RAF stützt sich auf das CBEST-Rahmenregelwerk und ist aufgeteilt in zwei Teile der Selbsteinschätzung[290] sowie einen Teil «intelligence-led Cyber Attack Simulation Testing (iCAST)». Die Selbsteinschätzung basiert auf dem FFIEC Cybersecurity Assessment Tool, dem NIST Framework und der BIS/IOSCO Guidance on Cyber Resilience for Financial Market Infrastructures;[291] gemäss Appendix A, B und C des C-RAF sind die Banken gehalten, die Sicherheit der Systeme an über 300 Kontrollpunkten zu prüfen und einzuschätzen.[292]

Gemäss Kap. 4 des C-RAF («intelligence-led Cyber Attack Simulation Testing (iCAST)») sind realitätsnahe Penetrationstests vorzunehmen. Die Durchführung des iCAST ist in fünf Phasen aufgeteilt (Kap. 4.4 ff.): Sondierung («Scoping»), Analyse von Bedrohungsdaten («Analysing Threat Intelligence Analysis»), Testszenarien («Testing Scenarios»), Tests («Testing») sowie Berichterstattung («Reporting»).

Eine der grössten Herausforderungen für das C-RAF ist der Mangel an qualifizierten Sachverständigen und Gutachtern, weshalb die HKMA auf eine phasenweise Implementierung das C-RAF setzte.[293] Mit dem PDP als Trainings- und Zertifizierungsprogramm wollte die HKMA den Mangel an qualifizierten

---

288 HKMA, 2015, 2 ff. Die HKMA schlägt als mögliche Benchmarks die ISACA COBIT, SANS Top 20 Critical Security Controls, ISF Standard of Good Practice for Information Security oder die ISO/IEC 27000-Reihe vor.

289 HKMA, 2016.

290 Kap. 1 des C-RAF behandelt die «Inherent Risk Assessment» und Kap. 2 regelt die «Maturity Assessment».

291 *Carter/Crumpler*, 2019, 11.

292 Vgl. ferner *Carter/Crumpler*, 2019, 11 f.

293 HKMA, 2018.

Sachverständigen beheben und Talente im Bereich der Cybersicherheit fördern; hierfür hat die HKMA u.a. verschiedene Zertifizierungslisten herausgegeben.[294]

Der dritte Teil der CFI ist die CISP, eine Plattform, welche die Kommunikation und den Informationsaustausch bzgl. Cybersicherheit und Cybergefahren zwischen den Banken verbessern soll. Die HKMA hat die Plattform zusammen mit der Hong Kong Association of Banks (HKAB) sowie Hong Kong Applied Science and Technology Research Institute (HKASTRI) errichtet. Die CISP verblieb jedoch wegen Vertrauensbedenken im Stadium «work in progress», wird aber trotzdem als Erfolg angesehen.[295]

Nachdem die CFI bei den Finanzinstituten gut ankam, hat die HKMA im Jahre 2020 die CFI 2.0 eingeleitet. Die am 1. Januar 2021 in Kraft getretene CFI 2.0 hat das C-RAF auf den neusten Stand gebracht und die internationalen Entwicklungen im Bereich der Cybersicherheit aufgenommen. Darüber hinaus hat die HKMA beim PDP die Zertifizierungsliste erweitert.[296]

c) Personal Data (Privacy) Ordinance

Die PDPO[297] reguliert sektorübergreifend Angelegenheiten im Bereich des Datenschutzes und wird unter der Aufsicht des Office of the Privacy Commissioner for Personal Data umgesetzt. Wichtiger Bestandteil der PDPO sind die Data Protection Principles (DPP), die den Umgang mit personenbezogenen Daten regeln. Gemäss Schedule 1 Section 4 Principle 4 der PDPO haben die Datennutzer alle Massnahmen zu ergreifen, damit personenbezogene Daten gegen unbefugten oder versehentlichen Zugriff, Verarbeitung, Löschung, Ver-

294 *Carter/Crumpler*, 2019, 12 m.w.H.

295 Die HKASTARI hat eine ähnliche Plattform für die Versicherungs- und Maklerbranche errichtet (s. *Enoch Yiu*, Cybersecurity Platform to Expand to Hong Kong's Brokers and Insurers, South China Morning Post, 5. Juni 2017, aufrufbar unter <https://www.scmp.com/business/companies/article/2096975/cybersecurity-platform-expand-hong-kongs-brokers-and-insurers>); vgl. ferner *Carter/Crumpler*, 2019, 12 m.w.H.

296 HKMA, 2020.

297 (Hong Kong) Personal Data (Privacy) Ordinance vom 1. August 1996, E-2 Cap. 486 (Stand am 20. April 2018), aufrufbar unter <https://www.elegislation.gov.hk/hk/cap486!en-zh-Hant-HK.pdf?FROMCAPINDEX=Y>.

lust oder Verwendung geschützt sind. Obwohl die DPP rechtlich nicht bindend sind, ist deren Missachtung für Untersuchungen des Commissioner bzgl. lauteren Geschäftsgebarens nicht unbeachtlich.[298]

Die PDPO enthält zwar (noch) keine Pflicht zur Meldung von Verletzungen des Schutzes personenbezogener Daten («Personal Data Breach Notification»).[299] Verletzungen des Schutzes personenbezogener Daten sind dennoch meldepflichtig gestützt auf ein Rundschreiben der HKMA. Gemäss dem Rundschreiben sind die Unternehmen verpflichtet, bei schwerwiegenden Datenschutzvorfällen mit einer grossen Anzahl betroffener Kunden und einem Verlust sensibler Kundendaten den Vorfall schnellstmöglich der HKMA und den betroffenen Kunden zu melden.[300]

5. China

a) Behördenorganisation

In China regulieren die China Banking and Insurance Regulatory Commission (CBIRC) und die Cybersecurity Administration of China (CAC) die Cybersicherheit der Finanzinstitute. Die CAC ist für den Vollzug des «critical information infrastructure protection regime», das seinen Ursprung im Cybersecurity Law (CSL)[301] hat, zuständig. Die Banken sind – unter der Aufsicht der CBIRC – verpflichtet, in Guidelines festgelegte Sicherheitskontrollen und Risikomanagementverfahren zu befolgen. Als Teil der «Critical Information Infrastructure» (CII) haben sich die Banken auch an die neue Regelung für Informationssicherheitsmassnahmen zu halten. Hierzu müssen sie einerseits eigene Sicherheitskontrollen einführen, andererseits haben sie das sich stets entwickelnde System von Sicherheitsüberprüfungen für kritische Produkte und Dienstleistungen der CAC und Ministry of Public Security (MPS) zu übernehmen. Ferner sind die Banken verpflichtet, die Datenschutzbestimmungen des CSL einzuhalten.[302]

---

298 *Crompton/Northcott/Buttoo* 2021, 2; *Tham*, 2020, 210; *Carter/Crumpler*, 2019, 15; vgl. ferner zur Bedeutung des Soft Law Kap. II.D und III.F.

299 *Crompton/Northcott/Buttoo* 2021, 3; *Tham*, 2020, 222.

300 *HKMA*, 2014; vgl. ferner *Carter/Crumpler*, 2019, 15.

301 Cybersecurity Law of the People's Republic of China (中华人民共和国网络安全法) vom 7. November 2016 (Stand am 1. Juni 2017, englische Übersetzung aufrufbar unter <https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china/>).

302 *Chen*, 2021, 3; *Ning/Wu/Jiang*, 2021, 4 ff.; *Ning/Wu*, 2020, 62 ff.; *Carter/Crumpler*, 2019, 30.

Als Zentralbank von China ist die People's Bank of China (PBoC) für die Geldpolitik und Regulierung der Finanzinstitute zuständig. Primär unterstehen Themen wie die Aufsicht über die Mindestreserven der Banken, die Interbankenkredit- und Anleihemärkte oder die Devisenmärkte der Aufsicht der PBoC. Obwohl die PBoC nicht ausdrücklich für die Entwicklung und Implementierung der Regulierungen im Bereich des Riskmanagements für Finanzinstitute zuständig ist, hat sie den Auftrag, ein System für die interne Revision und Inspektion des Zentralbanksystems einzurichten.[303]

Die CBIRC[304] ist der massgebende Regulator für kommerzielle Banken in China; noch bevor die CBIRC als gemeinsame Organisation der China Banking Regulatory Commission (CBRC) und China Insurance Regulatory Commission (CIRC) existierte, hat die CBRC verschiedene Regulierungsrichtlinien zu Cybersicherheitskontrollen für chinesische Finanzinstitute erlassen. Am bedeutendsten sind die Commercial Bank Information Technology Risk Management Guidelines vom März 2009[305]. Diese Guidelines umfassen verschiedenste Aspekte der IT-Sicherheit, wie z.B. die Entwicklung und das Testen von Informationssystemen, die Planung der Geschäftskontinuität oder das Risikomanagement für Auslagerungen (IT-Outsourceing); die Guidelines sind auf die Rahmenbedingungen der Cybersicherheit sinngemäss anwendbar. Art. 15 der Guidelines hält die allgemeinen Grundsätze der Cybersicherheit fest:[306]

- Klassifizierung und Schutz der Daten;
- Entwicklung, Prüfung und Wartung von Informationssystemen;
- Betrieb und Wartung der Informationstechnologie;
- Zugangskontrolle (einschliesslich physischer Sicherheit);
- Anfertigung von Geschäftskontinuitätsplan und Notfallplan.

Auch in China ist eine Anlehnung an die internationalen Standards und «best practices» ersichtlich.[307]

---

303 *Carter/Crumpler*, 2019, 30 f.

304 Bis April 2018 existierten die China Banking Regulatory Commission (CBRC) und China Insurance Regulatory Commission (CIRC) noch als separate Einrichtungen.

305 *CBIRC*, 2009.

306 Vgl. Kap. II.A.1 für die Grundsätze der Cybersicherheit.

307 Der Bereich der Informationssicherheitskontrollen bspw. ist an die ISO-27000 Standards angelehnt, die IT-Governance an das COBIT-Framework, das IT-Management an die Information Technology Infrastructure Library (ITIL) und die «business continuity» an die die BIS-Prinzipien (vgl. *Carter/Crumpler*, 2019, 31 m.w.H.).

b) Cybersecurity Law (CSL)

Die Finanzinstitute unterstehen – neben den Regulierungen der CBIRC – auch den Regeln des CSL, da sie als CII zu klassifizieren sind (Art. 31 CSL).

Das CSL ist die Grundlage für das neue Aufsichtssystem im Bereich der Cybersicherheit in China. Das Gesetz wird fortlaufend durch neue Richtlinien ergänzt, wie z.B. die Administrative Measures on Cybersecurity Classification Evaluating Institutions 2018,[308] die Guiding Opinions on Implementing the Multi-Level Protection System for Cybersecurity and the Security Protection System for Critical Information Infrastructure 2020[309] oder die Notice on Launching the Pilot Multi-Level Protection Scheme for Cybersecurity of Industrial Internet Enterprises 2021.[310]

Das «Cybersecurity Multi-Layer Protection Scheme (MLPS)» verlangt – gemessen an der Bedeutung des Netzwerks für die nationale Sicherheit – verschiedene Stufen an Sicherheitskontrollen (Art. 21 CSL):

- Formulierung interner Sicherheitsmanagementsysteme und Bestimmung von Personen, die für die Cybersicherheit verantwortlich sind;
- Ergreifen technischer Massnahmen zur Verhinderung von Cyberangriffen, Computerviren oder anderen Handlungen, welche die Cybersicherheit gefährden können;
- Ergreifen technischer Massnahmen zur Überwachung und Aufzeichnung von Netzwerkbetriebszuständen und Cybersicherheitsvorfällen;
- Ergreifen von Massnahmen wie Datenklassifizierung, Sicherung wichtiger Daten und Verschlüsselung;
- Sonstige durch Gesetze oder Verwaltungsvorschriften festgelegte Verpflichtungen.

Die Geräte der kritischen Netzwerke zusammen mit anderen Produkten für die Cybersicherheit brauchen ein Sicherheitszertifikat einer qualifizierten Einrichtung oder haben die Anforderungen der Sicherheitskontrollen zu erfüllen (Art. 23 CSL). Darüber hinaus sind die Netzwerkbetreiber verpflichtet, Notfallpläne für Cybersicherheitsvorfälle aufzustellen; bei Auftritt eines Cybersi-

308 MPS, 2018; vgl. ferner zur Bedeutung des Soft Law Kap. II.D und III.F.

309 MPS, 2020.

310 MIIT, 2021.

cherheitsvorfalls müssen die Netzbetreiber in der Lage sein, unverzüglich den Notfallplan zu implementieren und entsprechende Abhilfemassnahmen zu ergreifen (Art. 25 CSL).

Die CII-Hersteller sind verpflichtet, die Stabilität der Geschäftsaktivitäten und die Aufrechterhaltung des Betriebs zu unterstützen (Art. 33 CSL). Die CII-Betreiber haben zudem – neben Art. 21 CSL – noch weitere Pflichten gestützt auf Art. 34 CSL zu erfüllen, wie z.B. die Einrichtung von spezialisierten Sicherheitsmanagementgremien, die regelmässige Durchführung von Schulungen zur Cybersicherheit oder die Ausarbeitung von Notfallplänen für Cybersicherheitsvorfälle. Ferner haben sich die CII-Betreiber einer nationalen Sicherheitsprüfung, organisiert von der CAC, zu unterziehen (Art. 35 CSL).

Gestützt auf das CSL sind am 1. September 2021 neue Regulierungen im Bereich der Sicherheit und des Schutzes der CII in Kraft getreten (CII-Regulierung China). Diese kürzlich erlassenen CII-Regulierungen bringen keine inhaltlichen Neuerungen, jedoch unterstehen die Adressaten einer strikteren Beurteilung als beim CSL.[311]

c) Datenschutzregelungen

Neben Anforderungen an das Risikomanagement und Cybersicherheitskontrollen regelt das CSL auch die Pflichten der CII mit Bezug auf Kunden- und Geschäftsdaten. Gemäss Art. 41 CSL sind die Netzwerkbetreiber verpflichtet, die Regeln zur Erhebung oder Nutzung der personenbezogenen Daten zu veröffentlichen sowie die Zustimmung der Personen einzuholen, deren Daten sie zu erheben beabsichtigen. In den Regeln müssen der Zweck, die Mittel und der Umfang der Erhebung oder Nutzung der Daten ausdrücklich angegeben sein. Diese Regelungen sind an das Datenschutzrecht anderer Rechtssysteme (z.B. Personal Data (Privacy) Ordinance von Hong Kong[312]) angelehnt.[313]

Das National Information Security Standardisation Technical Committee of China (TC260) hat im Mai 2018 sodann Spezifikationen für die Sicherheit persönlicher Daten veröffentlicht und diese im Oktober 2020 auf den neusten

311 *Albrecht*, 2021, 147; *Zhu*, 2021, 2.

312 Vgl. Kap. III.E.4.c).

313 *Protiviti*, 2018, 5; die Definition und Interpretation bzgl. personenbezogenen Daten sind im Bereich des Datenschutzes der DSGVO angelehnt (s. Vgl. *Carter/Crumpler*, 2019, 36).

Stand gebracht.[314] Diese Spezifikationen enthalten «best practices» zur Datenerhebung, -verwendung und -übermittlung sowie Anforderungen an Sicherheitskontrollen und Reaktionen nach einem Cybervorfall.[315]

Im September 2021 ist in China das neue Data Security Law (DSL) in Kraft getreten.[316] Da dieses Gesetz vom Ständigen Ausschuss der Volksrepublik China erlassen wurde, hat es einen höheren rechtlichen Rang als die Verwaltungsmassnahmen zur Datensicherheit.[317] Eine wichtige Änderung im DSL ist das System zur Klassifizierung der Daten; die Regierung kann verschiedene Arten von Daten nach deren Wichtigkeit klassifizieren und Sicherheitsstandards für die jeweiligen Klassen erlassen (Art. 21 ff. DSL). Die Verarbeiter von wichtigen Daten sind zudem verpflichtet, eine Stelle für Datensicherheit und Datenschutz einzurichten (Art. 27 DSL).

Seit November 2021 ist auch das Personal Information Protection Law (PIPL)[318] in Kraft. Das PIPL regelt die Bearbeitung von Personendaten, die Rechte der betroffenen Personen und die Anforderungen für die Datenübermittlung an Dritte; es hat grosse Ähnlichkeiten mit der DSGVO, denn das PIPL definiert ebenfalls allgemeine Grundsätze für die Bearbeitung von Daten, legt Informationspflichten und Governance-Pflichten fest, hat eine «Breach Notification» und beschränkt den Datentransfer ins Ausland.[319]

6. Japan

a) Behördenorganisation

In Japan ist hauptsächlich die Japanese Financial Services Agency (JFSA) für die Cybersicherheits-Regelungen im Finanzsystem zuständig. In den Comprehen-

314 TC260, 2020.

315 Vgl. *Ning/Wu/Jiang*, 2021, 10; *Carter/Crumpler*, 2019, 36.

316 *Albrecht*, 2021, 142.

317 *Albrecht*, 2021, 142; *Qi/Li*, 2021.

318 Personal Information Protection Law of China (中华人民共和国个人信息保护法) vom 1. November 2021 (Stand am 20. August 2021, englische Übersetzung aufrufbar unter <https://digichina.stanford.edu/work/translation-personal-information-protection-law-of-the-peoples-republic-of-china-effective-nov-1-2021/>).

319 PCPD, 2021, Privacy Commissioner for Personal Data, Personal Information Protection Law of the Mainland, Highlights of the Mainland's Personal Information Protection Law, aufrufbar unter <https://www.pcpd.org.hk/english/data_privacy_law/mainland_law/mainland_law.html>; vgl. auch *Albrecht*, 2022, Rn. 1 ff., insb. auch Rn. 4 für die Unterschiede zwischen dem PIPL und der DSGVO.

sive Guidelines for Supervision of Financial Market Infrastructures ist die Aufsicht über die Finanzinstitute geregelt.[320] Banken unterstehen zusätzlich auch der Aufsicht der Bank of Japan und sind verpflichtet, mit dem National Center of Incident Readiness and Strategy for Cybersecurity (JNISC) zusammenzuarbeiten, um die neusten Standards für «Critical Information Infrastructure» (CII) einhalten zu können.

Die JFSA hat eine eigene Abteilung für die Cybersicherheit mit 25 Experten, welche die Risiken überwachen und das Sicherheitsniveau der Finanzinstitute kontrollieren. Gemäss den Guidelines «Evaluation items for supervision of major banks, etc.»[321] sind die Finanzinstitute verpflichtet, eine angemessene Überwachung einzuführen, um allfällige Cybervorfälle zu erkennen, sowie ein Computer Security Incident Response Team (CSIRT) zu bilden. Ferner benötigen die Finanzinstitute einen Reaktionsplan auf Cybervorfälle, müssen Massnahmen im Falle eines grösseren Cybervorfalls ergreifen sowie eine mehrschichtige Verteidigung zum Schutz vor Cyberangriffen aufrecht halten. Die JFSA führt jedoch keine Penetrationstests oder Audits durch und gibt auch keine spezifischen, technischen Anforderungen an die Finanzinstitute, sondern verfolgt einen prinzipienbasierten Ansatz, der dem NIST Framework, den ISO-Standards und den Guidelines der Financial Industry Information Systems (FISC) angelehnt ist.[322] Der prinzipienbasierte Ansatz in der Cybersicherheit ist auch aus den Comprehensive Guidelines for Supervision of Financial Market Infrastructures ersichtlich.

Die Bank of Japan hat zwar keine aufsichtsrechtliche Befugnis zur Bankenaufsicht, aber sie kann Prüfungen vor Ort («on-site examination») oder Kontrollen ausserhalb der Banken («off-site monitoring») durchführen. Im Rahmen dieser Zuständigkeiten bewertet die Bank of Japan die operationellen Risiken der eingesetzten Systeme, einschliesslich der IT- und Cybersicherheitsrisiken.[323]

320 JFSA, 2018.

321 JFSA, 2014.

322 Vgl. *Carter/Crumpler*, 2019, 17.

323 Vgl. *Carter/Crumpler*, 2019, 18 m.w.H.

b) Regelungen für Critical Information Infrastructure (CII)

Im Jahre 2014 hat der japanische Gesetzgeber ein allgemeines Gesetz zur Cybersicherheit verabschiedet (Basic Act on Cybersecurity, BAC)[324], das u.a. auch an die Finanzinstitute gerichtet ist. Gestützt auf Art. 25 BAC ist die Leitstelle für die Cybersicherheits-Strategie (Cybersecurity Strategic Headquarters, JCSH) mit dem National Center of Incident Readiness and Strategy for Cybersecurity (JNISC) als Sekretariat der Leitstelle eingerichtet worden.[325]

Gemäss Art. 12 BAC ist die Regierung verpflichtet, eine Cybersicherheits-Strategie zu entwickeln, welche folgende Themen beinhalten muss (Art 12 Abs. 2 BAC):

- Grundlegende Ziele der Cybersicherheitspolitik;
- Sicherstellung der Cybersicherheit innerhalb der nationalen Verwaltungsorgane und anderer damit verbundener Organe;
- Unterstützung bei der Sicherstellung der Cybersicherheit bei CII-Betreibern, ihren Berufsverbänden und lokalen Regierungen;
- Weitere Angelegenheiten, die für die umfassende und wirksame Förderung der Cybersicherheitspolitik erforderlich sind.

Darüber hinaus ist die Regierung gemäss Art. 14 BAC gehalten, im Hinblick auf die Cybersicherheit der CII-Betreiber und anderen damit verbundenen Einrichtungen die erforderlichen Massnahmen zu ergreifen (z.B. Formulierung von Standards, Übungen und Schulungen, Förderung des Informationsaustauschs sowie andere freiwillige Aktivitäten).

In diesem Rahmen hat das JNISC im Jahre 2016 die General Framework for Secured IoT Systems[326] und im Jahre 2017 die Cybersecurity Policy for Critical Infrastructure Protection[327] veröffentlicht. Letztere schafft einen Rahmen für die Zusammenarbeit zwischen Regierung und CII-Betreibern zur Verbesse-

---

324 Basic Act on Cybersecurity (サイバーセキュリティ基本法) vom 12. November 2014 (Act No. 104 of 2014, englische Übersetzung vom 30. September 2015 aufrufbar unter <http://www.japaneselawtranslation.go.jp/law/detail/?printID=&re=02&vm=02&id=2760&lvm=01>.

325 Vgl. *Hayashi/Yukawa/Tsuta*, 2020, 122; *Carter/Crumpler*, 2019, 19.

326 *JNISC*, 2016.

327 *JCSH*, 2017.

rung des Cybersicherheitsschutzes. Gemäss diesen Richtlinien sollen die CII-Betreiber die Aufrechterhaltung der Cybersicherheit gewährleisten und diese kontinuierlich den neusten Entwicklungen anpassen.[328]

Zudem geht die JCSH davon aus, dass das Informationsaustauschsystem verbesserungswürdig ist; betont wird deshalb, dass die CII-Betreiber weiterhin mit anderen CII-Betreibern in Kontakt sein und Informationen zu allfälligen Cybervorfällen austauschen sollen.[329] Dieser Informationsaustausch hat auch sektorenübergreifend zu funktionieren, indem die neusten Techniken der Cyberangriffe analysiert und zur Verfügung gestellt werden, um ein Training anhand dieser Daten zu ermöglichen.[330]

Die JCSH stellt weiter fest, dass nicht mehr alle Cyberangriffe früh erkennbar und Vorbereitungen für sog. «zero-day attacks» nicht umfassend möglich sind. Immerhin sollen die CII-Betreiber die mit Blick auf Cybersicherheitsrisiken zu ergreifenden Massnahmen in ihrer Geschäftsstrategie verankern und auf der Grundlage der Ergebnisse der Risikobewertung strategische Vorkehrungen zur Risikobewältigung ergreifen.[331]

Im Rahmen der Cybersecurity Policy for Critical Infrastructure Protection macht das JNISC zudem Umfragen und führt bei den CII-Betreibern pro Jahr einen Besuch durch, um die Cybersicherheitsmassnahmen zu überprüfen und festzustellen, wie die Sicherheitsgrundsätze von den Betreibern umgesetzt wurden.[332] Da das JNISC jedoch keine Durchsetzungsbefugnis für ihre Guidelines hat, aktualisiert sie die Richtlinien mit den Erkenntnissen aus den Fragebögen und Besuchen.[333]

Neben dem JNISC sorgt auch das National Institute of Information and Communications Technology (JNICT) für die Cybersicherheit. Dem JNICT ist es zusätzlich als einzige Stelle erlaubt, unaufgeforderte Penetrationstests durchzuführen, obwohl sie ansonsten als unbefugter Zugriff auf die Systeme zu qualifizieren sind. Diese Ausnahme wurde gesetzlich festgehalten, um wirksame Tests mit Überraschungseffekt zu ermöglichen.[334]

---

328 *JCSH*, 2017, 12 f.

329 *JCSH*, 2017, 14 ff.

330 *JCSH*, 2017, 18 ff.

331 *JCSH*, 2017, 21 ff.

332 *JCSH*, 2017, 13.

333 Vgl. *Carter/Crumpler*, 2019, 19; *Bartlett*, 2019, 27; vgl. ferner zur Bedeutung des Soft Law Kap. II.D und III.F.

334 *Hayashi/Yukawa/Tsuta*, 2020, 121; *Soesanto*, 2020, 15.

c) Cybersecurity Management Guidelines

Das Ministry of Economy, Trade and Industry (JMETI) hat zusammen mit der Information-technology Promotion Agency (JIPA) im Jahre 2017 Cybersecurity Management Guidelines erlassen.[335] Gemäss diesen Guidelines sind Unternehmen gehalten, sich vor Cyberangriffen zu schützen; hierfür erwähnen sie die folgenden zehn einzuhaltenden wesentlichen Massnahmen:[336]

- Erkennen von Cybersicherheitsrisiken und Entwicklung von Massnahmen für das gesamte Unternehmen;
- Einführung von Prozessen für das Cybersicherheits-Risikomanagement;
- Sicherung von Ressourcen zur Durchführung von Cybersicherheitsmassnahmen;
- Erkennen möglicher Cybersicherheitsrisiken und Entwicklung von Plänen zur Bewältigung solcher Risiken;
- Aufbau einer Struktur zur Bewältigung von Cybersicherheitsrisiken (d.h. einer Struktur zur Erkennung, Analyse und Abwehr von Cybersicherheitsrisiken);
- Veröffentlichung eines Framework für Cybersicherheitsmassnahmen und eines entsprechenden Aktionsplans;
- Entwicklung eines Notfallsystems (z.B. Notfallkontakte, Handbuch für Erstmassnahmen) und Durchführung regelmässiger praktischer Übungen;
- Entwicklung eines Systems zur Beseitigung von Schäden, die durch Cybervorfälle verursacht wurden;
- Sicherstellen, dass die Unternehmen der gesamten Lieferkette für den Systembetrieb des Unternehmens (auch die Geschäftspartner und Outsourcing-Unternehmen) Sicherheitsmassnahmen ergreifen;
- Sammeln von Informationen über Cyberangriffe zum Informationsaustausch und Entwicklung eines Umfelds zur Nutzung dieser Informationen.

335 JMETI/JIPA, 2017; vgl. ferner *Hayashi/Yukawa/Tsuta*, 2020, 123.

336 Vgl. *Hayashi/Yukawa/Tsuta*, 2020, 123 f.

d) Datenschutzregelungen

Die Finanzinstitute müssen auch die Bestimmungen des Act on the Protection of Personal Information (APPI)[337] befolgen. Der APPI enthält Beschränkungen für die Erhebung, Verwendung und internationale Übermittlung von Daten und wird von der Personal Information Protection Commission durchgesetzt.[338]

Gemäss Art. 18 APPI haben Unternehmen, die personenbezogene Daten sammeln und verarbeiten, ihre Kunden über den Zweck dieser Datennutzung zu informieren. Verarbeitet ein Unternehmen personenbezogene Daten, ist es gemäss Art. 20 APPI verpflichtet, die notwendigen und angemessenen Massnahmen zur Sicherheitskontrolle personenbezogener Daten zu ergreifen; dies beinhaltet u.a. die Verhinderung des Verlusts oder der Beschädigung der von ihm verarbeiteten personenbezogenen Daten.

Darüber hinaus haben im Jahre 2018 die Europäische Union und Japan gegenseitig ihre jeweiligen Datenschutzregelungen als angemessen für den Umgang mit personenbezogenen Daten anerkannt und somit den freien Austausch der Daten zwischen Unternehmen in den beiden Rechtsordnungen ohne zusätzliche Kontrollen erlaubt (vgl. Durchführungsbeschluss (EU) 2019/419).

Die Meldung von Verletzungen der Datensicherheit («Data Breach Notification») ist nicht im APPI geregelt, sondern in den Guidelines der Personal Information Protection Commission;[339] die Unternehmen sind nur im Rahmen der guten Praxis gehalten, die betroffenen Personen sowie die Aufsichtsbehörden zu benachrichtigen.[340]

Für Finanzinstitute existieren zusätzlich die Guidelines Targeting Financial Sectors Pertaining to the Protection of Personal Information.[341] Gemäss diesen Guidelines sind die Finanzinstitute verpflichtet, Datenschutzverletzungen im Zusammenhang mit personenbezogenen Daten unverzüglich der Aufsichts-

337 Act on the Protection of Personal Information (個人情報の保護に関する法律) vom 30. Mai 2003 (Act No. 57 of 2003, englische Überstzung vom 21. Dezember 2016 aufrufbar unter <http://www.japaneselawtranslation.go.jp/law/detail/?id=2781&vm=2&re=02>).

338 *Matsuda/Adachi/Kukimoto*, 2021, 2; *Ishiara*, 2020, 263 f.; *Onodera/Tanaka/Shimamura*, 2019, 6; *Carter/Crumpler*, 2019, 17.

339 JPPC, 2016; JPPC, 2017; vgl. ferner *Ishiara*, 2020, 281; *Carter/Crumpler*, 2019, 21.

340 *Matsuda/Adachi/Kukimoto*, 2021, 11; *Onodera/Tanaka/Shimamura*, 2019, 7, 12 und 14; *Carter/Crumpler*, 2019, 21.

341 JPPC/JFSA, 2017.

behörde und den betroffenen Personen mitzuteilen und eine öffentliche Bekanntmachung über den Sachverhalt der Verletzung zu veröffentlichen.[342] Die Guidelines verlangen zudem, dass die Finanzinstitute Verfahren zum Schutz personenbezogener Daten einführen, einschliesslich organisatorischer, technischer und menschlicher Sicherheitskontrollmassnahmen.[343]

7. Indien

a) Behördenorganisation

In Indien ist hauptsächlich die Reserve Bank of India (RBI) und der Securities and Exchange Board of India (SEBI) für die Regulierung der Finanzinstitute zuständig. Die Banken müssen zusätzlich auch die Regelungen des National Critical Information Infrastructure Protection Centre (NCIIPC) zu den «Critical Information Infrastructure» (CII) einhalten. Die von der RBI, dem SEBI und des NCIIPC herausgegebenen Richtlinien verlangen von den Banken die Beachtung bestimmter Sicherheitsstandards, welche hauptsächlich auf der ISO/IEC-27000-Reihe basieren, sowie die Verpflichtung zu regelmässigen Schwachstellenbewertungen, Penetrationstests und Audits der Informationssicherheit.[344]

b) Bestimmungen im Bereich der Cybersicherheit

Indien hat kein umfassendes Gesetz zur Cybersicherheit erlassen; die Cybersicherheit ist zusammen mit der Meldung von Verletzungen der Datensicherheit sowie den Vorgaben zu Reaktionen auf Vorfälle im Information Technology Act 2000 (ITA)[345] und in den ITA-Rules[346] geregelt. Gemäss der Legaldefinition des ITA gilt der Schutz von «information, equipment, devices, computer, compu-

342 *Carter/Crumpler*, 2019, 21; *Iwase/Shibata/Terada*, 2018.

343 *Carter/Crumpler*, 2019, 21.

344 In Art. 8 ITA-Rules ist die ISO/IEC-27000-Reihe als möglicher internationaler Standard, worauf sich die Richtlinien stützen können und sollen, ausdrücklich erwähnt; vgl. ferner *Narayanan/Gupta*, 2021, 12; *Carter/Crumpler*, 2019, 22.

345 Information Technology Act, 2000 vom 9. Juni 2000 (No. 21 of 2000, aufrufbar unter <https://www.meity.gov.in/writereaddata/files/itbill2000.pdf>).

346 The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 vom 13. April 2011, aufrufbar unter <https://www.wipo.int/edocs/lexdocs/laws/en/in/in098en.pdf>.

ter resource, communication device and information stored therein from unauthorised access, use, disclosure, disruption, modification or destruction» als Cybersicherheit (Art. 2 Abs. 1 lit. nb ITA Amendment[347]).

aa) Regulierung für «Critical Information Infrastructure» (CII)

Im Rahmen des ITA (Art. 70 ITA) hat die indische Regierung das Indian Computer Emergency Response Team (CERT-In) als nationale Zentralstelle für Cybersicherheit eingerichtet, das folgende Aufgaben wahrnehmen soll (Art. 70B Abs. 4 ITA):

- Sammlung, Analyse und Verbreitung von Informationen über Cybervorfälle;
- Vorhersage und Warnung vor Cybervorfällen;
- Notfallmassnahmen zur Bewältigung von Cybervorfällen;
- Koordinierung von Massnahmen zur Bewältigung von Cybervorfällen;
- Herausgabe von Leitlinien, Empfehlungen, Hinweisen auf Schwachstellen und «White Papers» zu Informationssicherheitspraktiken, Verfahren, Prävention, Reaktion und Meldung von Cybervorfällen;
- Sonstige Aufgaben im Zusammenhang mit der Cybersicherheit.

Die Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules 2013 (CERT-In Rules)[348] schreiben vor, dass das CERT-In für die Reaktion auf Cybersicherheitsvorfälle zuständig ist (Art. 9 CERT-In Rules). Dieses ist auch befugt, Anweisungen an u.a. Dienstanbieter, Vermittler, Datenzentren, Körperschaften zu erteilen, um die Cybersicherheitsinfrastruktur im Land zu verbessern (Art. 10 CERT-In Rules). Das CERT-In ist für alle Formen von Cybersicherheitsfällen zuständig, der Umfang der Unterstützung hängt jedoch von der Art und

347 Die Autoren übersetzen die in indischen Gesetzen übliche Bezeichnung «section» als Artikel. Im Übrigen enthält Art. 2 ITA eine lange Liste an Definitionen bzw. Begriffserklärungen, welche im revidierten Gesetz reichlich ergänzt wurde; aus diesem Grund ergibt sich eine Unterteilung wie in Art. 2 Abs. 1 lit. nb ITA Amendment.

348 *MeitY*, 2014.

Schwere des Vorfalls ab (Art. 11 CERT-In Rules). In Indien hat das CERT-In auch sektorale CERTs eingerichtet, um Cybersicherheitsmassnahmen auf sektoraler Ebene umzusetzen.[349]

Für kritische Sektoren hat die Regierung gestützt auf Art. 70A ITA das National Critical Information Infrastructure Protection Centre (NCIIPC) als Knotenpunkt geschaffen. Die NCIIPC-Regeln und NCIIPC-Richtlinien zum Schutz der CII vor unbefugtem Zugriff, Veränderung, Nutzung, Offenlegung und Störung sollten dazu beitragen, eine sichere und widerstandsfähige Informationsinfrastruktur für kritische Sektoren im Land zu gewährleisten. Die wichtigsten Richtlinien des NCIIPC sind die Guidelines for Protection of Critical Information Infrastructure[350] aus dem Jahr 2015.

Diese Guidelines sind in fünf Gruppen von Kontrollen unterteilt, welche die Anforderungen an die Planung, die Umsetzung, den Betrieb, die Notfallwiederherstellung und die Berichterstattung für CII-Betreiber abdecken. Zu den Kontrollen gehören u.a. die Anforderungen an eine organisatorische Informationssicherheitspolitik, die Einbeziehung von Risikobewertungen in die Unternehmensstrategie, die Implementierung von Systemen zur Erkennung und Überwachung von Eindringlingen, die Erstellung von Notfallplänen für die Wiederherstellung im Katastrophenfall, die Durchführung von Penetrationstests auf allen Sicherheitsebenen sowie die regelmässige Überprüfung und Schwachstellenbewertung kritischer Systeme.[351]

bb) Sektorspezifische Regulierung

Im Bankensektor ist die RBI für den Erlass der Richtlinien zuständig; die RBI war bereits für die Ausarbeitung von Leitlinien für das Internet-Banking und die Verwaltung digitaler Unterlagen sowie von Richtlinien für die Meldung von Internet-Banking-Betrug und das Management von Outsourcing-Risiken verantwortlich. Die derzeitige Grundlage des Regulierungssystems der RBI ist das Cyber Security Framework in Banks[352] aus dem Jahr 2016. Es beschreibt die notwendigen Komponenten eines umfassenden internen Cybersicherheitsrahmens für Banken und aktualisiert die Leitlinien der RBI zu Informations-

349 Vgl. *CERT-In*, 2017. CERT-In, Four Sectoral Computer Emergency Response Teams to mitigate Cyber Security Threats in Power Systems, aufrufbar unter <https://pib.gov.in/newsite/PrintRelease.aspx?relid=159537>.

350 *NCIIPC*, 2015.

351 *NCIIPC*, 2015, 11 ff., insb. 15 ff.

352 *RBI*, 2016.

sicherheit, elektronischem Banking, technologischem Risikomanagement und Cyberbetrug. Das Framework verpflichtet die Banken zudem, einen Cyber Crisis Management Plan (CCMP) einzuführen und Informationen zu Cybervorfällen mit der RBI zu teilen.[353]

Im Jahre 2017 hat die Reserve Bank Information Technology Private Limited (ReBIT) ein Cyber Security Maturity Model (CMM) veröffentlicht, um indische Banken bei der Umsetzung des RBI-Framework zu unterstützen und die Einheitlichkeit bei der Übernahme von Standards zu fördern.[354] Das CMM bietet Banken ein Instrument zur Selbsteinschätzung von Risiken und zur Bewertung des Reifegrads ihrer Sicherheitskontrollen an.[355] Das CMM basiert auf dem NIST Cybersecurity Framework und ist so konzipiert, dass es mit anderen internationalen Standards wie COBIT 5.0 und ISO 27000 vereinbar ist.[356]

Für den Versicherungssektor ist die Insurance Regulatory and Development Authority (IRDAI) zuständig, welche die Guidelines on Information and Cyber Security for Insurers[357] erlassen hat. Diese Guidelines schreiben eine jährliche Schwachstellenbewertung und Penetrationstests sowie die Schliessung aller festgestellten Lücken innerhalb eines Monats vor.

c) Datenschutzregelungen

In Indien sind die Daten durch den ITA (und ITA Amendment) geschützt; dieses Gesetz enthält jedoch keine allgemeine Pflicht zur Meldung von Verletzungen des Schutzes von Daten («Data Notification Breach»). Gemäss Art. 12 CERT-In Rules sind Dienstleister, Vermittler, Datenzentren und Körperschaften, die mit sensiblen personenbezogenen Daten umgehen, verpflichtet, alle Cybersicherheitsvorfälle «so früh wie möglich» an das CERT-In zu melden.

Darüber hinaus liegt dem Parlament Indiens die Personal Data Protection Bill, 2019 vor, welche u.a. die Meldepflicht für Datenschutzverletzungen aufneh-

353 *RBI*, 2016, 4.

354 *ReBIT*, 2017.

355 *ReBIT*, 2017, 5.

356 *Carter/Crumpler*, 2019, 23; vgl. ferner zur Bedeutung des Soft Law Kap. II.D und III.F.

357 IRDAI, 2017.

men würde. Das Parlament verwies den Gesetzentwurf zur weiteren Prüfung an einen ständigen Ausschuss, der noch keine überarbeitete Fassung des Gesetzesentwurfs vorgelegt hat.[358]

F. Soft Law

Wie einleitend festgestellt, hat das Soft Law im Rahmen der Cybersicherheit eine bedeutende Stellung und spielt in der Entwicklung der jeweiligen nationalen Gesetze und deren Implementierung eine zentrale Rolle. Nachfolgend sind die wichtigsten als Soft Law zu qualifizierenden Standards und Vorgaben – also Sammlungen bewährter Verfahren, die von Experten erstellt wurden, um Unternehmen vor Cyberbedrohungen zu schützen und ihre Cybersicherheit zu verbessern – zu erwähnen:

Die ISO/IEC 27000-Reihe umfasst Normen zur Informationssicherheit, die von der International Organisation for Standardisation (ISO) und der International Electrotechnical Commission (IEC) veröffentlicht werden. Die Reihe enthält Best-Practice-Empfehlungen und definiert häufig verwendete Begriffe des Informationssicherheitsmanagements. Im Zusammenhang mit der ISO/IEC-27000-Reihe ist insbesondere der ISO-27032-Standard zu erwähnen, der Leitlinien für das Cybersicherheitsmanagement bereitstellt. Dieser internationale Standard bietet Anleitungen für die Bewältigung einer breiten Palette von Cybersicherheitsrisiken, einschliesslich der Sicherheit der Endgeräte von Benutzern, der Netzsicherheit und des Schutzes kritischer Infrastrukturen. Im Übrigen dienen diese Standards in verschiedenen Rechtsordnungen als Referenzpunkt für die Ausarbeitung der eigenen regulatorischen Vorgaben.[359]

Ferner sind im Rahmen der Internetstandards auch die die Domain Name System Security Extensions (DNSSEC) zu beachten, welche die Internet En-

---

358 *Bhargava Yuthika/Nair Sobhana K.*, More delays on Data Protection Bill as panel reopens debate, The Hindu, 8. September 2021, aufrufbar unter <https://www.thehindu.com/news/national/more-delays-on-data-protection-bill-as-panel-reopens-debate/article36344706.ece>; vgl. ferner *Narayanan/Chandhoke*, 2021, 2.

359 Vgl. für die ISO-Standards als Referenzpunkt die Kap. III.E.2.c), III.E.4.a), III.E.5.a), III.E.6.a), III.E.7.a) und III.E.7.b)bb); vgl. auch International Organisation for Standardisation (ISO), ISO/IEC 27000:2018, Information technology – Security techniques – Information security management systems – Overview and vocabulary, aufrufbar unter <https://www.iso.org/standard/73906.html>; International Organisation for Standardisation (ISO), ISO/IEC 27032:2012, Information technology – Security techniques – Guidelines for cybersecurity, aufrufbar unter <https://www.iso.org/standard/44375.html>.

gineering Task Force (IETF) herausgegeben hat. Die DNSSEC umfassen eine Reihe von Internetstandards, welche dem Schutz der Authentizität und Integrität der abgefragten DNS-Daten[360] dienen. Dadurch kann man bei DNS-Abfragen verifizieren, ob die DNS-Zonendaten identisch sind mit jenen Daten, die der Ersteller der Zone autorisiert hat; die DNSSEC können also verhindern, dass Verbindungen durch gefälschte DNS-Antworten auf einen falschen Server umgeleitet werden. Diese Extensions wurden entwickelt, um Anwendungen, die DNS nutzen, davor zu schützen, gefälschte oder manipulierte DNS-Daten zu akzeptieren.[361]

Auch die Bank for International Settlements (BIS) hat Leitlinien zur Cybersicherheit und Cyber-Resilienz veröffentlicht. Der Zweck des Leitfadens besteht darin, Finanzunternehmen eine Anleitung zur Verbesserung ihrer Cyber-Resilienz zu geben, welche als ergänzende Leitlinien zu den «Principles for Financial Market Infrastructures (PFMI)»[362] dienen und nicht darauf abzielen, zusätzliche Standards aufzuerlegen. Stattdessen enthält der Leitfaden zur Cybersicherheit und Cyber-Resilienz zusätzliche Details zu den Vorbereitungen und Massnahmen, die Finanzunternehmen zu ergreifen haben, um ihre Cyber-Resilienz zu verbessern; das Ziel ist, die eskalierenden Risiken, welche die Cyberbedrohungen für die Finanzstabilität darstellen, zu begrenzen.[363]

Darüber hinaus identifiziert die Weltbank im Bericht «Financial Sector's Cybersecurity: Regulation and Supervision»[364] gängige Konzepte und Praktiken und empfiehlt den Behörden des Finanzsektors deren Anwendung. Der Bericht definiert verschiedene Begriffe und gibt im Bereich der Cybersicherheit eine gemeinsame Sprache vor, um Missverständnisse zu vermeiden. Von Bedeutung ist u.a. auch die notwendige Koordination zwischen den Behörden des Finanzsektors und anderen staatlichen Stellen im Umgang mit Cyberrisiken.[365]

---

360 Das Domain Name System (DNS) beantwortet Anfragen zur Namensauflösung.

361 *IETF*, DNS Security Introduction and Requirements, aufrufbar unter <https://datatracker.ietf.org/doc/html/rfc4033>; vgl. auch *Switch*, DNSSEC, aufrufbar unter <https://www.nic.ch/de/security/dnssec/>.

362 *BIS/IOSCO*, 2012. Bank for International Settlements und International Organization of Securities Commissions, Principles for financial market infrastructures, 2012, aufrufbar unter <https://www.bis.org/cpmi/publ/d101a.pdf>.

363 *BIS/IOSCO*, 2016, 4 ff.

364 *World Bank Group*, Financial Sector's Cybersecurity: Regulation and Supervision, Washington 2018.

365 *World Bank Group*, Financial Sector's Cybersecurity: Regulations and Supervision, aufrufbar unter <https://openknowledge.worldbank.org/handle/10986/29378>.

Schliesslich hat auch die Europäische Zentralbank verschiedene Rahmenwerke veröffentlicht und Initiativen gestartet. Einerseits ist in diesem Zusammenhang das «European Framework for Threat-Intelligence Based Ethical Red teaming» (TIBER-EU) von Bedeutung.[366] Es ist ein Rahmenwerk, das kontrollierte, massgeschneiderte und geführte Übungen und Tests für die Systeme der Finanzunternehmen vorschlägt (u.a. Red-Team-Tests und Penetrationstests). Diese Tests ahmen die Aktivitäten, Taktiken, Techniken und Verfahren realer Bedrohungsakteure nach und simulieren realitätsgetreue Bedrohungen. Die Tests helfen den Finanzunternehmen, ihre Schutz-, Erkennungs- und Reaktionsfähigkeiten zu bewerten und zu verbessern.

Andererseits beabsichtigt die Europäische Zentralbank mit dem «Euro Cyber Resilience Board for pan-European Financial Infrastructures (ECRB)», die Cyber-Resilienz von paneuropäischen Finanzmarktinfrastrukturen, ihrer kritischen Dienstleister und des gesamten EU-Finanzsektors zu verbessern (Art. 1 ECRB-Mandat). Als Teil der Umsetzung hat die Europäische Zentralbank die «Cyber Information and Intelligence Sharing Initiative (CIISI-EU)»[367] veröffentlicht, welche im Rahmen der Cybersicherheit die Bedeutung der Kommunikation hervorhebt und als multilaterale Initiative den systematischen und strukturierten Austausch wichtiger strategischer, operativer und taktischer Cyber-Informationen und Cyber-Intelligenz erleichtern soll.[368]

G. Erkenntnisse aus der rechtsvergleichenden Darstellung

Die zuvor untersuchten Rechtsordnungen weisen verschiedene Ähnlichkeiten, aber auch einige Unterschiede auf. Zunächst ist den Rechtsordnungen gemeinsam, dass ihre Datenschutzregelungen grundsätzlich auf Finanzmarktunternehmen anwendbar sind. Zudem verfolgen fast alle untersuchten Länder das Prinzip der Verhältnismässigkeit bzw. einen risikobasierten Ansatz im Bereich der Cybersicherheit und Cyber-Resilienz.[369]

366 *Europäische Zentralbank* (EZB), European Framework for Threat-Intelligence Based Ethical Red teaming, Frankfurt am Main 2018.

367 *Europäische Zentralbank* (EZB), Cyber Information and Intelligence Sharing Initiative (CIISI-EU), Cyber information and intelligence sharing: a practical example, Euro Cyber Resilience Board Secretariat, Frankfurt am Main 2020.

368 EZB, 2020, 3.

369 Vgl. Kap. III.C.1, III.D.2.e), III.D.5.b), III.D.5.c) und III.E.3.c).

Darüber hinaus fällt auf, dass im ostasiatischen Raum umfassende, sektorübergreifende Cybersicherheitsgesetze erlassen wurden, die u.a. auch auf den Finanzmarkt anwendbar sind;[370] teilweise ergänzen diese Länder ihre allgemeinen Cybersicherheitsgesetze mit sektorspezifischen Regelungen für den Finanzmarkt.[371] Auf dem europäischen Kontinent (in der Europäischen Union, im Vereinigten Königreich sowie in Liechtenstein) und in Indien hingegen haben die Gesetzgeber auf ein umfassendes, sektorübergreifendes Cybersicherheitsgesetz verzichtet; ungeachtet dessen ist der Finanzmarkt nicht ungeregelt, denn die zuständigen Autoritäten haben detaillierte Regelungen und Richtlinien in Kraft gesetzt.[372]

Ferner ist ersichtlich, dass die untersuchten Länder grosses Gewicht auf die Kommunikation bei bzw. nach einem Cyberangriff legen, damit ähnliche Vorfälle nicht innert kürzester Zeit bei verschiedenen Unternehmen stattfinden.[373] Überdies werden die Unternehmen verpflichtet (bzw. ihnen wird empfohlen), regelmässig Penetrationstests und Verwundbarkeitsanalysen durchzuführen, damit sie gegenüber den gegenwärtigen Risiken auf dem neusten Stand sind.[374]

In der Schweiz existiert – ähnlich wie bei den untersuchten Rechtsordnungen auf dem europäischen Kontinent – ebenfalls kein umfassendes, sektorübergreifendes Cybersicherheitsgesetz; die Eidgenössische Finanzmarktaufsicht FINMA hat in Rundschreiben die Grundzüge der Cybersicherheit und Cyber-Resilienz auf dem Finanzmarkt geregelt.[375] Diese Grundzüge erfordern aber Konkretisierungen (beispielsweise) in Form von Handlungsempfehlungen; dabei sind insbesondere Konkretisierungen im Rahmen des Risikomanagements[376], des Business-Continuity-Managements (u.a. Kommunikationsplan und Durchführung von Übungen und Tests)[377] sowie der Aufsicht über Drittanbieter[378] erforderlich, d.h. Handlungsempfehlungen, wie sie nachfolgend im Einzelnen erläutert werden.

370 Vgl. Kap. III.E.3.b), III.E.5.b), III.E.6.b) und teilweise III.E.4.b).

371 Vgl. Kap. III.E.3.c) und III.E.6.c).

372 Vgl. Kap. III.C.1, III.D.2, III.E.1.b)-III.E.1.d) und III.E.7.b).

373 Vgl. Kap. III.C.2.b), III.D.2.c), III.D.2.d), III.D.4, III.E.1.b)aa), III.E.1.c), III.E.3.b), III.E.4.b), III.E.7.b)aa) und III.F.

374 Vgl. Kap. III.C.2.b), III.D.2.e), III.E.1.d)aa), III.E.3.c), III.E.4.b), III.E.6.b) und III.E.7.b)aa).

375 Vgl. Kap. III.B.1.

376 Kap. IV.B.

377 Kap. IV.C (insb. Kap. IV.C.4 und IV.C.6).

378 Kap. IV.D.

IV. Handlungsempfehlungen für Finanzmarktunternehmen

Die Schweiz kennt weder ein allgemeines Cybersicherheitsgesetz noch umfassende entsprechende Regelungen für den Finanzmarkt, sondern (bloss) Rundschreiben der FINMA und Selbstregulierungen der Marktteilnehmer. Das Datenschutzgesetz (DSG) verlangt, eine angemessene Datensicherheit sicherzustellen, und verpflichtet dessen Adressaten, Verletzungen der Datensicherheit zu melden. Darüber hinaus sieht die nationale Strategie zum Schutz der Schweiz vor Cyberrisiken auf allgemeine Weise und sektorübergreifend vor, potenzielle Verwundbarkeiten zu minimieren und die Schweiz gegenüber der intensivierten Bedrohungslage im Bereich der Cybersicherheit zu schützen.[379]

Diese vereinzelten und in verschiedenen Gesetzen geregelten Normen zur Cybersicherheit sind nicht ausreichend; sie bieten keinen angemessenen Schutz für den Wirtschaftsstandort Schweiz. Die Verflechtungen zwischen den Finanzmärkten, Finanzdienstleistern und Finanzmarktinfrastrukturen sowie zwischen den verschiedenartigen IKT-Systemen führen zu Systemanfälligkeiten, welche die Stabilität des Finanzsystems der Schweiz beeinträchtigen und folglich zu einem Vertrauensverlust des Finanzsystems führen können. Um Systemausfälle zu verhindern und eine operationelle Resilienz gegenüber Cyberrisiken zu erreichen, sind harmonisierte Handlungsempfehlungen für den Schweizer Finanzmarkt unabdingbar.

In diesem Kapitel werden die Erkenntnisse aus dem Rechtsvergleich – mit allfälligen Anpassungen – für die Rechtsordnung in der Schweiz umgesetzt. Ziel dieses Kapitels ist, mit Empfehlungen für einen adäquaten Vollzug der Cybersicherheit und Cyber-Resilienz im Schweizer Finanzmarkt zu sorgen. Wichtig ist dabei, dass die rechtlichen Rahmenbedingungen in der Schweiz im internationalen Vergleich weder Schwächen noch andere Lücken aufweisen.

Die nachfolgend diskutierten Handlungsempfehlungen, die sich inhaltlich zum Teil an der geplanten DORA-Regulierung orientieren, grenzen zunächst den Anwendungsbereich mit Blick auf den Adressatenkreis ab (A.) und skizzieren ein sinnvolles Risikomanagement im Bereich der Cybersicherheit (B.). Über-

379 Vgl. Kap. III.B.

dies wird das Business-Continuity-Management mit Hinweisen zur Vorgehensweise bei einem Cybervorfall erläutert (C.). Die Unternehmen haben zudem eine sachgerechte Aufsicht über Drittanbieter einzurichten (D.).

A. Anwendungsbereich

Die Finanzmärkte befinden sich in einem weit vernetzten und verflochtenen System mit verschiedensten Akteuren aus unterschiedlichsten Branchen. Deshalb ist es wichtig, an erster Stelle den Adressatenkreis, also den persönlichen Geltungsbereich der Handlungsempfehlungen, festzulegen (1.). Da es sich aus einem risikobasierten Ansatz ergibt, dass nicht alle Unternehmen dieselben Massnahmen ergreifen müssen, sind die einzelnen Unternehmensgrössen, die kritischen Infrastrukturen und die systemrelevanten Institutionen zu umschreiben und ist auf deren Unterscheidung näher einzugehen (2.). Ferner wird die Anwendung eines risikobasierten Ansatzes noch einmal dargelegt (3.).

1. Adressatenkreis

a) Allgemeine Bemerkungen

Aufgrund der Verflechtung verschiedener Teilnehmer im Finanzmarkt ist es sinnvoll, die Handlungsempfehlungen nicht nur für Banken, sondern generell für den Finanzmarkt zu gestalten und IKT-Drittanbieter ebenfalls zu berücksichtigen. In diesem Rahmen richten sich die Handlungsempfehlungen insbesondere an folgende Unternehmen:[380]

- Kreditinstitute;
- Zahlungsinstitute (inkl. Infrastrukturen);
- Wertpapierfirmen;
- Anbieter von Krypto-Dienstleistungen, Emittenten von Kryptowerten, Emittenten von an Vermögenswerte geknüpften Token;
- Zentralverwahrer;
- Zentrale Gegenparteien;
- Handelsplätze (inkl. Infrastrukturen);

[380] Vgl. Art. 2 Abs. 1 DORA; diese Liste stützt sich auf europäisches Recht, ist aber sinngemäss auch für die Schweiz anwendbar.

- Transaktionsregister;
- Verwalter alternativer Investmentfonds;
- Verwaltungsgesellschaften;
- Datenbereitstellungsdienste;
- Versicherungs- und Rückversicherungsunternehmen;
- Versicherungsvermittler, Rückversicherungsvermittler und Versicherungsvermittler in Nebentätigkeit;
- Einrichtungen der betrieblichen Altersversorgung;
- Ratingagenturen;
- Abschlussprüfer und Prüfgesellschaften;
- Administratoren kritischer Benchmarks;
- Crowdfunding-Dienstleister;
- Verbriefungsregister;
- IKT-Drittanbieter.

Innerhalb des Unternehmens ist es der Geschäftsführung überlassen, die Handlungsempfehlungen angemessen einzuhalten und umzusetzen.

b) Finanzmarktinfrastrukturen im Besonderen

Gemäss Art. 2 lit. a FinfraG gelten Börsen (Art. 26 lit. b FinfraG), multilaterale Handelssysteme (Art. 26 lit. c FinfraG), zentrale Gegenparteien (Art. 48 FinfraG), Zentralverwahrer (Art. 61 FinfraG), Transaktionsregister (Art. 74 FinfraG), DLT-Handelssysteme (Art. 73*a* FinfraG) und Zahlungssysteme (Art. 81 FinfraG) als Finanzmarktinfrastrukturen; sie sind besonderen Cybersicherheits-Risiken ausgesetzt, und zwar sowohl mit Bezug auf die Abwicklung von Zahlungen als auch den Handel mit (digitalen) Werten.

Die Finanzmarktinfrastrukturen bilden die Pfeiler für einen funktionsfähigen Kapitalmarkt und sind auch ein Bindeglied für die internationale Vernetzung der Kapitalmärkte. Angesichts ihrer bedeutenden (nationalen) Funktion für den Handelsplatz Schweiz sowie der internationalen Relevanz erweist sich eine adäquate Cybersicherheit und Cyber-Resilienz als unabdingbar; dies gilt sowohl für die «traditionellen» Finanzmarktinfrastrukturen als auch für die in

der Schweiz neu geregelten DLT-Handelssysteme, die auf der Distributed Ledger Technologie (DLT) beruhen. Diese Technologie ist eine spezielle Form der Datenspeicherung und -verarbeitung; sie basiert auf dem Konsensmechanismus der Beteiligten und gilt deshalb als unveränderlich, transparent und überprüfbar.[381] Aufgrund dieser Besonderheit erfordern die DLT-basierten Systeme auch der Erarbeitung gesonderter Handlungsempfehlungen.[382]

2. Unternehmensgrösse, kritische Infrastrukturen und systemrelevante Institutionen

Da die Schweiz ähnlich wie die Europäische Union einen risikobasierten Ansatz im Rahmen der Cybersicherheit verfolgt,[383] ist es sinnvoll, mindestens zwischen den (i) einzelnen Unternehmensgrössen, (ii) den kritischen Infrastrukturen und (iii) den systemrelevanten Institutionen zu unterscheiden.[384] Die Empfehlungen sind zwar an alle Finanzunternehmen gerichtet, aber deren Umsetzung hat entsprechend Risiko, Bedürfnis, Grösse und Unternehmensprofil des Finanzunternehmens zu erfolgen; die Verhältnismässigkeit und der risikobasierte Ansatz sind folglich bei der Anwendung der Empfehlungen zu beachten.

(i) Das EU-Recht will im geplanten DORA die sog. Kleinstunternehmen von einigen regulatorischen Vorgaben (Art. 4-13 DORA) befreien. Nach geltendem europäischem Recht beschäftigen Kleinstunternehmen weniger als 10 Personen und haben einen Jahresumsatz bzw. eine Jahresbilanz von weniger als 2 Mio. Euro.[385] Die Schweiz kennt keine gesetzliche Definition von Kleinstunternehmen, sie verwendet in Statistiken jedoch den Begriff der «Mikrounternehmen» in vergleichbarer Weise und erfasst darunter alle Unternehmen mit

381 *Maull/Godsiff/Mulligan/Brown/Kewell*, 2017, 483 f.

382 Zu dieser Thematik vgl. *Rolf H. Weber*, Sicherheit und Resilienz in DLT-basierten Finanzinfrastrukturen, erscheint im Frühling 2022 in Weblaw (online).

383 Vgl. Kap. III.B.1 und III.B.2.

384 Vgl. auch die besondere Behandlung der Kleinstunternehmen in der Europäischen Union (Kap. III.D.2.b)) und der kritischen Infrastrukturen in den anderen Rechtsordnungen (Kap. III.E).

385 Art. 2 Abs. 3 des Anhangs der Empfehlung der Kommission vom 6. Mai 2003 betreffend die Definition der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen (Text von Bedeutung für den EWR) (Bekannt gegeben unter Aktenzeichen K(2003) 1422), OJ L 124, 20.5.2003, 36–41.

weniger als 10 Beschäftigten. Die Schweiz wendet also nicht eine Grenze des Jahresumsatzes bzw. der Jahresbilanz an, um den Begriff der Mikrounternehmen zu erfüllen.[386]

Ungeachtet des Fehlens einer klaren Definition fragt sich angesichts der Ähnlichkeit des Verständnisses, ob eine vergleichbare Befreiung von Kleinstunternehmen von regulatorischen Vorgaben auch in der Schweiz in Betracht zu ziehen ist. Die Beurteilung muss zurückhaltend ausfallen: In den sehr stark vernetzten Finanzmärkten ist das schwächste Glied das Einfallstor für Cyberattacken; der Angriff auch auf eine kleine Bank vermag grössere Teile der Infrastrukturen in Mitleidenschaft zu ziehen. Erleichterte Vorgaben sind also nur in beschränktem Masse zu rechtfertigen; die FINMA steht deshalb in ihren Überwachungstätigkeiten vor der Herausforderung, mehr Finanzunternehmen als bisher auf ihre Cyber-Resilienz hin zu beaufsichtigen.

(ii) Der Bundesrat definiert in der Botschaft zur nationalen Strategie zum Schutz der Schweiz vor Cyberrisiken die kritischen Infrastrukturen als Prozesse, Systeme und Einrichtungen, die essenziell für das Funktionieren der Wirtschaft oder das Wohlergehen der Bevölkerung sind.[387] Die kritischen Infrastrukturen umfassen gemäss der nationalen Strategie zum Schutz kritischer Infrastrukturen (SKI) neun Sektoren, unterteilt in 27 Teilsektoren (Branchen); zu den neun Sektoren (und deren Teilsektoren) gehören u.a. die Energie (Energieversorgung), der Verkehr (Personen- und Güterverkehr), die Gesundheit (medizinische Versorgung) sowie auch die Finanzen (Finanzdienstleistungen und Versicherungsdienstleistungen).[388]

Gemäss dem Bundesamt für Bevölkerungsschutz (BABS) sind die Dienstleistungen, wie z.B. die Abwicklung des Zahlungsverkehrs, die Versorgung der Bevölkerung mit Bargeld, die Kapitalisierung Dritter, die Entgegennahme von Einlagen oder die Sicherstellung der Preisstabilität entscheidend für die Aufrechthaltung der Volkswirtschaft; demnach kann die Schweizer Wirtschaft ohne Zugang zu Bargeld oder Kapital bzw. ohne die Möglichkeit, Einlagen zu tätigen und Zahlungen abzuwickeln, nicht bzw. nur sehr eingeschränkt funktionieren.[389]

---

386 *Bundesamt für Statistik*, *Kleine und mittlere Unternehmen*, Definition KMU, aufrufbar unter <https://www.bfs.admin.ch/bfs/de/home/statistiken/industrie-dienstleistungen/unternehmen-beschaeftigte/wirtschaftsstruktur-unternehmen/kmu.html>.

387 *Botschaft nationale Strategie*, BBl 2018, 511; vgl. ferner NCSC, 2018, 31.

388 *Botschaft nationale Strategie*, BBl 2018, 511 f.

389 BABS, 2016, 1; vgl. ferner EFK, 2020, 25.

Der Bundesrat hält dafür, dass – unabhängig der Kritikalität – sämtliche Elemente (u.a. Betreiberfirmen, IT-Systeme, Anlagen oder Bauten), in denen Leistungen in einem der 27 Teilsektoren erbracht werden, den Charakter von kritischen Infrastrukturen haben.[390] In der Schweiz sind die kritischen Infrastrukturen durch Massnahmen zu schützen, welche die Eintrittswahrscheinlichkeit bzw. das Schadensausmass von Störungen, Ausfällen oder Zerstörungen der kritischen Infrastrukturen reduzieren oder die Ausfallzeit minimieren. Dem risikobasierten Ansatz folgend sollen die Massnahmen – gemessen an der Bedeutung der kritischen Infrastrukturen – verhältnismässig sein. Die Bedeutung bzw. Kritikalität der kritischen Infrastrukturen ist von der jeweiligen Betrachtungsebene abhängig und auf Ebene des Bundes, der Kantone und der Gemeinden gesondert zu ermitteln.[391]

(iii) Innerhalb des Sektors «Finanzen» stehen die als «too big to fail» bezeichneten systemrelevanten Institutionen im Vordergrund. Gemäss dem risikobasierten Ansatz sind die systemrelevanten Banken gehalten, strengere Massnahmen umzusetzen. Sie müssen bereits gemäss Art. 9 BankG höhere prudentielle Anforderungen einhalten. Ähnliche Anforderungen sind auch im Rahmen der Cybersicherheit sinnvoll.

Als systemrelevante Banken gelten gemäss Art. 7 Abs. 1 BankG diejenigen Banken, «deren Ausfall die Schweizer Volkswirtschaft und das schweizerische Finanzsystem erheblich schädigen würde». Ferner sind nach Art. 8 Abs. 1 BankG Funktionen systemrelevant, «wenn sie für die schweizerische Volkswirtschaft unverzichtbar und nicht kurzfristig substituierbar sind» (z.B. das inländische Einlagen- und Kreditgeschäft sowie der Zahlungsverkehr). Die Systemrelevanz einer Bank «beurteilt sich nach deren Grösse, deren Vernetzung mit dem Finanzsystem und der Volkswirtschaft sowie der kurzfristigen Substituierbarkeit der von der Bank erbrachten Dienstleistungen» (Art. 8 Abs. 2 BankG); massgebend für die Beurteilung sind Kriterien wie u.a. der Marktanteil an den systemrelevanten Funktionen (lit. a) oder das Risikoprofil der Bank (lit. d).

In ähnlicher Weise unterstehen die systemisch bedeutsamen Finanzmarktinfrastrukturen einer besonderen Überwachung nach Art. 19 NBG i.V.m. Art. 22 ff. FinfraG. Gemäss Art. 22 FinfraG ist die systemische Bedeutsamkeit gegeben, wenn die Nichtverfügbarkeit zu schwerwiegenden Verlusten, Liquiditätsengpässen oder operationellen Problemen bei Finanzintermediären oder anderen

390 In diesem Zusammenhang sind in der Regel nicht die IT-Systeme an sich der Schutzgegenstand, sondern die kritischen Infrastrukturen selbst (vgl. auch *Stevens*, 2021, Rn. 15).

391 *Botschaft nationale Strategie*, BBl 2018, 512.

Finanzmarktinfrastrukturen führen oder schwerwiegende Störungen an den Finanzmärkten zur Folge haben kann (lit. a). Ferner liegt systemische Bedeutsamkeit vor, wenn Zahlungs- oder Lieferschwierigkeiten einzelner Teilnehmer über sie auf andere Teilnehmer oder verbundene Finanzmarktinfrastrukturen übertragen werden und bei diesen zu schwerwiegenden Verlusten, Liquiditätsengpässen oder operationellen Problemen führen oder schwerwiegende Störungen an den Finanzmärkten zur Folge haben können (lit. b).[392]

3. Anwendung eines risikobasierten Ansatzes

Die Cybersicherheitsstrategie muss einen umfassenden Ansatz verfolgen, also alle relevanten Verwundbarkeiten und Bedrohungen berücksichtigen. Aber gleichzeitig sind die nachfolgenden Empfehlungen im Sinne eines risikobasierten Ansatzes zu implementieren, d.h. es ist weder ein umfassender Schutz vor Cyberrisiken möglich noch gibt es einen pauschalen Mindeststandard für alle Finanzunternehmen. Die Risiken sind gemäss Grösse und Unternehmensprofil des Finanzinstituts gesondert einzuschätzen und zu behandeln, um zu gewährleisten, dass das verbleibende Restrisiko grundsätzlich tragbar ist.[393]

Die Bemerkungen im Bericht zur Cybersicherheit und Cyber-Resilienz für die Schweizer Stromversorgung[394] gelten in ähnlicher Weise auch für den Finanzmarkt. Die Auswirkungen eines Cybervorfalls können aufgrund der Kaskadeneffekte auf dem Finanzmarkt ebenfalls schnell eskalieren. Angesichts der Vernetzung des Finanzmarkts ist zudem die «Weakest-Link»-Problematik zu beachten: die Gesamtsicherheit des Markts ist grundsätzlich nur so robust wie der schwächste Teil des Systems.[395]

In diesem Zusammenhang ist auch der menschliche Faktor bzw. die menschliche Einflussgrösse (engl. «human factor») von grosser Bedeutung, da der Mensch in der Regel das wichtigste Glied der Cybersicherheitskette darstellt.[396] Durch den Menschen entstehen verschiedene Schwachstellen, indem er E-Mails öffnet, Links anklickt oder Aktualisierungen und das Führen von Si-

392 *Komm. NBG-Häusermann*, 2021, Art. 19 Rn. 8 ff.; *BSK FinfraG-Peyer*, 2019, Art. 22 Rn. 18 ff.

393 *Botschaft nationale Strategie*, BBl 2018, 514.

394 *Bundesamt für Energie*, 2021, Cyber-Sicherheit und Cyber Resilienz für die Schweizer Stromversorgung.

395 Vgl. *BFE*, 2021, 26 und 130; vgl. ferner *Weber/Studer*, 2016, 720; *Shackelford/Raymond/Balakrishnan/Dixit/Gjonaj/Kavi* 2016, 14; vgl. zur Bedeutung der «Weakest-Link»-Problematik in Finanzmärkten *Calliess/Baumgarten*, 2020, 1155 f.

396 *Bissell/Lasalle/Dal Cin*, 2019, 9; *Camillo*, 2017, 199; *Webley/Hardy*, 2015, 353.

cherheitskopien unterlässt.[397] Eine wirksame Regulierung der Cybersicherheit erkennt die Bedeutung der Ausbildung des Menschen und legt einen Schwerpunkt auf die Schulung von Führungskräften und Mitarbeitenden, auf das kontinuierliche Lernen sowie auf die Sensibilisierung für Risiken.[398] Sollten die Handlungsempfehlungen aufgrund des risikobasierten Ansatzes grossflächig nicht bzw. nicht genügend zur Anwendung kommen, besteht die Gefahr, dass auch strengere Massnahmenempfehlungen bei den kritischen Infrastrukturen nur bedingte Wirksamkeit haben.

Überdies erwähnt die Eidgenössische Finanzkontrolle in ihrer Prüfung der Aufsicht über die Cybersicherheit bei Finanzdienstleistern, dass sich eine Kategorisierung der Banken und eine Risikobeurteilung nach quantitativen Kriterien im Bereich der Cybersicherheit als nur bedingt sinnvoll erweist. Vielmehr ist – falls die Kategorisierung beibehalten wird – diese auszuweiten und weiterzuentwickeln, um dem Stellenwert der Cyberrisiken zu entsprechen und deren dynamischer Natur gerecht zu werden. Problematisch ist insbesondere, dass auch gleichzeitige Cyberangriffe auf mittlere und/oder kleine Institutionen einen grossen Einfluss auf den Finanzplatz Schweiz haben können; aufgrund der technischen Vernetzung und des Datenaustauschs gibt es eine potenziell grössere Angriffsfläche, welche sich über einen Angriff auf anfälligere Marktteilnehmer ausnutzen lässt.[399] Neben der grösseren Angriffsflächen für die Cyberangriffe ist auch die steigende Zahl von Cyberangriffen ein Problem, weil sie die Wahrscheinlichkeit problematischer Folgen vergrössert.[400]

Wie erwähnt ist bei der Aufsicht und Umsetzung der Handlungsempfehlungen zu beachten, dass gemäss der Europäischen Zentralbank (EZB) – aufgrund der Verbundenheit und Abhängigkeit des Finanzsektors – Teilnehmer, die nicht kritische Infrastrukturen betreiben, und kleine Teilnehmer genauso riskant sein können für das Finanzsystem wie grosse bzw. kritische Teilnehmer.[401] Aus diesem Grund muss eine wirksame Regulierung im Bereich der Cybersicherheit auf alle Akteure anwendbar sein und sich nicht bloss auf die grossen Teilnehmer konzentrieren.[402] In diesem Zusammenhang ist auch anzumerken,

397 Vgl. *Kaur/Lashkari/Lashkari*, 2021, 94 ff.; vgl. ferner *Kay/Hutcherson/Keene/Zhang/Terwilliger*, 2021, 65 mit dem simplen Beispiel der Phishing-Mails; *Pupillo/Griffith/Blockmans/Renda*, 2018, 8 f.

398 So auch *Calliess/Baumgarten*, 2020, 1154.

399 EFK 2020, 17 f.

400 BFE 2021, 128 und 130.

401 EZB 2018a, 2; vgl. ferner *Bouveret*, 2018, 11.

402 Gl.M. *Calliess/Baumgarten*, 2020, 1155; vgl. ferner *Almansi*, 2018, 25.

dass die kleineren Unternehmen von Cyberattacken nicht weniger betroffen sein werden, sondern viel eher noch in den Fokus der potenziellen Cyberattacken rücken können.

B. Risikomanagement

1. Einleitende Bemerkungen

Banken sind verpflichtet, im Rahmen ihres Risikomanagements alle relevanten Risiken mit einem möglichen negativen Einfluss auf das Unternehmen zu erfassen (Art. 1*b* Abs. 3 lit. b BankG; Art. 12 Abs. 2 BankV und Art. 14*e* BankV). Das Risikomanagement umfasst gemäss FINMA «die organisatorischen Strukturen sowie die Methoden und Prozesse, die der Festlegung von Risikostrategien und Risikosteuerungsmassnahmen sowie der Identifikation, Analyse, Bewertung, Bewirtschaftung, Überwachung und Berichterstattung von Risiken dienen».[403] Innerhalb dieses Risikomanagements kommt mit dem Aufkommen der Cyberbedrohungen nun auch den Cyberrisiken eine besondere Bedeutung zu.[404]

Ein solider und gut dokumentierter Risikomanagementrahmen ermöglicht den Finanzunternehmen, die Cyberrisiken schnell, effizient und umfassend anzugehen, und gewährleistet – entsprechend den geschäftlichen Bedürfnissen – ein hohes Mass an digitaler Betriebsstabilität und Cyber-Resilienz. Mit den geeigneten Strategien, Richtlinien, Verfahren, Protokollen und Instrumenten im Risikomanagementrahmen minimieren die Finanzunternehmen die Cyberrisiken.

Das Risikomanagement eines Unternehmens ist entscheidend für die Cybersicherheit bzw. Cyber-Resilienz und beinhaltet verschiedene Aspekte. Zu einem guten Risikomanagement im Rahmen der Cyberrisiken gehören funktionierende interne Governance- und Kontrollmechanismen (2.), die Identifizierung der cybersicherheitsbezogenen Unternehmensfunktionen (3.) sowie Massnahmen zum Schutz und zur Prävention vor Cyberattacken (4.). Ferner sind die Unternehmen gehalten, Mechanismen einzuführen, welche frühzeitig fremde Aktivitäten erkennen können, um deren Auswirkungen zu minimieren (5.); für ei-

403 FINMA, Rundschreiben 2017/1, Rn. 3.

404 Vgl. FINMA, Rundschreiben 2008/21, Rn. 135.6 ff., wonach im Rahmen der operationellen Risiken die Cyberrisiken ausdrücklich erwähnt und der Umgang mit den Cyberrisiken beschrieben wird.

nen effizienten Schutz sind die Mechanismen und Massnahmen mit einem guten Situationsbewusstsein zu koppeln (6.). Für die Datensicherung sind ebenfalls adäquate Vorkehrungen zu treffen (7.).

2. Governance- und Kontrollmechanismen

Die Leitungsorgane der Unternehmen haben adäquate Governance- und Kontrollmechanismen einzurichten und aktiv den Rahmen für das Risikomanagement zu steuern sowie für die Einhaltung der Cyberhygiene[405] zu sorgen. Es liegt in der Verantwortung der Leitungsorgane, einen übergeordneten Grundsatz für die Steuerung des Risikos festzulegen und dessen Beachtung sicherzustellen. Der Grundsatz ist sinnvollerweise in spezifische Anforderungen mit klarer Zuweisung der Zuständigkeiten aufzuspalten. Ziel und Zweck der Governance-Massnahmen ist, dass die Leitungsorgane die Cyber- und Sicherheitsrisiken des Unternehmens angemessen beherrschen können.[406]

Zudem haben die Leitungsorgane sicherzustellen, dass die Anzahl und die Fähigkeiten des Personals angemessen sind, um die Sicherheitsrisiko-Managementprozesse fortlaufend unterstützen sowie die Umsetzung der Cybersicherheitsstrategie gewährleisten zu können.[407] Die Leitungsorgane sind auch dafür verantwortlich, dass eine regelmässige und geeignete Schulung sowie Fortbildung des Personals sichergestellt ist.[408]

Im Rahmen der Governance-Mechanismen ist erforderlich, dass die Leitungsorgane ordnungsgemäss über die Vereinbarungen mit Drittanbietern und jeweiligen Änderungen dieser Vereinbarungen sowie auch über die möglichen Auswirkungen dieser Änderungen auf kritische Systeme informiert sind. Cybervorfälle und deren Auswirkungen sowie Gegen-, Wiederherstellungs- und Korrekturmassnahmen stellen ebenfalls ein Informationsthema dar.

Darüber hinaus sollte ein Finanzunternehmen über klare und transparente Governance-Regelungen verfügen, welche die Sicherheit und Effizienz des Unternehmens fördern und die Stabilität des Finanzsystems im weiteren Sinne

405 Zum Begriff, vgl. Erw. 8 des Rechtsakts zur Cybersicherheit. Als Cyberhygiene sind einfache Routinemassnahmen zu verstehen, deren regelmässige Umsetzung und Durchführung die Risiken von Cyberbedrohungen so gering wie möglich zu halten beabsichtigen; zur Notice on Cyber Hygiene in Singapur, vgl. Kap. III.E.3.d). Eine angemessene Cyberhygiene wird auch über Selbstregulierung im Völkerrecht gefördert (vgl. hierzu *Weber*, 2021g, 620).

406 *EIOPA*, 2021, 9.

407 *Ibid.*

408 Angelehnt an Art. 4 DORA.

sowie andere relevante Erwägungen des öffentlichen Interesses und die Ziele der relevanten Akteure unterstützen. Im Einzelnen sind die Leitungsorgane gehalten, den Risikomanagementrahmen zu definieren, zu genehmigen und zu überprüfen; sie sind auch für dessen Umsetzung rechenschaftspflichtig.

Da es sich bei der Cybersicherheit um einen dynamischen Bereich handelt, sollten die Mitglieder der Leitungsorgane regelmässig an Fachschulungen teilnehmen, um ihren Kenntnisstand jeweils auf dem neusten Niveau zu halten und die potenziellen Auswirkungen der Cyberrisiken auf dem Gebiet der Finanzunternehmen zu verstehen.

3. Identifizierung der cybersicherheitsbezogenen Unternehmensfunktionen

Die Finanzunternehmen sollten die cybersicherheitsbezogenen Unternehmensfunktionen angemessen identifizieren, klassifizieren und dokumentieren. Als Teil der Risikoidentifizierung sind u.a. die Daten, Personen, Geräte, Systeme sowie Anlagen der Unternehmen zu umschreiben und kategorisieren; dabei ist eine Risikoeinschätzung nach Kritikalität erforderlich.[409] Zudem sind alle Prozesse von Drittanbietern zu identifizieren und zu dokumentieren sowie die Vernetzung mit den Drittanbietern zu ermitteln.

Bereits im revidierten Rundschreiben 2008/21 empfahl die FINMA Massnahmen zur Identifikation von institutsspezifischen Bedrohungspotenzialen durch Cyberattacken.[410] Zur Umsetzung dieser Massnahmen sind geeignete Prozesse und Kontrollen erforderlich, die sicherstellen, dass alle Risiken identifiziert, analysiert, gemessen, überwacht, verwaltet, gemeldet und innerhalb der Grenzen der Risikobereitschaft der Finanzunternehmen gehalten werden.[411] Denkbar ist eine Übertragung dieser Arbeiten an die für das Risikomanagement zuständige Stelle, die von den Betriebsprozessen getrennt ist und somit unabhängig und objektiv agieren kann.[412]

Ferner ist erforderlich, dass die Finanzunternehmen die Risiken kontinuierlich ermitteln und bewerten; hierfür ist eine regelmässige Überprüfung der Risikoszenarien notwendig (mind. einmal jährlich). Bei wesentlichen Änderungen der Netz- und Informationssysteminfrastruktur sowie der Prozesse oder Verfah-

409 Vgl. Kap. II.C.1; vgl. ferner MAS, 2021, 13.

410 Vgl. FINMA, Rundschreiben 2008/21, Rn. 135.7.

411 So auch EBA, 2021, 9; FMA, Richtlinie 2021/3, 7.

412 Die Übertragung dieser Arbeiten ist an jede von den Betriebsprozessen getrennte Stelle vorstellbar; wichtig ist, dass diese Stelle unabhängig und objektiv agieren kann.

ren sind zudem Risikobewertungen durchzuführen; darüber hinaus erweisen sich Kontrollen nach Anschluss alter und neuer Technologien, Anwendungen oder Systeme als bedeutungsvoll.[413]

4. Schutz und Prävention

Die Finanzunternehmen sind gehalten, kontinuierlich ihre Systeme zu überprüfen und zu kontrollieren, damit sie einen angemessenen Cybersicherheits-Schutz bieten und Gegenmassnahmen planen können. Darüber hinaus sind mit geeigneten Sicherheitsinstrumenten, -strategien und -verfahren die Auswirkungen der Cyberrisiken zu minimieren. Das Ziel der Finanzdienstleister muss sein, die Resilienz, Kontinuität und Verfügbarkeit ihrer Systeme zu gewährleisten und die Sicherheit, Vertraulichkeit und Integrität der Daten aufrechtzuerhalten.[414]

Eine mögliche Option ist die «Resilience by Design», wonach die Finanzunternehmen bei der Entwicklung ihrer Systeme und Prozesse von Anfang an auf die Cyber-Resilienz achten. Die Einführung von «Resilience by Design» stellt unter anderem sicher, dass die Verbindungen zu den kritischen Systemen eines Unternehmens strengen Tests anhand entsprechender Sicherheitsstandards unterzogen werden und dass mögliche Angriffsflächen so weit wie möglich begrenzt werden.[415]

Ausserdem können die Finanzunternehmen den Schutz gegenüber Cyberangriffen erhöhen, indem sie nur autorisierten Personen, Prozessen und Geräten Zugriff auf die Systeme erlauben. Dabei ist insbesondere bei den autorisierten Personen Vorsicht geboten, da der «Human Factor» in der Cybersicherheit eine grosse Rolle spielt und nicht selten eine Schwachstelle darstellt.[416] Deshalb ist die Berechtigung des Zugangs zu Systemen auf Personen zu beschränken, die entsprechend geschult sind; hierfür ist es notwendig, dass die Finanzunternehmen Kontrollen einrichten, die den Zugang zu den Systemen zuverlässig auf diese Personen beschränken. Solche Kontrollen sind durch rol-

413 Vgl. Art. 7 DORA.

414 Vgl. Art. 8 DORA.

415 So auch BIS/IOSCO, 2016, 12.

416 Vgl. Kap. IV.A.3. Vgl. ferner für eine detaillierte Auseinandersetzung mit der Thematik des «Human Factor» in der Cybersicherheit *Kaur/Lashkari/Lashkari*, 2021, 94 ff.; *Hadlington*, 2018, 46 ff.; *Marble et al.*, 2015, 173 ff.

lenbasierten Zugang, Protokollierung und Überprüfung der Systemaktivitäten privilegierter Benutzer, starke Authentifizierung sowie Überwachung auf Anomalien realisierbar.[417]

Die Schutzmassnahmen der Finanzinstitute haben den führenden Standards für die Cyber-Resilienz zu entsprechen, um die Wahrscheinlichkeit und die Auswirkungen eines erfolgreichen Cyberangriffs auf identifizierte kritische Geschäftsfunktionen und Daten zu minimieren. Die Schutzmassnamen können mittels regelmässiger Verwundbarkeitsanalysen, Red-Team-Übungen und Penetrationstests von unabhängigen Dienstleistern umgesetzt werden; die Penetrationstests sind sowohl als Blackbox- als auch als Greybox-Tests durchführbar.[418] Denkbar ist ausserdem eine Adaptation der «Intelligence-Led»-Penetrationstests.[419] Um die Wirksamkeit und Robustheit dieser Tests bewerten und gewährleisten zu können, ist es sinnvoll, eine entsprechende Rahmenordnung einzurichten und umzusetzen, die sicherstellt, dass die Tests von unabhängigen Dritten bzw. Prüfern durchgeführt und das Verfahren der Schwachstellen- und Penetrationstests umfassend beschrieben werden.[420]

5. Erkennung der potenziellen Cyberrisiken

Obwohl die Identifizierung der cybersicherheitsbezogenen Unternehmensfunktionen und der Schutz der Systeme die Auswirkungen von Cyberrisiken eindämmen können, ist es ratsam, Mechanismen einzuführen, die frühzeitig fremde, anomale Aktivitäten erkennen. Diese Mechanismen dienen der Minimierung der Auswirkungen und vermögen die potenziellen Schwachstellen früh zu erkennen. Damit diese Mechanismen den internationalen Standards

417 Vgl. für ähnliche Handelsempfehlungen *BIS/IOSCO*, 2016, 13.

418 Vgl. hierzu insbesondere Art. 13.2 Technology Risk Management Guidelines (TRMG) in Kap. III.E.3.c). Bei Blackbox-Tests kennt der Tester die Umgebung nicht, mit Ausnahme der IP-Adressen und der URLs. Bei Greybox-Tests sind Tests mit Anmeldedaten betroffen, d.h. der Tester hat dieselben Rechte wie ein normaler Kunde.

419 Vgl. Kap. III.E.1.d)aa) zum «Intelligence-Led»-Ansatz des CBEST-Programms, der die Handlungen von Cyberangreifern nachahmt, die darauf abzielen, die wichtigen Unternehmensdienste einer Organisation zu beschädigen sowie die technologischen Anlagen und Prozesse zu stören; vgl. ferner Kap. III.E.4.b) für Kap. 4 des C-RAF («intelligence-led Cyber Attack Simulation Testing (iCAST)»).

420 Vgl. Kap. III.C.2.b); vgl. ferner FMA, Richtlinie 2021/3, 10 f.; *BIS/IOSCO*, 2016, 15.

entsprechen und mit den Entwicklungen im Rahmen der Cybersicherheit und der Cyberangriffe Schritt halten, ist es erforderlich, dass sie ebenfalls regelmässig getestet werden.[421]

Gängige Mechanismen für die Umsetzung der Cybersicherheit sind Netzwerkzonierungen, Firewalls, Systeme zur Erkennung von Eindringlingen («Intrusion Detection System», IDS), Antivirenanwendungen, kryptografische Techniken sowie Systeme zur Verwaltung von Sicherheitsinformationen und Ereignissen («Security Information and Event Management», SIEM). Jedoch kann keine dieser Mechanismen die totale Sicherheit gewährleisten, da die Angriffstechniken vielfältig sind und verschiedenste Schwachstellen in den Systemen und Protokollen der Unternehmensinfrastruktur auszunutzen vermögen.[422]

Angemessen ist eine kontinuierliche Überwachung in Echtzeit oder nahezu in Echtzeit («real time monitoring» oder «near real time monitoring»), welche die Finanzunternehmen beispielsweise mit der Einführung eines Sicherheitsoperationszentrums («Security Operations Center») erreichen können. Sinnvoll ist zudem, sowohl auf öffentlich bekannte Schwachstellen als auch auf noch nicht öffentlich bekannte Schwachstellen (sog. Zero-Day-Exploits) zu achten, indem zusätzlich verhaltensbasierte Erkennungsmechanismen verwendet werden.[423]

Komplementär zu diesen gängigen Mechanismen ist im Rahmen der frühzeitigen Erkennung von Cyberrisiken eine Plattform für den Informationsaustausch unter Finanzunternehmen ein sehr effizientes Instrument. Eine solche Plattform kann die Wahrscheinlichkeit verringern, dass gleiche oder ähnliche Cyberangriffe gegen verschiedene Unternehmen wirksam sind; sobald ein Unternehmen einen bestimmten Angriff entdeckt und der Plattform meldet, können andere Unternehmen ihre Systeme anpassen, um vergleichbare Cybervorfälle zu verhindern. Um eine effektive Nutzung der Plattform gewährleisten zu können, ist eine anonymisierte Meldung der Cybervorfälle zielführend. Die an-

421 Vgl. *NIST*, 2018, 37 ff.; vgl. auch Art. 9 DORA; *FINMA*, Rundschreiben 2008/21, Rn. 135.9.

422 Vgl. *DND/NATO/PfPC*, 2016, 24.

423 Vgl. *BIS/IOSCO*, 2016, 15 für ähnliche Handlungsempfehlungen.

onymisierte Meldung verhindert, dass die Unternehmen bloss zurückhaltend die Plattform benutzen, da sie preisgeben müssten, dass sie Opfer eines Cyberangriffs geworden sind.[424]

Mit diesen Erkennungsmechanismen lassen sich mehrere Kontrollebenen einführen, die verschiedene Alarmschwellen und -kriterien festlegen, welche der Erkennung der Cybervorfälle und der Einleitung von Gegenmassnahmen dienen. Jede Kontrollebene agiert dabei als Sicherheitsnetz für die vorhergehende Ebene. Da ein Cyberangriff in der Regel verschiedene Phasen durchläuft, bevor er sein Ziel erreicht, sollten die Finanzunternehmen mit ihren Mechanismen die Cyberangriffe verzögern oder stören können. Für die effektive Überwachung der Netzaktivitäten bzw. der Erkennung von Anomalien und Cybervorfällen brauchen die Finanzunternehmen selbsterklärend ausreichend Ressourcen und Kapazitäten.

6. Situationsbewusstsein

Neben der Fähigkeit, Cyberrisiken frühzeitig erkennen zu können, ist auch ein gutes Situationsbewusstsein (engl. «Situational Awareness») unabdingbar für die Finanzunternehmen. Das Situationsbewusstsein bezieht sich auf das *Verständnis* der Cyberbedrohungen und deren Auswirkungen im Geschäftsbereich des Unternehmens sowie das Verständnis für die Angemessenheit der Massnahmen zur Minderung von Cyberrisiken.[425]

Ein ausgeprägtes Situationsbewusstsein hat erheblichen Einfluss auf die Fähigkeit eines Finanzunternehmens, Cybervorfällen zuvorzukommen oder schnell und effektiv auf sie zu reagieren. Eine genaue Einschätzung der Bedrohungslage kann dem Unternehmen helfen, die Schwachstellen in seinen kritischen Geschäftsfunktionen besser zu verstehen und geeignete Strategien zur Risikominderung einzuschlagen. Ein wichtiges Mittel zur Erlangung eines Si-

424 Vgl. Kap. III.D.5.a); BIS/IOSCO, 2016, 21. In Japan existiert ein besonderes Programm für den Informationsaustausch, jedoch hat die japanische Regierung festgestellt, dass die Unternehmen zurückhaltend sind bei der Meldung von Vorfällen. Als mögliche Gründe stehen die Angst vor Auswirkungen in der Öffentlichkeit (z.B. negative Folgen auf der Börse) und die potenziell peinliche Lage für das Unternehmen im Vordergrund. Dennoch übersteigt der Nutzen einer funktionierenden Plattform die (teils unbegründete) Angst der Unternehmen (vgl. im Detail *Bartlett*, 2019, 18 f.).

425 BIS/IOSCO, 2016, 20.

tuationsbewusstseins ist die aktive Beteiligung an Vereinbarungen über den Informationsaustausch und die Zusammenarbeit mit vertrauenswürdigen Akteuren innerhalb und ausserhalb der Branche.[426]

Als Teil der Bedrohungsanalyse ist die Einrichtung eines Prozesses zur Sammlung und Analyse relevanter Cyberbedrohungsinformationen angebracht. Die Sammlung und Analyse hat in Verbindung mit anderen internen und externen Informationsquellen zu erfolgen, die einen geschäftsspezifischen Kontext schaffen. Durch die Kontextualisierung können die Informationen in verwertbare Cyberbedrohungsdaten umgewandelt werden, die wertvolle Erkenntnisse liefern und eine bessere Entscheidungsfindung ermöglichen, da die Finanzunternehmen die Absichten und den Modus Operandi der Cyberangriffe voraussehen können. Die Finanzunternehmen sollten darüber hinaus sicherstellen, dass die gewonnenen Kenntnisse den zuständigen Mitarbeitenden zur Verfügung gestellt werden, um die Minderung von Cyberrisiken auf strategischer, taktischer und operativer Ebene verwirklichen zu können.[427]

7. Datensicherung und Datensicherheit

Die Daten erlangen in der digitalisierten Welt eine immer grössere Bedeutung, weshalb es trotz aller Sicherheitsmassnahmen unabdingbar ist, eine Strategie zur Datensicherung und -sicherheit auszuarbeiten. Die Finanzunternehmen haben im Rahmen der Datensicherheit insbesondere zwei Rechtsquellen zu beachten: Einerseits enthält das Datenschutzgesetz (alt und neu) im Kontext der Personendaten besondere Vorgaben zur Datensicherung (Art. 8 nDSG, Art. 7 aDSG) und andererseits sind die bereits mehrfach erwähnten Vorgaben des FINMA Rundschreibens 2008/21 zur Cybersicherheit zu berücksichtigen.[428]

a) Datensicherung

Die Strategie zur Datensicherung zielt einerseits darauf ab, die Wiederherstellung der Daten und Systeme unter minimaler Ausfallzeit sicherzustellen. Andererseits hält sie auch einen Mindeststandard fest, der angibt, wie oft mindestens die Daten nach ihrer Kritikalität und Sensibilität zu sichern sind. Zur angemessenen Datensicherung gehört auch, dass die Finanzunternehmen ih-

426 Vgl. auch Kap. IV.C.4; vgl. ferner BIS/IOSCO, 2016, 20; EZB, 2018a, 46 ff.

427 So auch BIS/IOSCO, 2016, 20; EZB, 2018a, 46 ff.

428 Vgl. insbesondere FINMA, Rundschreiben 2008/21, Rn. 135.6 ff. und Kap. III.B.1.

re Daten verschlüsseln und den maximal erlaubten Datenverlust definieren.[429] Zudem ist es sinnvoll, die Systeme und Prozesse so zu gestalten und zu testen, dass nach einer Störung die fehlerfreie Wiederherstellung der Daten ermöglicht ist. Ferner verlangt das DSG, Massnahmen zur Datenwiederherstellung vorzusehen, wie z.B. die Aufbewahrung einer Kopie aller empfangenen und verarbeiteten Daten oder die Aufrechterhaltung der Fähigkeit zur Wiederholung von Transaktionen.[430]

b) Datensicherheit

Für die rechtlichen Rahmenbedingungen bei der Datensicherheit ist die Differenzierung zwischen den Personendaten und den Sachdaten von besonderer Bedeutung. Personendaten liegen vor, wenn die im Datum enthaltene Information sich auf eine bestimmte oder bestimmbare natürliche Person bezieht (Art. 5 lit. a nDSG und Art. 3 lit. a aDSG).[431] Dabei ist ein relatives Begriffsverständnis anzuwenden, das die Bestimmbarkeit der natürlichen Person anhand der Informationen und Informationsmöglichkeiten des jeweiligen Dateninhabers beurteilt.[432] Sachdaten hingegen fehlt der Personenbezug; alle Daten, die keine Personendaten sind, gelten als Sachdaten. Aus dem relativen Begriff der Personendaten und der negativen Definition des Sachdatenbegriffs folgt, dass kein Datum an sich als Personendatum oder Sachdatum qualifizierbar ist.[433]

Art. 8 Abs. 1 nDSG verlangt, dass der Verantwortliche bzw. der Auftragsbearbeiter durch geeignete technische und organisatorische Massnahmen eine dem Risiko angemessene Datensicherheit gewährleistet (sinngemäss Art. 7 Abs. 1 aDSG); der Bundesrat erlässt Bestimmungen über die Mindestanforderungen an die Datensicherheit (Art. 8 Abs. 3 nDSG und Art. 7 Abs. 2 aDSG). Der Vorentwurf betreffend die Verordnung zum Datenschutzgesetz (VE-VDSG) umschreibt die angemessene Datensicherheit ebenfalls mit einem risikoba-

429 Vgl. SVV, 2015, 8; SBVg, 2013, 9 für die Empfehlung, den maximal erlaubten Datenverlust zu definieren.

430 Vgl. für weiterführende Ausführungen Kap. IV.C.5; vgl. auch BIS/IOSCO, 2016, 16 f.

431 *Weber/Henseler*, 2020, 606. Unter dem neuen Datenschutzgesetz sind – im Gegensatz zur früheren Rechtslage – die Daten von juristischen Personen nicht mehr als Personendaten geschützt; vgl. auch *Beranek Zanon*, 2014, 97.

432 Vgl. im Detail zur Bestimmbarkeit der von Daten betroffenen Personen *Probst*, 2013, 1423–1436.

433 *Weber/Henseler*, 2020, 606; *Thouvenin/Weber/Früh*, 2019, 24 f.

sierten Ansatz und hält fest, dass sich die Beurteilung der angemessenen Sicherheit auf folgende Kriterien stützt (Art. 1 Abs. 1 VE-VDSG und Art. 8 aVDSG):[434]

- Zweck, Art, Umfang und Umstände der Datenbearbeitung (Art. 1 Abs. 1 lit. a VE-VDSG): Im Rahmen dieses Kriteriums wird das Schutzniveau unter Berücksichtigung der Gefährdung für die Persönlichkeitsrechte gewährleistet, d.h. je höher der Schutzbedarf ist, desto höher sind die Anforderungen an die Massnahmen.[435]
- Eintrittswahrscheinlichkeit einer Verletzung der Datensicherheit und deren potenzielle Auswirkungen für die betroffenen Personen (Art. 1 Abs. 1 lit. b VE-VDSG): Der erläuternde Bericht zur Totalrevision der Verordnung umschreibt dieses Kriterium wie folgt: «Je wahrscheinlicher der Eintritt einer Verletzung der Datensicherheit und je grösser die Auswirkungen für die betroffenen Personen, desto höher die Anforderungen an die Massnahmen.»[436]
- Stand der Technik (Art. 1 Abs. 1 lit. c VE-VDSG);
- Implementierungskosten (Art. 1 Abs. 1 lit. d VE-VDSG).

Die Verordnung verzichtet somit auf starre Mindestanforderungen; es liegt in erster Linie in der Verantwortung des Auftragsbearbeiters, die notwendigen Massnahmen zu ergreifen. Dies gewährt den Verantwortlichen eine gewisse Flexibilität, um die Vielfalt der Fallkonstellationen abdecken zu können.[437]

Zur Implementierung sind verschiedenste Massnahmen denkbar; der erläuternde Bericht zur Totalrevision der Verordnung nennt beispielhaft drei mögliche Massnahmen: Darunter fallen die Anonymisierung, Pseudonymisierung und Verschlüsselung von Personendaten, um allfällige negative Auswirkungen für die betroffenen Personen zu reduzieren.[438] Zudem können die Verantwortlichen spezifische Verfahren zur Identifikation, Bewertung und Evaluierung der Risiken sowie zur Überprüfung der Angemessenheit der getroffenen Massnahmen einführen.[439] Schliesslich empfiehlt der Bericht, das mit der

434 Art. 1 Abs. 1 VE-VDSG entspricht im Wesentlichen Art. 8 aVDSG, mit einer Reduktion der normativen Dichte; vgl. im Detail *EJPD*, 2021, 15 ff.

435 *EJPD*, 2021, 15.

436 *EJPD*, 2021, 16.

437 *EJPD*, 2021, 14.

438 *EJPD*, 2021, 16 f.

439 Vgl. im Detail zu Empfehlungen verschiedener Verfahren für die Finanzunternehmen Kap. IV.B.

Umsetzung betraute Personal zu schulen und zu beraten. Die letzten beiden Massnahmen sind für die Finanzunternehmen kein Neuland, denn diese Massnahmen sind im Rahmen der Cybersicherheit ebenfalls vorgesehen.[440]

Ähnliche Vorgaben galten bereits unter dem alten Datenschutzgesetz (Art. 7 aDSG), jedoch widmet das nDSG neu dem sog. Privacy by Design zwei besondere Absätze (Art. 7 Abs. 1 und 2 nDSG).[441] Die Vorgaben von Art. 7 nDSG dienen dazu, dass der Datenschutz bereits durch die Technik sowie durch datenschutzfreundliche Voreinstellungen gewährleistet wird. Ziel des Privacy by Design ist, dass sich Technik und Recht ergänzen und die technischen Vorkehren die Gefahr eines Verstosses gegen die Datenschutzvorschriften erheblich verringern.[442]

C. Business-Continuity-Management

1. Einleitung

Selbst das beste Risikomanagement mit sehr detailliertem Schutzkonzept kann nicht garantieren, dass es nie zu einem Cybervorfall kommt. Aus diesem Grund ist es unabdingbar, auch für die Vorgehensweise bei einem Cybervorfall zu planen. Es ist insbesondere eine kohärente und integrierte Überwachung, Handhabung und Weiterverfolgung der Cybervorfälle zu gewährleisten, damit die Finanzunternehmen die Ursachen ermitteln und beseitigen sowie hernach das weitere Auftreten solcher Vorfälle verhindern können.

Das Vorgehen bei einem Cybervorfall ist in den grösseren Kontext des Business-Continuity-Management einzubetten, der als unternehmerischer Ansatz sicherstellt, dass die Geschäftstätigkeit bei ausserordentlichen Situationen und Ereignissen überlebensfähig bleibt und aufrechterhalten werden kann.[443] Die FINMA hat für Banken und Versicherungen gewisse Mindeststandards und Empfehlungen für das Business-Continuity-Management als Selbstregu-

440 EJPD, 2021, 17; vgl. zur Schulung vom Personal u.a. Kap. III.E.5.b), III.E.6.b) und IV.B.2.

441 So *Rosenthal*, 2017, Rn. 40 f., mit dem Hinweis, dass dadurch die Verletzung des Grundsatzes der Privacy by Design weder als Persönlichkeitsverletzung (vgl. Art. 30 Abs. 2 lit. a nDSG) noch mit Strafe sanktionierbar ist.

442 *Botschaft DSG*, BBl 2017, 7028 f.

443 SVV, 2015, 4; SBV*g*, 2013, 6 f.

lierung anerkannt (Art. 7 Abs. 3 FINMAG).[444] Im Zusammenhang mit der Cybersicherheit und den Cyberrisiken sind diese Mindeststandards und Empfehlungen angemessen für die Cyberbedrohungen anzupassen und anzuwenden.

In einem ersten Schritt ist es sinnvoll, den Cybervorfall zu klassifizieren, um die Lage kontrollieren zu können (2.). Neben der Klassifikation des Vorfalls sind auch entsprechende Business-Continuity-Massnahmen – mit Details zu Gegenmassnahmen und allenfalls Wiederherstellungsverfahren – erforderlich (3.). Gestützt auf den Kommunikationsplan ist anschliessend eine Meldung vorzunehmen, welche andere Finanzunternehmen und die Behörden auf den neusten Stand der möglichen Risiken bringt und ihnen erlaubt, Präventionsmassnahmen zu treffen (4.). Da bei Cybervorfällen gemäss DSG geschützte Daten gefährdet sein könnten und gegebenenfalls eine Meldepflicht für Verletzungen der Datensicherheit auflebt, brauchen die Finanzunternehmen ein Konzept, wie bei solchen Vorfällen vorzugehen ist (5.). Im Rahmen des Business-Continuity-Management sind ausserdem regelmässige Übungen und Tests von besonderer Bedeutung (6.). Darüber hinaus ist auch für die Zukunft zu planen, weshalb die anwendbare Strategie im Bereich der Cybersicherheit und Cyber-Resilienz ständig weiterzuentwickeln und den neusten Gegebenheiten anzupassen ist; daraus folgt, dass die Cybersicherheit als fortlaufender Lernprozess anzusehen ist (7.).

2. Klassifikation

Gemäss den Empfehlungen der Schweizerischen Bankiervereinigung (SBVg) und des Schweizerischen Versicherungsverbands (SVV) sind im Rahmen der Business-Impact-Analyse die Cyberrisiken zu klassifizieren.[445] Die Klassifikation von Cybervorfällen kann der Festlegung der Wesentlichkeitsschwellen dienen; gleichzeitig hilft sie, potenzielle zukünftige Cybervorfälle einzugrenzen, um damit einen Beitrag zur schnelleren Verbesserung der Systeme zu leisten. Für die Klassifikation der Cybervorfälle sind folgende Kriterien von Bedeutung:[446]

444 Vgl. FINMA, Selbstregulierungen (mit einer Liste von der FINMA anerkannte oder genehmigte Selbstregulierungen), aufrufbar unter <https://www.finma.ch/de/dokumentation/selbstregulierung/anerkannte-selbstregulierung/>; vgl. ferner insbesondere SVV, 2015 und SBVg, 2013.

445 In diesem Zusammenhang sind die Cyberrisiken als potenzielle Auslöser von ausserordentlichen Situationen und Ereignissen zu verstehen (vgl. für die Business-Impact-Analyse SVV, 2015, 6; SBVg, 2013, 8 f.).

446 Gestützt auf Art. 16 Abs. 1 DORA und Anhang I der NIS-Richtlinie.

- Zahl der Nutzer oder anderer Akteure im Finanzbereich, die von der verursachten Störung betroffen sind;
- Verursachung eines Rufschadens durch den Cybervorfall;
- Dauer des Cybervorfalls und der Ausfallzeiten des Dienstes;
- Geografische Ausbreitung der vom Cybervorfall betroffenen Gebiete (insbesondere, wenn internationale Wirkungen vorliegen);
- Datenverluste in Verbindung mit dem Cybervorfalls (z.B. Verlust der Datenintegrität, Preisgabe oder Nichtverfügbarkeit von Daten);
- Schwere der Auswirkungen des Cybervorfalls auf die Systeme des Finanzunternehmens;
- Kritikalität der betroffenen Dienste und der Transaktionen bzw. Geschäfte des Finanzunternehmens;
- Wirtschaftliche Auswirkungen des Cybervorfalls auf absoluter und relativer Basis.

Gestützt auf diese Klassifikationskriterien ist das Finanzunternehmen verpflichtet, die Auswirkungen des Cybervorfalls abzuschätzen und entsprechend dieser Kenntnis eine erste Meldung an die zuständige Stelle abzugeben.[447]

3. Business-Continuity-Massnahmen

Als integralen Bestandteil der operativen Strategie ist es unabdingbar, eine spezifische und umfassende Strategie zur Fortführung des Geschäftsbetriebs auszuarbeiten, die Gegenmassnahmen vorsieht und die Wiederherstellung des Geschäftsbetriebs sicherstellt. Die Business-Continuity-Massnahmen definieren das Vorgehen und die Mittel für die Überbrückung und Wiederherstellung bei einem Cybervorfall.

a) Ziele

Im Rahmen der Business-Continuity-Strategie ist die Fortführung des Geschäftsbetriebs mit geeigneten und dokumentierten Plänen, Verfahren, Re-

447 Vgl. zur Meldung Kap. IV.C.4.

gelungen und Mechanismen sicherzustellen, welche regelmässigen, unabhängigen Prüfungen unterliegen sollten. Eine effiziente Strategie hat folgende Ziele:[448]

- Aufzeichnung der Cybervorfälle;
- Sicherstellung der Kontinuität der kritischen Funktionen des Finanzunternehmens;
- Rasche, wirksame und angemessene Reaktion auf die Cybervorfälle sowie Schadensbegrenzung durch schnelle Wiederaufnahme der Tätigkeiten;
- Aktivierung der Pläne, die Eindämmungsmassnahmen vorsehen, um weitere Schäden zu vermeiden;
- Vorläufige Einschätzung der Auswirkungen, Schäden und Verluste.

b) Gegenmassnahmen und Wiederherstellung

Von grosser Bedeutung ist – wie erwähnt – die Planung der Reaktion auf einen Cybervorfall. Sobald ein erfolgreicher Cyberangriff oder ein Angriffsversuch festgestellt wird, sind die Finanzunternehmen verpflichtet, eine gründliche Untersuchung durchzuführen, um Art und Umfang des Angriffs sowie den entstandenen Schaden zu ermitteln.[449] Während den Untersuchungen sind die Finanzunternehmen gehalten, sofortige Massnahmen zu ergreifen, um die Beeinträchtigungen zu mildern und weiteren Schaden zu verhindern.

Gleichzeitig sind auch die Wiederherstellungsmassnahmen einzuleiten, um den Betrieb auf der Grundlage ihrer Reaktionsplanung (engl. «Business Recovery Plan») wieder aufnehmen zu können. Die Business-Recovery-Pläne bezeichnen die notwendige Vorgehensweise, mögliche Ersatzlösungen und die dafür mindestens benötigten Ersatzressourcen.[450]

Anhand der Business-Impact-Analyse bewerten die Finanzunternehmen, inwiefern sie Betriebsausfällen ausgesetzt sind; ihre Systeme und Dienste sind so auszulegen, dass getroffene Schutzvorkehren potenzielle Störungen und Ausfälle von kritischen Komponenten minimieren können.[451] Ausserdem ist es unerlässlich, einen Reaktions- und Wiederherstellungsplan auszuarbeiten,

448 So auch *BIS/IOSCO*, 2016, 16; vgl. ferner Art. 10 DORA.

449 Für detailliertere Angaben hierzu vgl. Kap. IV.C.2.

450 *SBVg*, 2013, 10.

451 Vgl. hierzu Kap. IV.B.5.

welcher die Integrität, Verfügbarkeit, Kontinuität und Wiederherstellung der kritischen Systeme, Dienste und Daten gewährleistet. Damit eine koordinierte Reaktion und Wiederherstellung der Geschäftstätigkeiten möglich ist, sind Prioritäten für die Wiederherstellung festzulegen.[452]

Weil das Geschäftsgeschehen bei einem Cyberangriff nicht ganz ausfallen darf, spielt bei den Wiederherstellungsmassnahmen die Verfügbarkeit der Infrastrukturen bei bzw. nach einem Cyberangriff eine entscheidende Rolle. Deshalb empfehlen die Bank for International Settlements (BIS) und die International Organization of Securities Commissions (IOSCO)[453] ausdrücklich, dass die Finanzunternehmen in der Lage sein sollten, spätestens innerhalb zwei Stunden die kritischen Operationen wieder aufzunehmen und die Störungen – selbst bei extremen Szenarien – bis zum Ende des Tages zu beheben.[454] Im Rahmen des Business-Continuity-Management ist es sinnvoll, auch den gewünschten Grad der Wiederherstellung der Systeme zu definieren.[455] Um Folgerisiken für das eigene Ökosystem zu verhindern, ist immerhin zu beachten, dass es zu keiner überstürzten Wiederaufnahme kommen darf.[456]

Denkbar ist aber, dass die Systeme nach zwei Stunden bzw. einem Tag noch nicht verfügbar sind; deshalb bedürfen die Finanzunternehmen für diese Szenarien eines Notfallplans («Disaster Recovery Plan»). Für das Alternativszenario ist es sinnvoll, dass die Finanzunternehmen ihre kritischen Funktionen, Transaktionen und Abhängigkeiten analysieren und Prioritäten für die Wiederaufnahme und Wiederherstellungsmassnahmen gesetzt haben. Diese Analysen fallen je nach Finanzunternehmen anders aus und können beispielsweise vorsehen, die Abwicklung kritischer Transaktionen aufrechtzuerhalten, während die Wiederherstellungsmassnahmen durchgeführt werden. Darüber hinaus ist es ratsam, auch für Situationen zu planen, in denen kritische Personen, Prozesse oder Systeme für längere Zeit nicht verfügbar sind. Hierfür braucht

452 Vgl. Kap. III.D.5.c), III.E.1.c) und III.E.7.b)aa).

453 *BIS/IOSCO*, 2016. Bank for International Settlements und International Organization of Securities Commissions, Guidance on cyber resilience for financial market infrastructures, 2016.

454 Für die Empfehlung von zwei Stunden vgl. *BIS/IOSCO*, 2016, 16; vgl. ferner *SBVg*, 2013, 10 für eine Empfehlung einer definierten Zeitspanne als verbindlicher Mindeststandard des Business-Continuity-Management.

455 SVV, 2015, 8; *SBVg*, 2013, 9.

456 Vgl. Kap. III.E.3.c); *FINMA*, Rundschreiben 2008/21, Rn. 135.11; vgl. auch *BIS/IOSCO*, 2016, 16.

es beispielsweise Abklärungen, ob das Finanzunternehmen sicher und praktikabel auf die manuelle Verarbeitung gewisser Prozesse und Verfahren, solange die automatisierten Systeme nicht verfügbar sind, zurückgreifen kann.[457]

c) Massnahmen für Daten

Neben der Gewähr, dass die Infrastrukturen und kritischen Geschäftstätigkeiten bei einem Cyberangriff verfügbar bleiben bzw. innerhalb kürzester Zeit wieder verfügbar sind, ist es wichtig, dass die Finanzunternehmen geeignete Massnahmen zur Datensicherung und Datensicherheit treffen.[458]

d) «Business Continuity Reviews» und «Business Continuity Tests»

Mit Bezug auf die Gegenmassnahmen und Wiederherstellungspläne ist es unerlässlich, dass die Finanzunternehmen die Betriebskontinuitätsplanung mit den Reaktions- und Wiederherstellungsplänen regelmässig überprüfen, aus alten Vorfällen lernen und die neusten Entwicklungen im Bereich der Cybersicherheit implementieren. Im Übrigen kann auch ein Test mit verschiedenen plausiblen Störungsszenarien (mit vollständigem oder nur teilweisem Ausfall der Standorte) und grösseren Systemausfällen zur Stabilität der Systeme beitragen und die Wiederherstellungspläne verbessern.[459]

4. Kommunikationsplan und Meldung

Als Teil des Business-Continuity-Management sind Kommunikationspläne zu erstellen. Ziel dieser Kommunikationspläne ist einerseits die Sicherstellung der Erreichbarkeit in Krisensituationen, andererseits die verantwortungsbewusste Offenlegung der Cybervorfälle bzw. der erheblichen Anfälligkeiten gegenüber Kunden und anderen Finanzunternehmen sowie der Öffentlichkeit. Ein Kommunikationsplan erlaubt ausserdem, mit den relevanten Akteuren zusammenzuarbeiten, um wirksam auf Cyberangriffe zu reagieren und sich von ihnen zu erholen, und zwar unabhängig davon, ob sie das Finanzunternehmen oder das Finanzsystem als Ganzes betreffen.[460] Da die Cyberbedrohungen keine Grenzen kennen und folglich in der Regel eine internationale Auswirkung

457 Vgl. Kap. III.D.5.c), III.E.3.c) und III.E.5.b); vgl. ferner *Weber/Henseler*, 2020, 608.

458 Vgl. für eine detailliertere Ausführung Kap. IV.B.7 und IV.C.5.

459 Vgl. Kap. III.C.2.b), III.D.5.a), III.D.5.c), III.E.3.c), insbesondere Art. 8.3 TRMG und III.E.7.b)aa).

460 Vgl. Kap. III.E.1.c) und IV.B.6; vgl. ferner *BIS/IOSCO*, 2016, 9; *SVV*, 2015, 8; *SBVg*, 2013, 12.

aufweisen, ist eine grenzüberschreitende Kommunikation anzustreben; sollte dies nicht möglich sein, ist zumindest eine schweizweite Kommunikation unter den Finanzunternehmen, mit anderen Branchen, spezialisierten IT-Unternehmen und den Behörden angezeigt.[461]

Der Kommunikationsplan dient nicht nur dem Austausch zwischen Finanzunternehmen und potenziell externen IT-Unternehmen, sondern auch der Meldung wesentlicher Cybervorfälle an die Behörden. Die FINMA hat mit der Aufsichtsmitteilung 05/2020[462] bekannt gemacht, dass wesentliche Cyberangriffe gestützt auf Art. 29 Abs. 2 FINMAG der FINMA zu melden sind. Diese Meldungen sind von grösster Bedeutung für den Schweizer Finanzplatz, da einerseits die Gefahr von Cyberangriffen weiterhin sehr hoch ist, andererseits die Cyberkriminellen nebst monetären Interessen oft auch auf die Beeinträchtigung der Verfügbarkeit, Vertraulichkeit und Integrität kritischer Technologieinfrastrukturen und sensitiver Informationen abzielen. Insbesondere im Lichte der Resultate der Eidgenössische Finanzkontrolle (EFK) könnten die neuen Ziele der Cyberkriminellen den Finanzunternehmen falsche Gewissheit bieten, die Vorfälle weiterhin nicht zu melden, und so noch grössere Probleme bereiten.[463]

Die EFK hat im Jahre 2020 in ihrer Prüfung der Aufsicht über die Cybersicherheit bei Finanzdienstleistern festgestellt, dass die allgemeine Meldepflicht nach Art. 29 Abs. 2 FINMAG noch nicht funktioniert und nicht alle relevanten Vorfälle gemeldet wurden.[464] Da nicht-monetäre Vorfälle möglicherweise den Anschein vermitteln könnten, dass der Vorfall ohne Nachverfolgungsmöglichkeiten und somit ohne Entdeckung durch die Behörden behebbar sei, wird ein falscher Anreiz geschaffen, keine Verbesserung dieser Situation anzustreben. Dies führt zu einer lückenhaften Kontrolle der FINMA im Bereich der Cybersicherheit und potenziell zur Gefährdung des Schweizer Finanzplatzes.

Die FINMA konkretisiert, dass im Hinblick auf Cyberangriffe die Wesentlichkeit vorliegt, wenn einerseits der Individualschutz (Schutz der Gläubiger, der Anleger sowie der Versicherten), andererseits die Funktionsfähigkeit der Finanzmärkte direkt oder indirekt beeinträchtigt sein könnte. Erfasst sind dabei erfolgreiche und teilweise erfolgreiche Cyberangriffe auf kritische Funktionen der Beaufsichtigten, bei denen der Ausfall oder die Fehlfunktion erhebliche Auswirkungen auf den Individualschutz hätte bzw. den Individualschutz er-

461 Vgl. auch Kap. IV.B.6; SVV, 2015, 8; SBVg, 2013, 12.

462 FINMA, Aufsichtsmitteilung 05/2020.

463 Vgl. Kap. III.B.1.b) und EFK, 2020, 18 f.

464 Vgl. EKF, 2020, 18 f.

heblich beeinträchtigen würde. Als Schutzziele erwähnt die FINMA einerseits die Verfügbarkeit der Systeme, andererseits aber auch die Integrität und Vertraulichkeit von Informationen bzw. Daten. Falls ein Cyberangriff auf die kritischen Aktiven[465] eines Beaufsichtigten dazu führt, dass Schutzziele von kritischen Funktionen und ihrer Geschäftsprozesse gefährdet sind, hat dies der Beaufsichtigte unverzüglich der FINMA zu melden.[466]

Die Kategorisierung in wesentliche und weniger wesentliche Vorfälle kann einerseits die Zurückhaltung der Finanzunternehmen bei der Meldung von Cybervorfällen[467] überwinden, andererseits die Funktionsfähigkeit des Finanzplatzes Schweiz verbessern, indem ein vergleichbarer Cybervorfall auf externe Systeme frühzeitig erkannt und gegebenenfalls verhindert werden kann.

In den Kommunikationsplänen ist auch die unverzügliche Meldung wesentlicher Cybervorfälle innerhalb kurzer Frist festzulegen. Für die Fristen sind verschiedene Konstellationen denkbar: Die FINMA führt in der Aufsichtsmitteilung aus, dass die Erstmitteilung über die Kritikalität des Cyberangriffs innerhalb von 24 Stunden zu erfolgen hat; die eigentliche Meldung jedoch erst innerhalb 72 Stunden.[468] Falls nach vollständig erfüllter Meldepflicht neue Entwicklungen oder Einschätzungen zur selben Attacke vorliegen, ist innerhalb dieser Frist von 72 Stunden eine erneute Meldung erforderlich, welche die Informationen auf den neusten Stand bringt.[469] Darüber hinaus ist es sinnvoll,

---

465 Als beispielhafte Aufzählung von kritischen Aktiven nennt die FINMA sensitive bzw. vertrauliche Informationen, gewisse Technologieinfrastrukturen, essenzielle Gebäude und Mitarbeitende, die kritischen Funktionen ausführen oder wesentlich dazu beitragen (s. FINMA, Aufsichtsmitteilung 05/2020, Anhang 2).

466 FINMA, Aufsichtsmitteilung 05/2020, 2 f.; auch die Financial Conduct Authority (FCA) hat ähnliche Abgrenzungskriterien für die Ermittlung der Wesentlichkeit eines Cybervorfalls, vgl. Principle 11 der Principles for Business in Kap. III.E.1.b)aa); vgl. auch *Mathys/Zollinger-Löw*, 2019, 2.

467 Vgl. Fn. 424.

468 Der DORA verfeinert die Vorgaben zu dieser Meldung und verlangt, dass «eine erste Meldung, die unverzüglich, spätestens jedoch am Ende des Geschäftstags oder – bei einem schwerwiegenden IKT-bezogenen Vorfall, der später als 2 Stunden vor dem Ende des Geschäftstages eintrat – spätestens 4 Stunden nach Beginn des folgenden Geschäftstags zu erfolgen hat» (Art. 17 Abs. 3 lit. a DORA).

469 FINMA, Aufsichtsmitteilung 05/2020, 5; gemäss DORA ist «spätestens 1 Woche nach der ursprünglichen Meldung gemäss Buchstabe a ein […] Zwischenbericht [erforderlich], gegebenenfalls gefolgt von aktualisierten Meldungen, wann immer eine entsprechende Statusaktualisierung vorliegt, sowie auf ausdrücklichen Antrag der zuständigen Behörde» (Art. 17 Abs. 3 lit. b DORA).

nicht später als einen Monat nach Übermittlung des ersten Berichts einen Abschlussbericht einzureichen; der Abschlussbericht erfolgt, nachdem die Ursachenanalyse abgeschlossen ist und sich die tatsächlichen Auswirkungen beziffern lassen.[470]

5. Datensicherheitsvorfälle nach Datenschutzgesetz (DSG)

Obwohl die Massnahmen im Rahmen des Risikomanagements mögliche Verletzungen der Datensicherheit zu verhindern versuchen, sind solche Verletzungen nicht ausgeschlossen. In diesem Zusammenhang ist insbesondere die Totalrevision des DSG und der VDSG von Bedeutung, welche Vorgaben zur Meldepflicht im Falle von Verletzungen der Datensicherheit und von Persönlichkeitsverletzungen vorsehen.

Die Meldepflicht gemäss DSG ist von der Meldepflicht gemäss FINMAG zu unterscheiden; die Finanzunternehmen müssen jegliche (wesentlichen) Cybervorfälle an die FINMA melden, die Meldepflicht gemäss DSG hingegen betrifft «bloss» Fälle, bei denen die Datensicherheit verletzt ist. Durch die Digitalisierung ist aber sehr wohl denkbar, dass die Verletzung der Datensicherheit aufgrund eines Cybervorfalls entsteht; in einer solchen Konstellation ist der Vorfall sowohl der FINMA als auch dem Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) zu melden.

Gemäss Art. 24 Abs. 1 nDSG (keine entsprechende Regelung im aDSG) meldet der Verantwortliche dem EDÖB so rasch als möglich eine Verletzung der Datensicherheit, die voraussichtlich zu einem hohen Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person führt.[471] Er nennt dabei mindestens die Art der Verletzung der Datensicherheit, deren Folgen und die ergriffenen oder vorgesehenen Massnahmen (Art. 24 Abs. 2 nDSG; keine entsprechende Regelung im aDSG). Der EDÖB führt zu dieser Gesetzesbestimmung weiter aus, dass die Verantwortlichen auch freiwillig eine Meldung abgeben können, falls sie das Risiko (noch) nicht als hoch einschätzen.[472]

Für die Finanzunternehmen ist von grosser Bedeutung, die Meldungen nach Art. 24 nDSG (keine entsprechende Regelung im aDSG) sowie etwaigen freiwilligen Meldungen gleichzeitig an eine zentrale Stelle abzugeben, auf die auch andere Finanzunternehmen Zugriff haben; dadurch können weitere Cybervor-

470 So auch Art. 17 Abs. 3 lit. c DORA.

471 *Füzesséry/Schneider*, 2020, 148; vgl. ferner *Weber/Henseler*, 2020, 607 f.

472 EDÖB, 2021, Das neue Datenschutzgesetz aus Sicht des EDÖB, 7.

fälle vergleichbarer Art verhindert und der Finanzplatz gestärkt werden.[473] Im Rahmen der Datensicherheit ist es angebracht, dass sich die Finanzunternehmen in einer Task Force organisieren, welche sich vornehmlich auf diese Fälle konzentrieren kann.

Eine Verletzung der Datensicherheit liegt vor, wenn ein Cybervorfall dazu führt, dass Personendaten unbeabsichtigt oder widerrechtlich verlorengehen, gelöscht, vernichtet oder verändert werden oder Unbefugten offengelegt oder zugänglich gemacht werden (Art. 5 lit. h nDSG; keine entsprechende Regelung im aDSG). In der Schweiz sind nur jene Verletzungen meldepflichtig, die das hohe Risiko überschreiten (Art. 24 Abs. 1 nDSG; keine entsprechende Regelung im aDSG); dabei gilt zu beachten, dass Finanzunternehmen, die grenzüberschreitend ihre Dienstleistungen anbieten bzw. Kunden aus dem Ausland betreuen, die Vorgaben der DSGVO beachten müssen, die gestützt auf das Auswirkungsprinzip einen sehr weiten Anwendungsbereich aufweist (Art. 3 DSGVO). Da Art. 33 DSGVO bei jeder Verletzung des Schutzes personenbezogener Daten zur Anwendung kommt, hat die DSGVO eine tiefere Schwelle für die Meldepflicht als das nDSG;[474] folglich haben grenzüberschreitend tätige Finanzunternehmen grundsätzlich keinen weiteren wesentlichen Handlungsbedarf mehr nach Inkrafttreten des nDSG, da sie bereits den strengeren Voraussetzungen des DSGVO nachkommen müssen.[475]

Im Übrigen ist die Nichteinhaltung der Vorgaben der Datensicherheit von Art. 8 nDSG und Art. 7 aDSG als Persönlichkeitsverletzung zu qualifizieren (Art. 30 Abs. 2 lit. a nDSG und Art. Abs. 2 lit. a aDSG) und führt bei einem Verstoss gegen die bundesrätlichen Mindestanforderungen zum Risiko einer Busse (Art. 61 lit. c nDSG; keine entsprechende Regelung im aDSG).[476]

6. Übungen und Tests

Übungen und Tests sind ein wesentlicher Bestandteil der Cybersicherheit und Cyber-Resilienz; sie sind als Teil des Business-Continuity-Management im Bereich der «Business Continuity Tests» einzuordnen.[477] Alle Elemente der Vor-

473 Vgl. Kap. IV.C.4.

474 In der Schweiz ist gemäss Art. 24 nDSG eine Meldung an den EDÖB erst bei einer Verletzung der Datensicherheit, die voraussichtlich zu einem hohen Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person führt, erforderlich.

475 Vgl. EDÖB, 2021, 6 f.; *Weber/Henseler*, 2020, 606; *Rosenthal*, 2020a, 2.

476 Vgl. für Massnahmen zur Verhinderung von Datensicherheitsvorfällen Kap. IV.B.7.

477 Vgl. SVV, 2015, 6 f. und 9; SBVg, 2013, 11.

gaben für Übungen und Tests sind vor deren Einführung bei einem Finanzunternehmen auf die Gesamtwirksamkeit hin zu prüfen; zudem haben die Finanzunternehmen sicherzustellen, dass eine regelmässige Kontrolle nach der Einführung der Systeme durchgeführt wird (z.B. Prüfung auf korrekte Implementierung oder auf die Erzielung gewünschter Ergebnisse).[478]

Ein solides Testverfahren erlaubt Schwachstellen, Mängel oder Lücken zu ermitteln und liefert aussagekräftige Beiträge zum Cyber-Risikomanagementprozess des Finanzunternehmens. Die Analyse der Testergebnisse gibt Hinweise darauf, wie Schwachstellen oder Mängel in der Cyber-Resilienz zu korrigieren und festgestellte Lücken zu verringern oder zu beseitigen sind.[479]

a) Anforderungen an Prüfer

Die FINMA hat im Jahre 2017 die spezifisch auf den IT-Bereich spezialisierte Querschnittsfunktion «Operationelle, Cyber- und IT-Risiken» (B-OCI) gegründet. B-OCI ist das Kompetenzzentrum für operationelle Risiken und führt u.a. Vor-Ort-Kontrollen durch. Problematisch ist, dass keine Fachspezialisten der Gruppe B-OCI bei Banken der Kategorie 3, 4 und 5 – also 98% der beaufsichtigten Banken – gewissen Aufsichtstätigkeiten nachgehen.[480] Die Übungen und Tests können durch unabhängige, interne Personen durchgeführt werden; jedoch ist – da bereits die Selbstregulierung bei der Meldepflicht gemäss Eidgenössische Finanzkontrolle (EFK) nicht gut funktioniert[481] – die Prüfung durch externe Personen sinnvoll.

Die Finanzunternehmen haben folglich sicherzustellen, dass die Prüfer von höchster Eignung sind und über technische und organisatorische Fähigkeiten verfügen; sie müssen ausserdem spezifisches Fachwissen im Bereich der durchzuführenden Tests besitzen. Bei externen Prüfern ist zudem die Gewähr für einen angemessenen Schutz von vertraulichen Informationen des Finanzunternehmens zwecks Vermeidung geschäftlicher Risiken erforderlich. Darüber hinaus ist bei externen Prüfern auch eine ordnungsgemässe und vollständige Berufshaftpflichtversicherung gegen das Risiko von Fehlverhalten

478 *BIS/IOSCO*, 2016, 18; vgl. ferner SVV, 2015, 6; *SBVg*, 2013, 11.

479 *BIS/IOSCO*, 2016, 18; *SBVg*, 2013, 11.

480 *EFK*, 2020, 13, 17 und 21.

481 *EFK*, 2020, 17 ff.

und Fahrlässigkeit sinnvoll.[482] Denkbar ist ausserdem eine Cooling-Off-Periode (Rotationspflichten bzw. Abkühlfristen), damit die Unabhängigkeit und Wirksamkeit der Prüfungen gewahrt sind.

b) Methoden

Die Finanzunternehmen stellen sinnvollerweise ein umfassendes Testprogramm auf, um die Wirksamkeit des Cyber-Resilienz-Rahmens regelmässig zu testen; durch Simulation plausibler Cybervorfälle bzw. Szenarien können die Testmethoden überprüft werden. Die Ergebnisse des Testprogramms dienen den Finanzunternehmen als Grundlage, um die kontinuierliche Verbesserung der Cyber-Resilienz sicherzustellen. Für die Durchführung der Tests ist es angebracht, verschiedene Testmethoden bzw. -praktiken, die auch kombiniert werden können, anzuwenden. Denkbar sind folgende Methoden und Praktiken:[483]

aa) Schwachstellenbewertung

Schwachstellenbewertungen können Sicherheitsschwachstellen in den Systemen und Prozessen identifizieren und bewerten. Finanzunternehmen haben ein Verfahren zur Behebung der Schwachstellen einzurichten und mit einer anschliessenden Kontrolle zu beurteilen, ob die Lücken vollständig geschlossen wurden. Die Schwachstellenbewertung ist grundsätzlich vor der Einführung bzw. Umstellung neuer oder bestehender Dienste durchzuführen und hat jede Art von ausnutzbaren Schwachstellen (technische, prozessuale, organisatorische und entstehende) zu erkennen.[484]

bb) Szenariobasierte Tests

Die Reaktions- und Wiederherstellungspläne der Finanzunternehmen sind in regelmässigen Abständen zu prüfen und zu testen. Diese Tests sollen verschie-

---

482 Vgl. auch Art. 24 DORA.

483 Vgl. BIS/IOSCO, 2016, 18 f.; EZB 2018a, 42 ff.; weitere vorstellbare Methoden sind gemäss Art. 22 DORA die Bewertungen und Überprüfungen der Anfälligkeit, Analysen von Open-Source-Software, Bewertungen der Netzsicherheit, Lückenanalysen, Analysen der physischen Sicherheit, Überprüfungen der physischen Sicherheit, Fragebögen und Scansoftwarelösungen, Quellcodeprüfungen soweit durchführbar, Kompatibilitätstests, Leistungstests oder End-to-End-Tests. Die Tests sind insbesondere entsprechend den Besonderheiten der jeweiligen Finanzunternehmen durchzuführen.

484 Vgl. ferner Kap. III.C.2.b), III.D.5.b), III.E.3.c) und III.E.7.b)aa).

dene Szenarien abdecken, z.B. externe, aber plausible Cyberangriffe simulieren und so die Governance-Mechanismen, den Schutz bzw. die Prävention, die Erkennung der Cybergefahren, die Kommunikationspläne und die Wiederherstellungsmassnahmen auf die Probe stellen. Ferner könnten diese Szenarien auch die Datenzerstörung, die Datenintegrität, den Datenverlust sowie die System- und Datenverfügbarkeit umfassen. Solche Tests greifen auf «Cyber Threat Intelligence» (CTI) zurück und versuchen, die Merkmale der Cyberbedrohungen nachzuahmen; gleichzeitig erlaubt diese Methode, die Fähigkeit der Mitarbeitenden und Prozesse auf denkbare (ungewohnte) Szenarien zu testen, um so im Ernstfall eine stärkere operative Widerstandsfähigkeit zu erreichen.

cc) Penetrationstests

Mit den Penetrationstests können die Finanzunternehmen Schwachstellen, die potenziell die Systeme, Netzwerke, Personen oder Prozesse betreffen, identifizieren. Eine umfassende Kontrolle der Systemsicherheit ist erreichbar durch Tests, die tatsächliche Angriffe auf die Systeme simulieren.[485] Darüber hinaus sind die Finanzunternehmen gehalten, insbesondere auch Penetrationstests für Systeme, die mit dem Internet verbunden sind, regelmässig durchzuführen; dies ist vor allem erforderlich, wenn die Finanzunternehmen ihre Systeme aktualisieren oder neu einführen.

Zudem erweist es sich für Finanzunternehmen als sinnvoll, szenariobasierte Penetrationstests durchzuführen, welche Vorfälle simulieren, die mehrere Teile des Ökosystems des Finanzunternehmens betreffen. Dieses Vorgehen erlaubt eine angemessene Vorbereitung auf potenzielle Komplexitäten, indem sie gegenseitige Abhängigkeiten und mögliche schädliche Einflüsse – die im Rahmen der Cyber-Resilienz berücksichtigt werden sollten – sowohl auf geschäftlicher als auch auf betrieblicher Ebene ermitteln und analysieren.[486]

Ferner ist es möglich, die Penetrationstests sowohl als Blackbox- als auch als Greybox-Tests durchzuführen. Bei Blackbox-Tests kennt der Tester nur die IP-Adressen und die URLs, nicht aber die übrige Testumgebung. Bei Greybox-Tests handelt es sich um Tests mit Anmeldedaten, d.h. der Tester hat dieselben Rechte und dieselbe Umgebung wie ein normaler Kunde. Schliesslich ist auch eine Adaptation der «Intelligence-Led»-Penetrationstests vorstellbar, welche die Handlungen von Cyberangreifern nachahmt, die darauf abzielen,

485 Ähnliche Simulation tatsächlicher Angriffe wie in Kap. IV.C.6.b)bb).

486 Vgl. EZB, 2018a, 46.

die wichtigen Unternehmensdienste einer Organisation zu beschädigen sowie die technologischen Anlagen und Prozesse zu stören. Diese Unterteilung der Penetrationstests erlaubt es den Finanzunternehmen, potenziell vorstellbare Szenarien zu simulieren.[487]

dd) Red-Team-Tests

Mit den Red-Team-Tests besteht für die Finanzunternehmen die Möglichkeit, ihre eigenen Organisationen und Ökosysteme auf den Prüfstand zu stellen, indem sie in einem kontrollierten Umfeld die Perspektive eines Cyberangreifers einnehmen. Die Red-Teams dienen dazu, mögliche Schwachstellen und die Wirksamkeit der Schutzmassnahmen der Finanzunternehmen zu testen. Die Red-Teams können aus eigenen Mitarbeitenden und/oder aus externen Experten bestehen; sie müssen jedoch auf alle Fälle unabhängig von den zu testenden Funktionen sein. Bei den Red-Team-Tests besteht die Möglichkeit, auf das «European Framework for Threat-Intelligence Based Ethical Red Teaming» (TIBER-EU) zurückzugreifen.[488]

Aufgrund möglicher Kombinationen ist auch ein «Intelligence-Led»-Red-Team-Test vorstellbar; dabei werden verschiedene Techniken eingesetzt, um einen Cyberangriff auf die Einrichtung (d.h. auf die Mitarbeitenden, Verfahren und Technologien) zu simulieren. Dieser Test umfasst sowohl Angriffe durch böswillige Aussenstehende als auch «Angriffe» durch eigene Mitarbeitende und hilft den Finanzunternehmen, ihre Schutz-, Erkennungs- und Reaktionsfähigkeiten zu bewerten. Das TIBER-EU empfiehlt, dass der Test ohne Kenntnis der Sicherheits- oder Reaktionsteams des Finanzunternehmens[489] durchgeführt wird; nur eine kleine Gruppe darf vom Test wissen, damit die Wirksamkeit der geltenden Sicherheitsmassnahmen angemessen geprüft und allenfalls angepasst werden kann.[490]

---

487 Vgl. zur Umsetzung der Penetrationstests in verschiedenen Rechtsordnungen Kap. III.B.1.a), III.C.2.b), III.D.2.e), III.E.1.d)aa), III.E.3.c), III.E.4.b), III.E.6.b) und III.E.7.b)aa).

488 EZB, 2018b. Europäische Zentralbank (EZB), European Framework for Threat-Intelligence Based Ethical Red teaming, Frankfurt am Main 2018.

489 Das TIBER-EU nennt dises Team das «Blue Team».

490 Vgl. ferner Kap. III.C.2.b).

c) Prüfungen und erweiterte Prüfungen

Um eine ausreichende Sicherheit und Resilienz gewährleisten zu können, ist es für Finanzunternehmen sinnvoll, die Übungen und Tests in regelmässigen Abständen durchzuführen; denkbar sind jährliche oder halbjährliche Prüfungen bzw. auch Prüfungen in kleineren Abständen.[491]

Erweiterte Prüfungen können in grösseren Abständen durchgeführt werden; Art. 23 DORA schlägt eine erweiterte Prüfung anhand bedrohungsorientierter Penetrationstests mindestens alle drei Jahre vor. Dieser Test hat alle kritischen Funktionen der Finanzunternehmen einzubeziehen und wird an Live-Produktsystemen durchgeführt. Hierfür müssen die Finanzunternehmen ihre relevanten Prozesse, Systeme und Technologien, die zur Unterstützung kritischer Funktionen und Dienste erforderlich sind, ermitteln; auch die ausgelagerten Prozesse und Systeme sind in diese Ermittlung miteinzubeziehen und deren Resilienz sicherzustellen.

7. Weiterentwicklung

Der Rahmen für die Cybersicherheit und Cyber-Resilienz beschränkt sich nicht nur auf bereits bekannte Gefahren, sondern muss eine kontinuierliche Cybersicherheit und Cyber-Resilienz in diesem sich schnell verändernden Bedrohungsumfeld gewährleisten. Die Finanzunternehmen sind verpflichtet, um mit der raschen Entwicklung von Cyberbedrohungen Schritt halten zu können, einen anpassungsfähigen Rahmen für die Cybersicherheit und Cyber-Resilienz einzuführen, der sich mit der dynamischen Natur von Cyber-Risiken weiterentwickelt. Dies ermöglicht den Finanzunternehmen, Sicherheitsbedrohungen und Schwachstellen zu identifizieren, zu bewerten und zu verwalten sowie geeignete Schutzmassnahmen frühzeitig in ihre Systeme zu implementieren.[492] Ein Finanzunternehmen sollte folglich darauf abzielen, eine Kultur des Bewusstseins für Cyber-Risiken zu schaffen, bei der es seine Resilienz auf allen Ebenen häufig und regelmässig neu bewertet.[493]

Die Finanzunternehmen müssen systematisch die wichtigsten Lehren aus Cybervorfällen innerhalb und ausserhalb der Organisation ziehen und analysie-

---

491 Vgl. zu regelmässigen Prüfungen auch Kap. III.B.1.a), III.C.2, III.D.5, III.E.1.b)bb), III.E.3.c), III.E.6.b), III.E.6.c), III.E.7.b)aa) und III.E.7.b)bb).

492 Vgl. auch *BIS/IOSCO*, 2012, 94 (Principle 17, Consideration 7).

493 Vgl. *BIS/IOSCO*, 2016, 22; vgl. ferner Kap. II.C.3 und III.E.1.b)bb); Art. 13 DORA; *NCSC*, 2018, 2; *JCSH*, 2017, 12 f.

ren, um so die eigene Resilienzfähigkeit zu verbessern. Ausserdem ist es sinnvoll, die technologischen Entwicklungen aktiv zu verfolgen und sich über neue Verfahren der Cyberbedrohungen auf dem Laufenden zu halten. Mit der Aneignung neuer Kenntnisse und Fähigkeiten ist auch das Risikomanagement des Unternehmens laufend anzupassen, damit es sowohl den bestehenden als auch den neuen, sich entwickelnden Formen von Cyberangriffen wirksam begegnen kann.[494]

Mit dem fortlaufenden Lernprozess und den Weiterentwicklungen sind gute reaktive Kontrollmechanismen verbunden. Jedoch ist sinnvollerweise darüber hinaus auch ein proaktiver Schutz vor künftigen Cybervorfällen im Sinne von vorausschauenden Fähigkeiten aufzubauen. In diesem Umfeld ist es empfehlenswert, auch vorausschauende Fähigkeiten zu erwerben, um zukünftige Cybervorfälle besser antizipieren zu können. Dies gelingt durch Auswertung verschiedener interner und externer Quellen, die Verhaltens- und Systemaktivitäten erfassen und definieren.[495]

D. Aufsicht über Drittanbieter

Neben den unternehmensinternen Risiken sind im Bereich der Cybersicherheit auch Risiken als Folge des Outsourcing von Bedeutung. Ein Outsourcing (bzw. eine Auslagerung) von Systemen, Verfahren oder Prozessen liegt vor, wenn die Finanzunternehmen einen Dienstleister als Drittanbieter beauftragen, selbstständig und dauernd Funktionen, die für die Geschäftstätigkeit des Unternehmens wesentlich sind, ganz oder teilweise zu erfüllen.[496] Gegenwärtig ist insbesondere die Nutzung von Cloud-Dienstleistungen[497], bei der ein Outsourcing der IT-Funktionen stattfindet, ein wichtiges Thema für Finanzdienstleister.[498]

494 So auch *BIS/IOSCO*, 2016, 22.

495 *Ibid.*

496 *FINMA*, Rundschreiben 2018/3, Rn. 3.

497 Die Cloud-Dienstleistungen ermöglichen einen bequemen, bedarfsgerechten Netzwerkzugriff auf einen gemeinsamen Pool konfigurierbarer Computing-Ressourcen (z.B. Netzwerke, Server, Speicher, Anwendungen und Dienste), die mit minimalem Verwaltungsaufwand oder geringer Interaktion mit dem Dienstanbieter schnell bereitgestellt werden können (*Weber/Henseler*, 2020, 605 gestützt auf die Definition von «Cloud Computing» des Computer Security Resource Center des National Institute of Standard and Technology (NIST), aufrufbar unter <https://csrc.nist.gov/projects/cloud-computing>).

498 *Weber/Henseler*, 2020, 605; *Rosenthal*, 2020a, Rn. 2; vgl. auch *SBVg*, 2020, 4.

Die nachfolgenden Ausführungen zu den Herausforderungen des Outsourcing nehmen insbesondere Bezug auf das FINMA Rundschreiben 2018/3 «Outsourcing», die Empfehlungen des Cloud-Leitfadens der Schweizerischen Bankiervereinigung (SBVg) und die Regelungen im DORA. Vorerst sind die allgemeinen Grundsätze der Aufsicht über Drittanbieter darzulegen (1.) und anschliessend sind die Steuerung bzw. Governance (2.) sowie die Prüfung und Aufsicht der Drittanbieter zu behandeln (3.).

1. Allgemeine Grundsätze

Gemäss dem FINMA Rundschreiben 2018/3 «Outsourcing» sind zwar auch wesentliche Funktionen auslagerbar, nicht jedoch die Oberleitung, die Aufsicht und die Kontrolle durch das Oberleitungsorgan, die zentralen Führungsaufgaben der Geschäftsleitung sowie die Funktionen, die für das Fällen strategischer Entscheidungen zuständig sind.[499]

Es liegt in der Verantwortung der Finanzunternehmen, die Überwachung der Risiken durch die Drittanbieter sicherzustellen. Auch bei der Auslagerung ist der Grundsatz der Verhältnismässigkeit bzw. ein risikobasierter Ansatz zu verfolgen, d.h. die Finanzunternehmen haben das Ausmass, die Komplexität und die Relevanz der ausgelagerten Systeme sowie die potenziellen Risiken der Auslagerung zu berücksichtigen. Die entsprechenden Überlegungen sind im Lichte der eigenen Grösse und der Komplexität des eigenen Geschäftsmodells vorzunehmen.[500]

Bevor ein Finanzunternehmen eine Funktion vertraglich an einen Drittanbieter auslagert, ist zunächst zu beurteilen, ob – wie erwähnt – die Funktion tatsächlich auslagerbar ist, ob alle relevanten Risiken im Rahmen der Auslagerung ermittelt worden sind und ob Interessenkonflikte bestehen könnten. In der vertraglichen Vereinbarung sind die Zuständigkeiten des Drittanbieters (insbesondere bzgl. Schnittstellen und Verantwortlichkeiten) und darüber hinaus die aktuellen und angemessenen Standards für die Cybersicherheit festzuhalten.[501]

499 FINMA, Rundschreiben 2018/3, Rn. 7 ff.

500 SBVg, 2020, 9 und 20; vgl. ferner Art. 25 Abs. 2 DORA.

501 FINMA, Rundschreiben 2018/3, Rn. 19; Vgl. SBVg, 2020, 14; Art. 25 Abs. 5 und 6 DORA.

In den Vertrag zur Auslagerung sind überdies angemessene Kündigungsmöglichkeiten aufzunehmen, um eine solide Überwachung des Drittanbieters zur Einhaltung eigener Pflichten sicherstellen zu können. Zu den «kritischen» Situationen gehören:[502]

- Verstoss des Drittanbieters gegen Gesetze, Verordnungen, Verfügungen, Rundschreiben oder anerkannte bzw. obligatorische Selbstregulierungen;
- Umstände, welche die Wahrnehmung der vertraglichen Pflichten beeinträchtigen könnten und erst während der Überwachung des Risikos aufgefallen sind (z.B. aufgrund wesentlicher Änderungen, die sich auf das Vertragsverhältnis auswirken);
- Nachweisliche Schwächen des Drittanbieters;
- Vertraglich bedingte Umstände, welche die angemessene Aufsicht des Finanzunternehmens durch die Aufsichtsbehörde nicht mehr zulassen.

Ausserdem haben die Finanzunternehmen auch zu bedenken, dass sie bei einem allfälligen Ausscheiden aus dem Vertrag den Geschäftsbetrieb ohne grössere Störung weiterführen müssen. Sie sind stets verpflichtet, die eigenen aufsichtsrechtlichen Anforderungen einzuhalten; ferner darf das Ausscheiden aus dem Vertrag die Kontinuität und Qualität der Leistungserbringung nicht beeinträchtigen.

Aus diesem Grund ist erforderlich, dass die Finanzunternehmen eine nahtlose Weiterführung aller Geschäftstätigkeiten gewährleisten. Hierfür sind Übergangspläne, welche die Löschung der vertraglichen Funktionen und Daten beim ehemaligen Anbieter berücksichtigen sowie die sichere und vollständige Weiterleitung an einen alternativen Anbieter erlauben, zu erarbeiten.[503]

2. Governance

Unter Governance ist die allgemeine Steuerung der Auslagerung von Systemen und Prozessen zu verstehen. In diesem Zusammenhang ist zunächst ein Verfahren vorzusehen, das den Rahmen für die generelle Entscheidung zur Beschaffung von Dienstleistungen Dritter erfasst (a)). Darüber hinaus ist es wichtig, die Verantwortung und Rollen einer Auslagerung zu regeln (b)). Sind diese Punkte festgelegt, kommt der Auswahl und Instruktion des zukünftigen Drittanbieters ebenfalls grosse Bedeutung zu (c)).

502 Vgl. FINMA, Rundschreiben 2018/3, Rn. 33; Art. 25 Abs. 8 DORA.

503 FINMA, Rundschreiben 2018/3, Rn. 18 f. und 33; Art. 25 Abs. 8 DORA.

a) Entscheid

Denkbar ist sowohl die Auslagerung standardisierter Infrastrukturen als auch individuell erforderlicher, spezifischer Prozesse in die Cloud. Um alle potenziellen Auslagerungen vergleichbaren Voraussetzungen zu unterwerfen, empfiehlt die Schweizerische Bankiervereinigung (SBVg) ein strukturiertes Verfahren für die Entscheidung zur Beschaffung von Cloud-Dienstleistungen.[504]

Damit die Finanzunternehmen ihre eigenen Risikomanagement-Vorgaben weiterhin einhalten können, ist eine vorangehende Risikoanalyse bei der Entscheidung der Auslagerung unerlässlich; deshalb sind die Finanzunternehmen zu verpflichten, im Rahmen ihres Risikomanagements vorgängig eine Strategie für das Risiko der Drittanbieter zu verabschieden.[505] Mit der Risikoanalyse wird den Chancen und Risiken der Auslagerung Rechnung getragen sowie die Möglichkeit zur Auslagerung der Dienstleistungen ermittelt.[506] Insbesondere haben die Banken sicherzustellen, dass jene Drittanbieter, die im Rahmen der ausgelagerten Dienstleistungen die Daten bearbeiten (v.a. Kundenidentifikationsdaten nach FINMA Rundschreiben 2008/21[507]), sich verpflichten, diese bearbeiteten Daten angemessen zu schützen.[508]

Stellen die Finanzunternehmen bei der Entscheidung zur Auslagerung fest, dass damit Risiken einhergehen, haben sie mitigierende Massnahmen einzurichten, die im Risikomanagement des betroffenen Finanzunternehmens reflektiert werden müssen. Diese Massnahmen sind während der Laufzeit der Auslagerung regelmässig zu überprüfen und zu befolgen.[509]

b) Verantwortung

Gegenüber der FINMA trägt weiterhin das Finanzunternehmen selbst die Verantwortung, d.h. es haftet in vollem Umfang für die Einhaltung der vertrag-

504 SBV*g*, 2020, 24.

505 Vgl. *FINMA*, Rundschreiben 2018/3, Rn. 18; zum Risikomanagement im Zusammenhang mit der Cybersicherheit Kap. IV.B; vgl. zu den Sicherheitsanforderungen *FINMA*, Rundschreiben 2018/3, Rn. 24 f.; vgl. ferner Art. 25 Abs. 3 DORA.

506 Vgl. für die auslagerbaren Funktionen *FINMA*, Rundschreiben 2018/3, Rn. 7 ff.; vgl. ferner Kap. IV.D.1.

507 *FINMA*, Rundschreiben 2008/21, Rn. 9 ff. und Anhang 3 Rn. 52.

508 Vgl. SBV*g*, 2020, 24. Dieser Schutz der Kundenidentifikationsdaten ist insbesondere auch im Rahmen des Bankkundengeheimnisses gemäss Art. 47 BankG von Bedeutung, vgl. hierzu Kap. III.B.3.b).

509 Vgl. *FINMA*, Rundschreiben 2018/3, Rn. 24 f.; vgl. auch SBV*g*, 2020, 24 f.

lichen Pflichten, als würde es diese selbst erbringen; insbesondere unterliegt das Finanzunternehmen unmittelbar der FINMA-Aufsicht, nicht der kontrahierte Drittanbieter, d.h. es muss zu jeder Zeit die ordnungsgemässe Geschäftsleitung gewährleisten.[510]

Das Finanzunternehmen braucht hierfür eine verantwortliche Stelle, welche fortlaufend die Leistungen des Drittanbieters beurteilt und entscheidet, ob allfällige Massnahmen erforderlich sind. Auch wenn der Drittanbieter dem Finanzunternehmen Weisungsrechte einzuräumen hat,[511] ist es möglich, dass sich der Drittanbieter – vor allem im Rahmen von hochstandardisierten Dienstleistungen – die Design-Autorität vertraglich zusprechen lässt, d.h. sich die Freiheit ausbedingt, eigene Betriebsmodelle oder andere massgebliche Faktoren festzulegen.[512]

Neben der aufsichtsrechtlichen Verantwortung müssen die Finanzunternehmen potenziell auch andere finanzmarktrechtliche Vorschriften, das Bankkundengeheimnis oder das Datenschutzgesetz (DSG, z.B. falls Personendaten bearbeitet werden) berücksichtigen.[513] Im Zusammenhang mit dem nDSG haben sowohl das Finanzunternehmen (als Verantwortlicher nach Art. 5 lit. j nDSG[514]; keine entsprechende Regelung im aDSG) als auch die Drittanbieter (als Auftragsbearbeiter nach Art. 5 lit. k nDSG[515]; keine entsprechende Regelung im aDSG) die datenschutzrechtlichen Vorgaben zu beachten.[516] Dabei ist insbesondere Art. 9 nDSG (Art. 10*a* aDSG) von Bedeutung, wonach sich das Finanzunternehmen als Verantwortlicher vergewissern muss, dass der Drittanbieter als Auftragsbearbeiter in der Lage ist, die Datensicherheit zu gewährleisten (Art. 9 Abs. 2 nDSG und Art. 10*a* Abs. 2 aDSG). Diese Auftragsbearbeitung ist auch im revidierten Datenschutzgesetz ohne Einwilligung der betroffenen Personen zulässig.[517]

---

510 FINMA, Rundschreiben 2018/3, Rn. 23, vgl. ferner Art. 25 Abs. 1 DORA.

511 FINMA, Rundschreiben 2018/3, Rn. 20 f.; vgl. auch Kap. IV.D.3.

512 SBV*g*, 2020, 25.

513 Für das Bankkundengeheimnis, vgl. Kap. III.B.3.b).

514 Ein Verantwortlicher ist, wer «über den Zweck und die Mittel der Bearbeitung entscheidet» (*Botschaft DSG*, BBl 2017, 7023).

515 Auftragsbearbeiter ist insbesondere, wer die Datenbearbeitung bloss nach Weisungen ausführt (z.B. Cloud-Provider, vgl. *Rosenthal*, 2020b, Rn. 15).

516 Vgl. zu den Begrifflichkeiten des Verantwortlichen und des Auftragsbearbeiters *Botschaft DSG*, BBl 2017, 7023 und *Rosenthal*, 2020b, Rn. 13 ff.

517 *Rosenthal*, 2020b, Rn. 57.

Die Vereinbarung zwischen dem Finanzunternehmen und dem Drittanbieter sollte alle Rechte und Pflichten, die Verantwortlichkeiten sowie die Rollen der jeweiligen Parteien oder Beteiligten regeln.[518]

c) Auswahl und Instruktion

Die Finanzunternehmen sind verpflichtet, bei der Auswahl die professionellen Fähigkeiten sowie die finanziellen und personellen Ressourcen der Drittanbieter zu prüfen; ferner haben sie dem Konzentrationsrisiko Rechnung zu tragen, falls sie mehrere Dienstleistungen an denselben Drittanbieter auslagern.[519]

Bei der Auswahl eines Drittanbieters ist ausserdem dessen Bereitschaft zur Übernahme von finanzmarktrechtlichen (inkl. Bankkundengeheimnis) und datenschutzrechtlichen Vorgaben zu berücksichtigen. Soll der Drittanbieter Kundenidentifikationsdaten oder andere Personendaten bearbeiten, ist die Vertraulichkeit und Sicherheit der Daten ein massgebliches Kriterium sowie integraler Bestandteil der Due Diligence.[520]

Ferner sind im Rahmen der Datensicherheit und des Datenschutzes des Finanzunternehmens auch die Daten, die durch den Drittanbieter bearbeitet werden, zu klassifizieren.[521] Damit insbesondere das Bankkundengeheimnis weiterhin eingehalten wird, sind technische Massnahmen zum Schutz der Kundenidentifikationsdaten einzuführen. Als denkbare Massnahmen kommen die Anonymisierung, Pseudonymisierung oder Verschlüsselung der Daten in Betracht. Wichtig ist, dass die Übermittlung der Kundenidentifikationsdaten zu jeder Zeit verschlüsselt zu erfolgen hat. Die Finanzunternehmen können zusätzlich auch vertragliche Massnahmen zum Schutz der Kundenidentifikationsdaten ergreifen; es lassen sich insbesondere angemessene technische und organisatorische Massnahmen im Vertrag festhalten oder Verpflichtungen für Drittanbieter zur Wahrung der Vertraulichkeit vorsehen.[522]

3. Prüfung und Aufsicht

Schliesslich ist auch mit Bezug auf Drittanbieter eine regelmässige Prüfung der Einhaltung von anwendbaren oder vertraglich übertragenen Anforderun-

518 SBV*g*, 2020, 25.

519 FINMA, Rundschreiben 2018/3, Rn. 17.

520 SBV*g*, 2020, 26.

521 Vgl. zur Klassifikation der Cyberrisiken und damit einhergehend der Daten Kap. IV.C.2.

522 SBV*g*, 2020, 33 ff.

gen (insb. gesetzliche oder regulatorische Anforderungen an das Outsourcing, an den Datenschutz oder an die Informationssicherheit) erforderlich. In Bezug auf die Aufsicht ist eine enge Zusammenarbeit zwischen Finanzunternehmen und Drittanbieter sinnvoll; für die Prüfung des Drittanbieters ist – ähnlich wie bei der Aufsichts-Prüfung gemäss Art. 24 FINMAG und Art. 84 FinfraG – als unabhängige Prüfgesellschaft entweder eine gesonderte interne Prüfstelle des Finanzunternehmens oder eine externe Prüfgesellschaft heranzuziehen. Ferner können mehrere Finanzunternehmen auch sogenannte Poolaudits organisieren, falls die Prüfgesellschaft die notwendige Unabhängigkeit und fachliche Kompetenz aufweist.[523]

Obwohl weiterhin das Finanzunternehmen unmittelbar der Aufsicht der FINMA unterliegt,[524] haben die Drittanbieter die aufsichtsrechtlichen Bestimmungen einzuhalten und zuzulassen, dass die FINMA die Einhaltung dieser Bestimmungen überprüft. Angebracht ist, dass die Finanzunternehmen zu ihren eigenen Gunsten, zu Gunsten ihrer Prüfgesellschaften sowie zu Gunsten der FINMA jederzeit ein vollumfängliches und ungehindertes Einsichts- und Prüfrecht in die vertraglichen Vereinbarungen aufnehmen;[525] darüber hinaus ist vertraglich zu vereinbaren, dass der Drittanbieter der FINMA sämtliche Auskünfte und Unterlagen zur ausgelagerten Tätigkeit zur Verfügung stellt, selbst wenn der Drittanbieter nicht der FINMA-Aufsicht untersteht.[526]

Die Auslagerung der Dienstleistungen darf zudem die Aufsicht durch die FINMA nicht erschweren;[527] auch Auslagerungen ins Ausland sind dennoch erlaubt, sofern das Finanzunternehmen (beispielsweise vertraglich) sicherstellen kann, dass es selbst, seine Prüfgesellschaft und die FINMA die Einsichts- und Prüfrechte durchsetzen können.[528]

523 SBV*g*, 2020, 42 f.; der Cloud-Leitfaden sieht auch vor, dass allenfalls auch die FINMA selbst die Prüfung durchführen kann (SBV*g*, 2020, 42 f.).

524 Vgl. IV.D.2.b).

525 FINMA, Rundschreiben 2018/3, Rn. 26.

526 FINMA, Rundschreiben 2018/3, Rn. 29.

527 FINMA, Rundschreiben 2018/3, Rn. 28.

528 FINMA, Rundschreiben 2018/3, Rn. 30; vgl. ferner SBV*g*, 2020, 43.

V. Weitere Rechtsbereiche

Im Rahmen der Cybersicherheit und Cyber-Resilienz sind grundsätzlich noch weitere Rechtsbereiche relevant, die anzusprechen als gerechtfertigt erscheint. Nachfolgend ist zunächst zu untersuchen, welche Aufsichtsbehörden für die Cybersicherheit in den behandelten Bereichen zuständig sind (A.). Ausserdem braucht es auch Sanktionsmechanismen, die greifen, falls die Finanzunternehmen den geltenden Vorgaben nicht nachkommen (B.). Schliesslich lohnt es sich, die verschiedenen zivilrechtlichen Haftungskonstellationen kurz zu erörtern (C.).

A. Aufsichtsbehörden

Die Finanzunternehmen haben verschiedenen gesetzlichen und regulatorischen Vorgaben nachzukommen. Die Aufsicht über die Einhaltung dieser Vorschriften obliegt in der Schweiz unterschiedlichen Behörden; als Aufsichtsbehörde kommen die Eidgenössische Finanzmarktaufsicht FINMA, die Schweizerische Nationalbank sowie der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte in Frage, die je unterschiedliche Cybersicherheitsaspekte beurteilen.

1. Eidgenössische Finanzmarktaufsicht (FINMA)

Gemäss Art. 5 FINMAG beaufsichtigt die Eidgenössische Finanzmarktaufsicht (FINMA) den Finanzmarkt. Sie hat den gesetzlichen Auftrag, die Finanzmarktkunden – namentlich Gläubiger, Anleger und Versicherte – sowie die Funktionsfähigkeit der Finanzmärkte zu schützen.

Als unabhängige, öffentlich-rechtliche Anstalt reguliert die FINMA den Finanzmarkt durch Rundschreiben, welche die Anwendung der Finanzmarktgesetzgebung konkretisieren, und durch Verordnungen, sofern dies die Finanzmarktgesetzgebung zulässt. Die FINMA kann darüber hinaus auch Selbstregulierungen als Mindeststandards festlegen, wie sie dies für Teile des

Business-Continuity-Managements getan hat (Art. 7 FINMAG).[529] Zudem hat die FINMA gestützt auf die Meldepflicht gemäss Art. 29 Abs. 2 FINMAG mit der Aufsichtsmitteilung 05/2020[530] bekannt gemacht, dass über wesentliche Cyberangriffe zu informieren ist.

Ähnlich wie das Financial Sector Cyber Collaboration Centre (FSCCC) im Vereinigten Königreich[531] hat auch die FINMA eine spezifisch auf den IT-Bereich spezialisierte Querschnittsfunktion «Operationelle, Cyber- und IT-Risiken» (B-OCI) gegründet, die für diesen Fachbereich zuständig ist.

Im Zusammenhang mit der Aufsicht durch die FINMA hat die Eidgenössische Finanzkontrolle (EFK) im Jahre 2020 bei der Prüfung der Aufsicht über die Cybersicherheit bei Finanzdienstleistern festgestellt, dass die FINMA trotz ihrer Funktion als Aufsichtsbehörde nur einen lückenhaften Überblick über die Cybersicherheit der beaufsichtigten Institute hat. Gemäss dem Bericht funktioniert insbesondere die allgemeine Meldepflicht nach Art. 29 Abs. 2 FINMAG nicht ausreichend; die FINMA selbst hat bestätigt, dass bisher nicht alle relevanten Vorfälle gemeldet wurden.[532]

2. Schweizerische Nationalbank (SNB)

Neben der FINMA kommt auch der Schweizerischen Nationalbank (SNB) grosse Bedeutung zu, denn sie führt als unabhängige Zentralbank nicht nur die Geld- und Währungspolitik der Schweiz und gewährleistet die Preisstabilität (Art. 5 NBG), sondern sie hat gemäss dem Nationalbankgesetz auch den Auftrag, zur Stabilität des Finanzsystems beizutragen. Gemäss Art. 19 ff. NBG überwacht die SNB aus diesem Grund die systemisch bedeutsamen Finanzmarktinfrastrukturen nach Art. 22 FinfraG. Mit dieser Überwachung fördert sie die Sicherheit und Effizienz der privatwirtschaftlich betriebenen Finanzmarktinfrastrukturen, und zwar mit dem Hauptaugenmerk auf die Reduktion der systemischen Risiken.[533]

---

529 Vgl. *FINMA*, Selbstregulierungen (mit einer Liste der von der FINMA anerkannten oder genehmigten Selbstregulierungen), aufrufbar unter <https://www.finma.ch/de/dokumentation/selbstregulierung/anerkannte-selbstregulierung/>; vgl. ferner insbesondere *SVV*, 2015 und *SBVg*, 2013.

530 *FINMA*, Aufsichtsmitteilung 05/2020.

531 Vgl. Kap. III.E.1.a).

532 *EFK*, 2020, 17 ff.

533 Vgl. *Schweizerische Nationalbank* (SNB), Überwachung von Finanzmarktinfrastrukturen, Überwachungsauftrag der Schweizerischen Nationalbank, aufrufbar unter <https://www.snb.ch/de/iabout/finstab/finover/id/finstab_oversight>.

Auf Verlangen der SNB sind die zentralen Gegenparteien, die Zentralverwahrer, die Zahlungssysteme und die DLT-Handelssysteme nach Artikel 73*a* FinfraG verpflichtet, der SNB alle Auskünfte und Unterlagen zur Verfügung zu stellen, welche die SNB benötigt, um die Risiken für die Stabilität des Finanzsystems frühzeitig zu erkennen und um deren systemische Bedeutsamkeit zu beurteilen (Art. 20 Abs. 1 NBG). Ebenso müssen systemisch bedeutsame Finanzmarktinfrastrukturen und ihre Prüfgesellschaften der SNB alle Auskünfte erteilen und Unterlagen herausgeben sowie unverzüglich Vorkommnisse melden, die für die Überwachung von wesentlicher Bedeutung sind (Art. 20 Abs. 2 NBG).[534]

Im Rahmen der Aufsicht und Überprüfung kann die SNB bei systemisch bedeutsamen Finanzmarktinfrastrukturen direkte Prüfungen durchführen oder durch von den Finanzmarktinfrastrukturen nach Art. 84 FinfraG beauftragte Prüfgesellschaften durchführen lassen (Art. 20 Abs. 3 NBG).

Im Bereich der Finanzstabilität arbeitet die SNB eng mit der Eidgenössischen Finanzmarktaufsicht (FINMA) zusammen; die beiden Behörden haben in einem Memorandum of Understanding die Zusammenarbeit geregelt und die Aufgaben abgegrenzt.[535]

3. Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter (EDÖB)

Der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB) beaufsichtigt die Anwendung der bundesrechtlichen Datenschutzvorschriften (Art. 4 nDSG und Art. 27 ff. aDSG). Das DSG reguliert sektorübergreifend die Angelegenheiten im Bereich des Datenschutzes. Obwohl das DSG nicht spezifisch auf die Cybersicherheit zugeschnitten ist, kommt es namentlich auch in diesen Fragen zur Anwendung, da bei einem Cybervorfall in der Regel potenzielle Datenschutzfragen relevant sind.

Wenn eine Bearbeitung ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person mit sich bringen kann, haben die Finanz-

534 Mit weiterführenden Hinweisen zu Art. 20 NBG vgl. Komm. NBG-*Häusermann*, 2021, Art. 20 Rn. 4 ff. und Rn. 10 ff.

535 Vgl. *Schweizerische Nationalbank* (SNB), Auftrag an die SNB, aufrufbar unter <https://www.snb.ch/de/iabout/finstab>; vgl. für das Memorandum of Understanding FINMA/SNB, 2017. Memorandum of Understanding im Bereich Finanzstabilität zwischen der Eidgenössischen Finanzmarktaufsicht FINMA und der Schweizerischen Nationalbank SNB, Bern 2017.

unternehmen gemäss Art. 22 Abs. 1 nDSG (keine entsprechende Regelung im aDSG) eine Datenschutz-Folgenabschätzung durchzuführen. Ergibt sich aus der Datenschutz-Folgenabschätzung, dass die geplante Bearbeitung trotz der vom Verantwortlichen vorgesehenen Massnahmen noch ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person zur Folge hat, muss das Finanzunternehmen vorgängig die Stellungnahme des EDÖB einholen (Art. 23 Abs. 1 nDSG; keine entsprechende Regelung im aDSG).

Im Zusammenhang mit der Cybersicherheit ist ausserdem zu beachten, dass die Meldepflicht gemäss DSG von der Meldepflicht gemäss FINMAG zu unterscheiden ist. Nach Art. 29 Abs. 2 FINMAG sind die die Finanzunternehmen gehalten, alle (wesentlichen) Cybervorfälle der FINMA zu melden. Das DSG hingegen hält fest, dass «nur» diejenigen Fälle, bei denen die Datensicherheit verletzt ist und die voraussichtlich zu einem hohen Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person führen, so rasch als möglich zu melden sind (Art. 24 nDSG; keine entsprechende Regelung im aDSG). Aufgrund der fortschreitenden Digitalisierung ist es aber naheliegend, dass bei einem Cybervorfall eine Verletzung der Datensicherheit vorliegt, die bei den Finanzunternehmen in der Regel auch zu einem hohen Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person führt. In diesen Konstellationen ist der Fall sowohl der FINMA als auch dem EDÖB zu melden.

B. Sanktionen bei Pflichtverletzungen

Integraler Bestandteil der Aufsicht durch die verschiedenen Behörden sind die unterschiedlichen Sanktionsmechanismen. Einerseits ist dabei an die verwaltungsrechtlichen Sanktionen zu denken, andererseits sind verschiedene Strafbestimmungen einschlägig.

1. Sanktionsbefugnisse der FINMA

Der FINMA stehen verschiedene Enforcement-Instrumente zur Verfügung, mit denen sie das Aufsichtsrecht durchsetzen kann. In Frage kommen namentlich vorsorgliche Massnahmen, Anordnungen zur Wiederherstellung des ordnungsgemässen Zustands, Feststellungsverfügungen, ein Berufsverbot, Unterlassungsanweisungen und Tätigkeitsverbote, die Veröffentlichung von

Verfügungen, die Einziehung sowie der Bewilligungsentzug, die Liquidation und der Konkurs (insb. Art. 29 ff. FINMAG). Der FINMA obliegt die Aufgabe, diese Instrumente der jeweiligen Situation angepasst anzuwenden.[536]

2. Sanktionen nach Nationalbankgesetz (NBG)

Das NBG sieht in Art. 23 Abs. 2 NBG als verwaltungsrechtliche Sanktion vor, dass die Nationalbank systemisch bedeutsame Finanzmarktinfrastrukturen im Falle etwaiger fehlender Erfüllung der besonderen Anforderungen von Art. 23 FinfraG der FINMA zur Kenntnis bringen soll. Darüber hinaus wird nach Art. 24 NBG mit einer Busse bis zu 200'000 Franken bestraft, wer vorsätzlich der Nationalbank die vorgeschriebenen Auskünfte oder Nachweise gemäss dem dritten Kapitel des NBG (Art. 14 ff. NBG, somit auch Art. 19 ff. NBG) nicht oder nicht formrichtig, unvollständig oder fehlerhaft erstattet (Art. 24 Abs. 1 lit. a NBG), sowie wer vorsätzlich eine durch die Nationalbank angeordnete oder durchgeführte Überprüfung verhindert (Art. 24 Abs. 1 lit. b NBG).

3. Sanktionen nach Datenschutzgesetz (DSG)

Auch das DSG sieht bei Verletzung des Gesetzes verschiedene Massnahmen vor. Zunächst kann der EDÖB als Verwaltungsmassnahme u.a. anordnen, dass das Finanzunternehmen die Vorkehren nach Art. 7 und 8 nDSG trifft (Art. 51 Abs. 3 lit. b nDSG; keine entsprechende Regelung im aDSG).[537] Darüber hinaus kennt das Datenschutzgesetz verschiedene Strafbestimmungen in Art. 60 ff. nDSG; im Rahmen der Cybersicherheit sind insbesondere Art. 61 lit. c nDSG und Art. 63 nDSG von Bedeutung. Gemäss Art. 61 lit. c nDSG (keine entsprechende Regelung im aDSG) ist strafbar, wer die Mindestanforderungen an die Datensicherheit, die der Bundesrat nach Art. 8 Abs. 3 nDSG (Art. 7 Abs. 2 aDSG)[538] erlassen hat, nicht einhält. Überdies wird gemäss Art. 63 nDSG (keine entsprechende Regelung im aDSG) mit Busse bestraft, wer einer Verfügung des EDÖB oder einem Entscheid der Rechtsmittelinstanzen, die oder der unter Hinweis auf die Strafdrohung dieses Artikels ergangen ist, vorsätzlich nicht Folge leistet.

---

536 *Eidgenössische Finanzmarktaufsicht FINMA*, Enforcement-Instrumente, aufrufbar unter <https://www.finma.ch/de/durchsetzung/enforcementinstrumente/>. Vgl. im Detail zu den Enforcement-Instrumenten *Zulauf et al.*, 2014, 219 ff.

537 Vgl. zur Bedeutung von Art. 7 und 8 nDSG Kap. IV.B.7.b).

538 Vgl. zu den Mindestanforderungen Kap. IV.B.7.b).

4. Weitere Sanktionen

Für die Banken enthält zudem das Bankkundengeheimnis nach Art. 47 BankG eine wichtige Strafbestimmung.[539] Demgemäss wird mit Freiheitsstrafe oder Geldstrafe sanktioniert, wer vorsätzlich ein Geheimnis offenbart, das ihm in seiner Eigenschaft als Organ, Angestellter, Beauftragter oder Liquidator einer Bank oder einer Person nach Art. 1*b* BankG oder als Organ oder Angestellter einer Prüfgesellschaft anvertraut worden ist oder das er in dieser Eigenschaft wahrgenommen hat (Art. 47 Abs. 1 lit. a BankG). Zudem wird bestraft, wer zu einer solchen Verletzung des Berufsgeheimnisses zu verleiten versucht (Art. 47 Abs. 1 lit. b BankG) oder ein ihm nach Art. 47 Abs. 1 lit. a BankG offenbartes Geheimnis weiteren Personen offenbart oder für sich oder einen anderen ausnützt (Art. 47 Abs. 1 lit. c BankG).

Ferner können die Finanzunternehmen nicht nur Verstösse begehen und sanktioniert werden, sondern – aus anderer Perspektive betrachtet – selbst Opfer von Cyberkriminalität sein. In diesen Fällen sind potenziell die sogenannten «Computerstraftatbestände»[540] (Art. 143, 143bis, 144bis, 147 StGB) anwendbar.[541]

C. Zivilrechtliche Haftungskonstellationen

In Bezug auf die Cybersicherheit und die Cyber-Resilienz stellen sich schliesslich verschiedene zivilrechtliche Haftungsaspekte. Die entsprechenden Fragen betreffen insbesondere die Sorgfaltspflichten des Finanzunternehmens im Rahmen des Risikomanagements und des Business-Continuity-Managements, aber auch das Verhältnis zwischen Finanzunternehmen und Drittanbieter; nachfolgend werden die wichtigsten Haftungskonstellationen kurz erläutert.

---

539 Vgl. im Detail zu den strafrechtlichen Folgen im Rahmen von Art. 47 BankG *Schulthess Komm. BankG-Kleiner/Schwob/Winzeler*, Art. 47 Rn. 383 ff.

540 *Aebi*, 2020, 95 mit Fn. 507; zur Benutzung der Terminologie des «Computerstrafrechts» vgl. bereits *Schwarzenegger*, 492.

541 Vgl. zu den Tatbeständen im Detail BSK StGB II-*Weissenberger*, 2019, Art. 143 Rn. 1 ff.; BSK StGB II-*Weissenberger*, 2019, Art. 143bis Rn. 1 ff.; BSK StGB II-*Weissenberger*, 2019, Art. 144bis Rn. 1 ff.; BSK StGB II-*Fiolka*, 2019, Art. 147 Rn. 1 ff.

1. Haftungsvoraussetzungen

Um eine Haftung zu begründen, ist eine Pflichtverletzung oder ein widerrechtliches Handeln vorausgesetzt – im Kontext der Cybersicherheit und der Cyber-Resilienz ist dies insbesondere in Form von fehlender bzw. fehlerhafter Erfüllung der Handlungsempfehlungen (u.a. Massnahmen im Rahmen des Risikomanagements, des Business-Continuity-Managements und der Aufsicht über Drittanbieter) vorstellbar.[542]

Die Haftung verlangt zudem den Eintritt eines Schadens sowie das Vorliegen des adäquaten Kausalzusammenhangs zwischen der Widerrechtlichkeit und dem Schadenseintritt. Schliesslich bedarf es eines Verschuldens, das im Vertrag vermutet wird und ausservertraglich nachzuweisen ist.[543]

2. Ausgewählte Haftungskonstellationen

a) Verhältnis Finanzunternehmen – Kunde

Im Kontext der Cybersicherheit und der Cyber-Resilienz ist insbesondere die Haftung aus Auftrag (Art. 394 ff. OR) von Bedeutung, weil die Regeln des Auftragsrechts bzw. auftragsähnliche Elemente mit Bezug auf verschiedene Dienstleistungen der Finanzunternehmen zur Anwendung kommen. In diesen Konstellationen ist das Finanzunternehmen verpflichtet, die Vertragsziele zweckgerecht, zweckmässig und erfolgsbezogen zu verfolgen und das Risikomanagement dementsprechend umzusetzen; der jeweilige Vertrag mit dem Kunden dient dabei als objektiviert zu verstehender Sorgfaltsmassstab.

Das Finanzunternehmen haftet als Beauftragter im Allgemeinen für die gleiche Sorgfalt wie der Arbeitnehmer im Arbeitsverhältnis (Art. 398 Abs. 1 OR). Im Auftragsverhältnis ist eine Sorgfalt geschuldet, die ein gewissenhafter Beauftragter in gleicher Lage an den Tag gelegt hätte. Hält der Beauftragte die erforderliche Sorgfalt nicht ein, liegt eine Vertragsverletzung vor und der Kunde kann Ansprüche aus Auftrag geltend machen.[544]

Im Rahmen der Cybersicherheit und der Cyber-Resilienz ist insbesondere eine Missachtung der Verhaltensanweisungen im Bereich der Qualitätsmanage-

542 Zu den Handlungsempfehlungen vgl. Kap. IV.

543 *Gauch/Schluep/Emmenegger*, 2020, Rn. 2486a ff. m.w.H.

544 BGE 115 II 62 E. 3.a); BSK OR I-*Oser/Weber*, 2020, Art. 398 Rn. 24.

ment-Systeme[545] von Bedeutung, denn sowohl das Fehlen als auch die Lückenhaftigkeit der Qualitätsmanagement-Systeme können eine Sorgfaltspflichtverletzung begründen.[546] Das Risikomanagement ist ein wesentliches Element eines wirksamen Qualitätsmanagements und Teil des ISO-9001:2015-Standards.[547] Neben dieser engen Verknüpfung enthält die ISO-9000-Reihe ausserdem verschiedene Verweise auf das Risikomanagement; die ISO-9001-Norm beispielsweise setzt sich mit der Anwendung eines risikobasierten Ansatzes auseinander und verlangt, die Risiken bei der Planung des Qualitätsmanagements zu berücksichtigen.

Gestützt auf diese Erkenntnisse ist die offensichtliche Missachtung anwendbarer Handlungsempfehlungen (u.a. des Risikomanagements)[548] geeignet, eine Sorgfaltspflichtverletzung im Sinne von Art. 398 OR herbeizuführen. In solchen Fällen ist insbesondere zu beachten, dass eine adäquate Cybersicherheit und Cyber-Resilienz aufgrund der steigenden Relevanz der Cyberrisiken bzw. Cybervorfälle für jedes Unternehmen unerlässlich geworden ist.[549]

Eine weitere Quelle für eine mögliche Sorgfaltspflichtverletzung stellt der Beizug eines Drittanbieters dar.[550] Wie bereits im Kontext der Handlungsempfehlungen erwähnt, sind die Finanzunternehmen verpflichtet, die Auswahl und Überwachung der Drittanbieter vertraglich zu regeln.[551] Lagert ein Finanzunternehmen einzelne Prozesse an Drittanbieter aus, ist zu ermitteln, ob eine

---

545 Die ISO-9001-Norm macht systematische Vorgaben für die Erarbeitung eines Qualitätsmanagement-Systems und empfiehlt den Anwendern, ihre Systeme auf der Basis von bestimmten Modellen aufzubauen (vgl. auch *Fellmann*, 2016, 97).

546 *Fellmann*, 2016, 97 f.; *Fellmann*, 2008, 125 f.; *Moser*, 1997, 190.

547 *Anttila/Jussila*, 2017, 1094 f.

548 Vgl. Kap. IV.

549 Vgl. auch Kap. I.

550 Beim Beizug eines Drittanbieters ist zu unterscheiden, ob dieser als Hilfsperson (Erfüllungsgehilfe) oder als Substitut (Substitution) agiert. Der Beauftragte kann auch bei gesteigertem Vertrauensverhältnis eine Hilfsperson für die Erfüllung bestimmter Aufgaben beiziehen (BGE 85 II 46, 48). Bei einer Substitution hängen die Rechtsfolgen davon ab, ob sie befugt oder unbefugt war. Entscheidend ist, ob der Beauftragte den Dritten in seine «Erfüllungsorganisation» integriert (BGE 112 II 354 E. 2b)) oder ob er im Interesse des Auftraggebers einen Fachmann für die optimale Geschäftsführung beizieht (vgl. *Weber*, 1990, 80). Für die Substitution sprechen die Übertragung der Vertragserfüllung an den Dritten, seine besonderen Sachkenntnisse oder auch das Interesse des Auftraggebers am Beizug des Substituten (BSK OR I-*Oser/Weber*, 2020, Art. 398 Rn. 3 m.w.H.; vgl. zur Hilfspersonenhaftung auch BK OR-*Weber/Emmenegger*, 2020, Art. 101 Rn. 1 ff., insb. Rn. 5 m.w.H.).

551 Vgl. Kap. IV.D.

befugte Substitution (Art. 399 Abs. 2 OR)[552] oder eine unbefugte Substitution (Art. 399 Abs. 1 OR)[553] vorliegt. Im ersten Fall muss das Finanzunternehmen nur für Auswahl und Instruktion des Drittanbieters einstehen;[554] im zweiten Fall haftet das Finanzunternehmen für die Handlungen «wie wenn es seine eigenen wären», aber ohne Möglichkeit zur Exkulpation, da der Beizug an sich bereits eine Vertragsverletzung darstellt.[555]

Darüber hinaus ist mit Blick auf die sich schnell entwickelnden Technologien zu berücksichtigen, dass die Haftung entfällt, wenn der Schaden aufgrund von Ursachen, die nach dem gegenwärtigen Stand der Wissenschaft auch bei aufmerksamer und gewissenhafter Prüfung nicht erkennbar sind, eingetreten ist.[556]

Da die Finanzunternehmen den Vorgaben des Datenschutzgesetzes (DSG) nachkommen und Personendaten schützen müssen, sind auch die Haftungskonstellationen im DSG von Bedeutung. Die datenschutzrechtliche Haftung lebt auf, falls es an den angemessenen Datensicherheitsvorkehren fehlt und deshalb unberechtigte Dritte Zugang zu Personendaten haben. Von Bedeutung ist dabei insbesondere eine Verletzung von Art. 7 nDSG (Privacy by Design; Art. 7 aDSG), die als gesetzliche Vorgabe an die Sorgfaltspflicht der Kausalhaftung nahekommt. Diese Haftung lebt u.a. auf, wenn die erforderlichen Massnahmen zur Vermeidung von Persönlichkeitsverletzungen nicht getroffen worden sind.[557]

Ferner ist bei Persönlichkeitsverletzungen ein Anspruch gegen jeden möglich, der an einer Verletzung mitgewirkt hat. Bei den Verantwortlichen (Art. 5 lit. j nDSG; keine entsprechende Regelung im aDSG) fällt namentlich die Geschäftsherrenhaftung von Art. 55 OR und bei Vorliegen einer Vertragsbeziehung zwischen dem Verantwortlichen und der betroffenen Person allenfalls eine Hilfspersonenhaftung (Art. 101 OR) in Betracht.[558]

Im Übrigen vermag unter Umständen auch die gesellschaftsrechtliche Haftung nach Art. 754 OR (Haftung für Verwaltung bzw. Geschäftsführung) zur An-

552 Im Detail zur befugten Substitution *BSK OR I-Oser/Weber*, 2020, Art. 399 Rn. 2 ff.

553 Im Detail zur unbefugten Substitution *BSK OR I-Oser/Weber*, 2020, Art. 399 Rn. 5.

554 *BSK OR I-Oser/Weber*, 2020, Art. 399 Rn. 2.

555 *BSK OR I-Oser/Weber*, 2020, Art. 399 Rn. 5 m.w.H.

556 *BSK OR I-Oser/Weber*, 2020, Art. 398 Rn. 27; vgl. ferner im Zusammenhang mit Tierärzten BGE 93 II 19.

557 *Rosenthal*, 2020b, Rn. 43 ff. m.w.H.

558 Vgl. hierzu *Rosenthal*, 2020b, Rn. 61.

wendung zu gelangen, weil der Verwaltungsrat für die sorgfältige und adäquate Umsetzung des Risikomanagements und des Business-Continuity-Managements zuständig ist.[559] Die haftungsbegründenden Pflichten sind u.a. in Art. 716 Abs. 2 OR (Geschäftsführungspflicht) sowie in Art. 716a OR zu finden.[560] Im Rahmen der gesellschaftsrechtlichen Haftung ist zwischen den Ansprüchen im Konkurs und ausserhalb einer Konkurssituation (Art. 756 f. OR) zu differenzieren; je nachdem handelt es sich um die Geltendmachung von Ansprüchen aus unmittelbarem oder mittelbarem Schaden.[561]

Im Rahmen der vorliegenden Haftungskonstellationen spielt hingegen das Produkthaftpflichtgesetz (PrHG) keine Rolle, weil dessen Anwendungsbereich die Finanzprodukte[562] nicht umfasst, sondern dieser sich auf bewegliche Sachen und Elektrizität beschränkt (Art. 3 PrHG).[563]

b) Verhältnis Finanzunternehmen – Drittanbieter

Das Finanzunternehmen selbst hat gegebenenfalls vertragsrechtliche Ansprüche gegenüber dem Drittanbieter; auf diese Konstellation gelangen – je nach Produkt bzw. Dienstleistung – grundsätzlich die Regelungen des Werkvertrags oder des Auftrags zur Anwendung.

Die Bestimmungen des Werkvertrags sind anwendbar, wenn der Drittanbieter beispielsweise eine individuelle Software im Sinne eines unkörperlichen Werkes liefert.[564] Befinden sich Finanzunternehmen und Drittanbieter in einem Werkvertragsverhältnis, haftet der Drittanbieter im Allgemeinen für die gleiche Sorgfalt wie der Arbeitnehmer im Arbeitsverhältnis (Art. 364 Abs. 1 OR).[565] In dieser Konstellation ist es wichtig, dass das Finanzunternehmen nach Ablie-

559 Die Implementierung eines funktionierenden Risikomanagements ist Teil der Oberleitung (vgl. BSK OR II-*Watter/Roth Pellanda*, 2016, Art. 716a Rn. 6; vgl. ferner *Weber*, 2006, 132 m.w.H.) und die Handlungsempfehlungen im Rahmen der Cybersicherheit sind integraler Bestandteil des Risikomanagements (vgl. Kap. IV.B.).

560 BSK OR II-*Gericke/Waller*, 2016, Art. 754 Rn. 26.

561 BSK OR II-*Gericke/Waller*, 2016, Art. 756 Rn. 1.

562 Für den Begriff der Finanzprodukte, vgl. *Eggen*, 2015, 8 ff.

563 *Weber*, 2021h, 684 f.; *Sethe*, 2020, Rn. 8.19; vgl. ferner für eine ähnliche Schlussfolgerung im Rahmen der Produktehaftung in der Europäischen Union, *Weber*, 2017b, 210.

564 BSK OR I-*Zindel/Schott*, 2020, Vor Art. 363–379 Rn. 2; vgl. auch Kap. IV.D.2.a) und IV.D.2.b) zur Thematik der Verwendung hochstandardisierter bzw. individueller Prozesse im Rahmen der Auslagerung an Dritte.

565 Vgl. im Detail zur Haftung für Mängel am Werk BSK OR I-*Zindel/Schott*, 2020, Art. 367 Rn. 1 ff.

ferung des Werkes dessen Beschaffenheit prüft und den Drittanbieter von allfälligen Mängeln in Kenntnis setzt (Art. 367 Abs. 1 OR); als Massstab für die Prüfung ist auf die Sorgfalt und Aufmerksamkeit eines durchschnittlichen (nicht spezialisierten) Abnehmers von Werken der betreffenden Art abzustellen.[566]

Das Verhältnis zwischen Finanzunternehmen und Drittanbieter begründet aber gegebenenfalls auch einen Auftrag bzw. ein auftragsähnliches Rechtsverhältnis; in diesem Fall kommen die Normen von Art. 394 ff. OR zur Anwendung.[567] Der Drittanbieter wahrt im Auftragsverhältnis die Interessen des auftraggebenden Finanzunternehmens und schuldet – unter Wahrung der angemessenen Sorgfalt – gewisse Dienstleistungen, jedoch keinen Erfolgseintritt.[568] Diese Konstellation ist insbesondere bei der Auslagerung von cybersicherheitsbezogenen Übungen und Tests möglich.[569] Auch in dieser Situation haftet der Beauftragte im Allgemeinen für die gleiche Sorgfalt wie der Arbeitnehmer im Arbeitsverhältnis (Art. 398 Abs. 1 OR).[570]

c) Weitere Verhältnisse

Aufgrund der engen Vernetzung der Akteure auf dem Finanzmarkt sind auch ausservertragliche (deliktische) Ansprüche möglich. Denkbar ist folgende Situation: Ein Kunde befindet sich in einem Vertragsverhältnis mit der Bank A, die eine beauftragte Transaktion (z.B. Erwerb ausländischer Aktien) über die spezialisierte Bank B ausführen lässt. Da die Bank B die erforderlichen Massnahmen im Rahmen des Risikomanagements nicht umgesetzt hat und keine adäquate Cybersicherheit und Cyber-Resilienz sicherstellt, wird die Transaktion von unbekannten Dritten zulasten des Kunden abgefangen. Da sich der Kunde nur mit der Bank A in einem Vertragsverhältnis befindet, die sich sorgfältig verhalten hat, der Schaden jedoch aufgrund des Verhaltens der Bank B entsteht, kann eine ausservertragliche Haftung der Bank B relevant sein.

Die anwendbare Deliktshaftung basiert auf dem allgemeinen Grundtatbestand der unerlaubten Handlung, d.h. eines deliktischen Verhaltens (Art. 41 OR).[571] Für den Kunden wirkt sich aber nachteilig aus, dass der reine Vermögensscha-

566 BSK OR I-*Zindel/Schott*, 2020, Art. 367 Rn. 9; *Gauch*, 2019, Rn. 2122.

567 Vgl. BSK OR I-*Oser/Weber*, 2020, Art. 394 Rn. 1 ff.

568 BSK OR II-*Oser/Weber*, 2020, Art. 394 Rn. 2.

569 Ferner auch im Rahmen von Art. 9 nDSG vorstellbar; vgl. auch *Wittmann/Haidenthaler*, 2022, 8 m.w.H.

570 Vgl. im Detail für die auftragsrechtlichen Ausführungen Kap. V.C.2.a).

571 BSK OR I-*Kessler*, 2020, Art. 41 Rn. 3 ff.

den nur dann widerrechtlich ist, wenn eine besondere Verhaltensnorm «nach ihrem Zweck (auch) vor Schädigungen von der Art der (konkret) eingetretenen schützen soll».[572] Es ist in jedem Einzelfall zu untersuchen, ob eine solche Verhaltensschutznorm tatsächlich vorliegt. Zudem muss der Geschädigte ein Verschulden des Schädigers nachweisen.

572 BSK OR I-*Kessler*, 2020, Art. 41 Rn. 34; BGE 132 III 122 E. 4.1; BGE 124 III 297 E. 5b); BGE 119 II 127 E. 3.

VI. Zusammenfassung und Ausblick

Cyberrisiken sind ein zunehmend relevantes Thema; aus diesem Grund ist eine adäquate Cybersicherheit und Cyber-Resilienz unerlässlich für jedes Unternehmen. Diese Aussage trifft insbesondere auf den Finanzmarkt zu, der sich immer mehr zu einem zusammenhängenden und verflochtenen System, das verschiedenste Transaktionen erfasst, entwickelt. Mit der steigenden Abhängigkeit von den Informations- und Kommunikationstechnologien erhöht sich auch die Verwundbarkeit auf dem Finanzmarkt.

Die Relevanz der Cybersicherheit und der Cyber-Resilienz ist auch mit Blick auf den Finanzplatz Schweiz nicht zu unterschätzen. Zurzeit sind in der Schweiz nur Grundzüge zum Umgang mit Cyberrisiken durch die FINMA geregelt; es besteht Handlungsbedarf einerseits mit Bezug auf die Konkretisierung dieser Grundzüge, andererseits aber auch hinsichtlich einer funktionierenden Kontrolle bei der Umsetzung und beim Vollzug der bestehenden Verpflichtungen.[573] Ausserdem weist das heute geltende Datenschutzgesetz im internationalen Vergleich einige Schwächen auf (beispielsweise besteht keine Pflicht zur Meldung von Verletzungen der Datensicherheit); dieser Mangel ändert sich mit dem Inkrafttreten des nDSG (Pflicht zur Meldung von Verletzungen der Datensicherheit in Art. 24 nDSG).

Offensichtlich sind in der Schweiz einige Bereiche der Cybersicherheit und der Cyber-Resilienz noch ungenügend geregelt. Zunächst fällt auf, dass die Schweiz im internationalen Vergleich über keine ausdrücklichen Regelungen zu den Governance- und Kontrollmechanismen sowie zum Situationsbewusstsein der Finanzunternehmen verfügt.[574] Die vorliegend diskutierten Handlungsempfehlungen füllen diese Lücke in Anlehnung an die Leitlinien und Empfehlungen in der Europäischen Union sowie an die Empfehlungen der BIS/IOSCO und der Europäischen Zentralbank.[575]

Ausserdem ist der grundlegende Umgang mit Cyberrisiken im Finanzbereich im Wesentlichen einzig im FINMA Rundschreiben 2008/21 geregelt.[576] Zwar

---

573 Vgl. hierfür insbesondere die Prüfung der Eidgenössischen Finanzkontrolle zur Aufsicht über die Cybersicherheit bei Finanzdienstleistern (EFK, 2020, 18 f.).

574 Vgl. insbesondere EIOPA, 2021, 9; ferner Art. 4 DORA.

575 Vgl. Kap. IV.B.2 und IV.B.6.

576 FINMA, Rundschreiben 2008/21, Rn. 135.6 ff.

verlangt die FINMA geeignete Prozesse, um institutsspezifische Bedrohungspotenziale durch Cyberattacken zu identifizieren, ohne aber Details anzuordnen; die Handlungsempfehlungen konkretisieren diese Verpflichtung mit Anlehnung an die Regulierung in der Europäischen Union.

Ferner schreibt die FINMA einen angemessenen Schutz der Geschäftsprozesse vor Cyberattacken vor; in den Untersuchungen hat sich indessen herausgestellt, dass das Konzept der Resilience by Design – ähnlich wie Privacy by Design – als angebrachte Konkretisierung dieser Vorgabe erst ansatzweise realisiert ist.[577] Überdies verlangt ein geeigneter Schutz auch regelmässige Tests und Übungen, um die Wirksamkeit des Schutzes zu überprüfen; da weder die FINMA noch der Schweizer Gesetzgeber besondere Vorgaben zu den Tests und Übungen machen, lehnen sich die Handlungsempfehlungen an die internationalen Standards an; dabei sind die Verwundbarkeitsanalysen und Penetrationstests im Vereinigten Königreich, in Singapur und in Hong Kong als ausgereifte Modelle durchaus nachahmenswert.[578]

Die FINMA auferlegt im FINMA Rundschreiben 2008/21 der Geschäftsleitung von Banken, Finanzgruppen und Effektenhändlern ausserdem die Umsetzung geeigneter Prozesse für eine zeitnahe Erkennung potenzieller Cyberattacken. Diese Vorgabe lässt sich insbesondere durch die Empfehlungen der BIS/IOSCO und des NIST Rahmenwerks umsetzen, indem Systeme zur Erkennung von Eindringlingen und eine kontinuierliche Überwachung in Echtzeit oder nahezu in Echtzeit angewendet werden.[579] Eine weitere effiziente Methode, um Cyberattacken frühzeitig zu erkennen, ist die Einführung einer Plattform für den Informationsaustausch unter Finanzunternehmen, wie sie bereits in Japan existiert.[580]

In der Schweiz steht ein Ausbau der Meldepflichten zur Diskussion; zudem hat die FINMA nach der Publikation der Prüfungsresultate seitens der Eidgenössischen Finanzkontrolle (EFK) die FINMA-Aufsichtsmitteilung 05/2020 erlassen,

577 So auch BIS/IOSCO, 2016, 12.

578 Vgl. Kap. III.E.1.d)aa), III.E.3.c) und III.E.4.b).

579 Vgl. BIS/IOSCO, 2016, 20; NIST, 2018, 37 ff.

580 Vgl. Kap. III.E.6.b); dieselbe Empfehlung auch in BIS/IOSCO, 2016, 21.

um die Meldepflichten und einen potenziellen Informationsaustausch zu stärken.[581] Die Aufsichtsmitteilung hat Ähnlichkeiten mit Art. 17 DORA;[582] ob sie ihren Zweck tatsächlich erfüllt, bleibt abzuwarten.

Im Zusammenhang mit dem Business-Continuity-Management ist bis heute keine ausdrückliche Erwähnung der Cyberrisiken erkennbar; die Spezifikationen für die Cybersicherheit und die Cyber-Resilienz sind jedoch auf Grundlage vorhandener Vorgaben möglich. Hierfür erweisen sich die im Rahmen der Selbstregulierung erlassenen Empfehlungen zum Business-Continuity-Management der Schweizerischen Bankiervereinigung (SBVg) und des Schweizerischen Versicherungsverbands (SVV) als relevant; ferner ist auch der Cloud-Leitfaden der Schweizerischen Bankiervereinigung (SBVg) von Bedeutung. Die ausgeführten Handlungsempfehlungen ergänzen diese Leitlinien mit Vorgaben im DORA sowie mit Vorschlägen der BIS/IOSCO und mit in Singapur angeordneten Massnahmen.[583]

Der Cybersicherheit und der Cyber-Resilienz kommt auf DLT-Handelssystemen und anderen Bereichen im Rahmen der Distributed Ledger Technology besondere Bedeutung zu; die entsprechenden Herausforderungen und die potenziellen Gefahren sind deshalb gesondert zu beleuchten.[584]

581 Vgl. Kap. III.B.2.b) und IV.C.4.

582 Auch die Kriterien für die Feststellung der Wesentlichkeit eines Cybervorfalls ist vergleichbar mit den Abgrenzungskriterien der Financial Conduct Authority (FCA) im Vereinigten Königreich (vgl. Kap. III.E.1.b)aa)).

583 Vgl. IV.C; ferner BIS/IOSCO, 2016, 16, SVV, 2015, 8 ff.; SBVg, 2013, 9 ff. und III.E.3.c).

584 Vgl. dazu *Rolf H. Weber*, Sicherheit und Resilienz in DLT-basierten Finanzinfrastrukturen, erscheint im Frühling 2022 in Weblaw (online).

Veröffentlichungen des Center für Information Technology, Society and Law (ITSL) der Universität Zürich

erschienen bei Schulthess Juristische Medien AG, Zürich

Vol. 1: **Werbung – Online**
FLORENT THOUVENIN/ROLF H. WEBER (Hrsg.)
Zürich 2017

Vol. 2: **Transatlantic Data Protection in Practice**
ROLF H. WEBER/DOMINIC N. STAIGER
Zürich 2017

Vol. 3: **Endorsements and Behavioral Advertising in Social Media under EU, Swiss, and US Law**
MANE SARGSYAN
Zürich 2017

Vol. 4: **Nutzung von Cloud-Diensten durch Anwältinnen und Anwälte/ Utilisation des services de cloud par les avocates et avocats**
CHRISTIAN SCHWARZENEGGER/FLORENT THOUVENIN/BURKHARD STILLER
Zürich 2019

Vol. 5: **Die Informationspflichten des Unternehmers im E-Commerce**
DOMINIC OERTLY
Zürich 2019

Vol. 6: **Der IT-Outsourcingvertrag im schweizerischen Recht**
ALEXANDER SCHMID
Zürich 2019

Vol. 7: **Elemente einer Datenpolitik**
FLORENT THOUVENIN/ROLF H. WEBER/ALFRED FRÜH
Zürich 2019

Vol. 8: **Prinzipien und Rechtmässigkeitsbedingungen im privaten Datenschutzrecht**
DAMIAN GEORGE
Zürich 2021

Angesichts der zunehmenden Zahl von Cybervorfällen steigt für die in den Finanzmärkten tätigen Unternehmen der Bedarf, Vorkehren zum Schutz der Cybersicherheit und der Cyber-Resilienz zu treffen. Die regulatorischen Vorgaben in der Schweiz sind nicht sehr spezifisch, weshalb von Branchenorganisationen entwickelte Standards und Compliance-Massnahmen (z.B. mit Blick auf das Risikomanagement und auf die Kontinuität der Geschäftsprozesse) an Bedeutung gewinnen. Das Buch erläutert rechtsvergleichend das regulatorische Umfeld der Cybersicherheit und entwickelt Handlungsempfehlungen für Unternehmen in den Finanzmärkten.