Cybersecurity

Kipker

2. Auflage 2023
ISBN 978-3-406-79263-2
C.H.BECK

Cybersecurity

Herausgegeben von

Prof. Dr. Dennis-Kenji Kipker

Professor für IT-Sicherheitsrecht an der HSB
Legal Advisor für den VDE Verband der Elektrotechnik Elektronik Informationstechnik e.V. in Offenbach am Main

Bearbeitet von dem Herausgeber und von

Dr. Malek Barudi, M.Jur. (Oxford), Hamburg; Klaus Beucher, LL.M. (Wisconsin), Düsseldorf; Richard Bird, Hong Kong; Rolf Blunk, Bremen; Prof. Dr. Dominik Brodowski, LL.M. (UPenn), Saarbrücken; Arnd Böken, Berlin; Dr. Axel Freiherr von dem Bussche, LL.M., Hamburg; Mathew Chacko, Bangalore; Sunghee Chae, Seoul; Olga Chislova, London; Georgia Dawson, Hong Kong; Prof. Dr. Wolfgang Däubler, Bremen; Dr. Carsten Dochow, Berlin; Dr. Theresa Ehlen, Düsseldorf; Eike Ekrot, Berlin; Matthias Fischer, Berlin; Dr. Justus Gaden, Berlin; Dr. Markus Gollrad, Berlin; Franz-Josef Herpers, Berlin; Samuel Johnson, Singapore; Dr. Peter Lutz Kalmbach, Bremen; Prof. Dr. Tobias Keber, Stuttgart; Prof. Dr. Thomas Kemmerich, Bremen; Dr. David Klein, LL.M. (Univ. of Wash.), Hamburg; Dr. Thomas Lapp, Frankfurt a. M.; Markus Lutz, Berlin; Dr. Sönke Maseberg, Bremen; Andreas H. Michael, Bielefeld; Aadya Misra, Bangalore; Dipl. Ing. Sven Müller, Frankfurt a. M.; Kwang Bae Park, Seoul; Christopher Philipp, Berlin; Prof. Dr. Christoph Rademacher, Tokyo; Prof. Dr. Georgios Raptis, Regensburg; Thomas Rehbohm, Bremen; Dirk Reimers, Wentorf AS; Prof. Dr. Jörn Reinhardt, Fulda; Steve Ritter, Königswinter; Prof. Dr. Michael Schmidl, München; Dr. Jost-Benjamin Schrooten, Berlin; Enrico Seidel, München; Dr. Karsten Sohr, Bremen; Marina Sokolova, Brüssel; Florian Tannen, München; Prof. Dr. Mayu Terada, Tokyo; Julia Utzerath, LL.M. (Exeter), Düsseldorf; Dr. Friederike Voskamp, LL.M. (Berkeley), Hamburg; Prof. Dr. Gunter Warg, Brühl; Dr. Nicolai Wiegand, LL.M. (NYU), München

2. Auflage 2023

C.H.BECK

Zitiervorschlag:
Kipker Cybersecurity-HdB/Schrooten Kap. 2 Rn. 1

www.beck.de

ISBN 978 3 406 79263 2

Wilhelmstraße 9, 80801 München
Druck und Bindung: Beltz Grafische Betriebe GmbH,
Am Fliegerhorst 8, 99947 Bad Langensalza

Satz: 3w+p GmbH, Rimpar
Umschlaggestaltung: Druckerei C.H. Beck Nördlingen

CO_2 neutral
chbeck.de/nachhaltig

Gedruck auf säurefreiem, alterungsbeständigem Papier
(hergestellt aus chlorfrei gebleichtem Zellstoff)

Vorwort zur 2. Auflage

Die Corona-Pandemie hat verdeutlicht, wie vulnerabel moderne Industriegesellschaften sind – und das in vielerlei Hinsicht. Auch mit Blick auf die Cybersecurity hat die weltweite Ausnahmesituation in den letzten zwei Jahren erhebliche Herausforderungen mit sich gebracht: So beim Home Office und Home Schooling, bei der Absicherung kritischer Infrastrukturen im Pharma- und Gesundheitsbereich, für Corona Tracing- und Tracking-Apps oder mit Blick auf die Nutzung von cloudbasierten Kollaborationstools und Videokonferenzsystemen. Darüber hinaus hat die Corona-Pandemie für eine Verlagerung der Kriminalität insbesondere in den virtuellen Raum hinein gesorgt. Dabei spielt nicht nur der unberechtigte Zugriff auf IT-Systeme und die Manipulation von Daten eine Rolle, sondern auch der Einsatz nicht technischer Angriffsmittel, um Personen und Prozesse zu beeinflussen. Ebenso hat sich gezeigt, dass das Maß an Cyberkriminalität in den vergangenen Jahren deutlich zugenommen hat und nicht nur kleine und mittelständische Betriebe, sondern in der jüngeren Vergangenheit vor allem Großkonzerne und Behörden erfolgreich angegriffen wurden – das mit teils verheerenden versorgungsrelevanten und wirtschaftlichen Folgen. Insbesondere sind im öffentlichen Sektor zunehmend die kommunalen Verwaltungen von erfolgreichen Cyberangriffen betroffen. Das durch die Pandemie erzwungene Mehr an Digitalisierung hat somit zwangsläufig zu einer Intensivierung der Bedrohungslage für die Cybersecurity geführt.

Der zunehmende Verlust von Sicherheit ist aber nicht allein auf den digitalen Raum begrenzt. So hat sich die weltweite Notlage ebenso als Nährboden für Desinformation („Fake News“) erwiesen – ein Thema, das nicht unmittelbar der Cybersecurity zuzuordnen ist, aber dennoch untrennbar hiermit zusammenhängt, wenn beispielsweise erfolgreiche Social Engineering-Angriffe geplant und durchgeführt werden. Ebenfalls während der Pandemielage verstärkt in die Schlagzeilen geraten ist die digitale Souveränität, die mehr und mehr als Technologiesouveränität verstanden werden kann. Ging es vor einigen Jahren noch darum, im betriebswirtschaftlichen Sinne möglichst viele Prozesse auch in das Ausland auszulagern, so zeigt sich nun, dass es mittelfristig gedacht gar ein strategischer Vorteil sein kann, bestehende Prozesse innerhalb eines Unternehmens oder zumindest in der Europäischen Union zu belassen, auch wenn dies auf den ersten Blick keine unmittelbaren wirtschaftlichen Vorteile bringen mag. Der politische Konflikt zwischen der Volksrepublik China und Taiwan und die globalen Lieferengpässe als eine Folge von Corona beschleunigen dabei nur eine Entwicklung, die früher oder später ohnehin ihren Anfang gefunden hätte. Der Schutz von globalen Lieferketten ist dabei aus verschiedenen Gründen auch für die Cybersecurity relevant: So können ohne die benötigte Hardware zuvorderst keine technischen Komponenten hergestellt werden, die zentrale Steuerungsfunktionen erfüllen. Außerdem muss gewährleistet sein, dass die häufig aus dem Ausland gelieferten Bauteile keine technischen und sicherheitsrelevanten Schwachstellen aufweisen. Überdies spielt das rechtliche Regelungsregime eine Rolle, dem Hard- und Software aus Drittstaaten unterliegen. Hier zeigt sich ebenfalls deutlicher als bislang, dass Staaten die Anforderungen an Cybersecurity zusehends strenger regulieren – und das mit teils erheblicher extraterritorialer Wirkung der Gesetze. Zu all diesen Entwicklungen hinzu tritt seit Februar 2022 der Russland-Ukraine-Krieg, der die Cybersicherheitsbedrohungen nochmals auf ein völlig neues Niveau gehoben hat, indem staatliche Akteure und „Hacktivism“ gleichzeitig versuchen, parallel zum kriegerischen Geschehen auch im virtuellen Raum die Oberhand zu erlangen. Die Folgen sind auch in Deutschland spürbar: Erhebliche wirtschaftliche Schäden als kausale Folge von teils auch nur kollateralen Cyberangriffen sowie hybride Bedrohungen für Kritische Infrastruktur, die über den virtuellen Raum hinausgehen.

Feststellen lässt sich folglich, dass einerseits digitale Vernetzung und technologische Abhängigkeiten grenzübergreifend steigen, Nationalstaaten andererseits (oder gerade deshalb)

zunehmend politisch und regulatorisch auf diesen Trend reagieren, um Abhängigkeiten zu reduzieren. Deutlich zutage tritt dabei, dass Cybersecurity-Gesetzgebung immer stärker durch ein Misstrauen gegenüber ausländischen Staaten sowie privaten Akteuren geprägt ist. Diese unterschiedlichen Interessenlagen und neuen Herausforderungen haben zur Folge, dass Cybersecurity seit dem Erscheinen der ersten Auflage dieses Werkes im Jahr 2020 nicht nur nochmals deutlich an Relevanz gewonnen hat, sondern vielschichtiger denn je ist. Die Aufgabe eines Rechtshandbuches, das sich als umfassendes Kompendium und erste Anlaufstelle für die juristische Betrachtung von Cybersicherheit versteht, ist es, diesen neuen und in den letzten Jahren erheblich geänderten Anforderungen gerecht zu werden, was sich auch im erheblich gesteigerten Umfang und Themenzuschnitt dieser zweiten Auflage widerspiegelt.

So war es nicht nur das Ziel, die Ausführungen innerhalb der Bestandskapitel zu aktualisieren und inhaltlich zu vertiefen, sondern zusätzliche Inhalte zu gewinnen, die dem Facettenreichtum des Themas angemessen Rechnung tragen. In der Werksystematik neu hinzugekommen ist daher zuvorderst ein umfassender Abschnitt zu den verfassungsrechtlichen Grundlagen von Cybersecurity (Kapitel 2). Das Kapitel 4 zum „Stand der Technik" ist erhalten geblieben, wurde aber um ein neues Kapitel zu Normen und Standards und zur Zertifizierung (Kapitel 5) ergänzt. Auch wurden die Ausführungen zu den Kritischen Infrastrukturen (Kapitel 14) komplett aktualisiert und auf den Stand des IT-Sicherheitsgesetzes 2.0 gebracht. Ein neuer Abschnitt zur Verwaltung (Kapitel 15) stellt die vielschichtige Behörden- und Zuständigkeitsstruktur in der Cybersecurity in der EU sowie in Bund, Ländern und Kommunen vor. Der Datenverarbeitung im Gesundheits- und Sozialsektor widmet sich das ebenfalls neue Kapitel 16 – dargestellt werden in diesem Kapitel außerdem die IT-Sicherheitsanforderungen an Arztpraxen und Gesundheitseinrichtungen unterhalb der Schwellenwerte für Kritische Infrastrukturen. Ausführungen zu neuen Technologien und dem Verbraucherschutz finden sich im Kapitel 20, so beispielsweise im Hinblick auf sichere digitale Identitäten, Updatability von IoT, Verbraucherkennzeichnungen und Desinformation. Schon bisher enthielt das Rechtshandbuch überdies ein Kapitel zum internationalen regulatorischen Rahmen der Cybersicherheit (Kapitel 21), das in dieser zweiten Auflage erweitert wurde und folgende aktuelle Länderberichte zum Thema beinhaltet: Europäische Union, Israel, Volksrepublik China, Japan, Russische Föderation, Südkorea, die Vereinigten Staaten und Indien. Den Abschluss des Buches bildet das ebenfalls neue Kapitel 23, das technisch-organisatorische Best Practices für ausgewählte Anwendungsszenarien der Cybersicherheit vorstellt.

Als Herausgeber des Rechtshandbuchs Cybersecurity wünsche ich mir, mit diesen Neuerungen bei einem Thema Schritt halten zu können, das sich infolge seiner steigenden Relevanz immer schneller entwickelt und nicht nur aufgrund seiner Interdisziplinarität, sondern vor allem infolge seiner Schnittstellen zu den unterschiedlichsten Lebens- und Wirtschaftsbereichen immer facettenreicher wird. Ihnen als Leser wünsche ich auch mit dieser zweiten Auflage des Werkes vor allem neue Erkenntnisse, die Sie in Ihrer Arbeit unterstützen und die einen unmittelbaren Mehrwert im täglichen Umgang mit einem komplexen Rechtsgebiet bringen. Und wie immer gilt: Sollten Sie Kommentare, Anregungen, Fragen oder Verbesserungsvorschläge haben, so zögern Sie bitte nicht, sich jederzeit gerne an mich zu wenden:

Prof. Dr. Dennis-Kenji Kipker
Hochschule Bremen
Fakultät für Elektrotechnik und Informatik
Flughafenallee 10
28199 Bremen
E-Mail: contact@denniskenjikipker.de

Bremen, im Dezember 2022 *Dennis-Kenji Kipker*

Inhaltsübersicht

Kapitel 12. Arbeitsrecht und IT-Sicherheit

Kapitel 13. Prozessuale Durchsetzung

Kapitel 14. Kritische Infrastrukturen

Kapitel 15. Verwaltung

Kapitel 15.1. Cybersicherheitsarchitektur des Bundes

Kapitel 15.2. Kompetenzen und Arbeit des BSI

Kapitel 15.3. IT-Sicherheitsrecht der (Bundes)Länder

Kapitel 15.4. Sichere elektronische Identitäten und sichere Identifizierung im E-Government

Kapitel 16. Gesundheit und Soziales

Kapitel 17. Gefahrenabwehr und Sanktionierung

Kapitel 18. Nachrichtendienstrecht

Kapitel 19. IT-Sicherheitsforschung

Kapitel 20. Neue Technologien und Verbraucherschutz

Kapitel 20.1 Vertrauensdienste im privaten Sektor

Kapitel 20.2 Blockchain, Smart Contracts und Künstliche Intelligenz

Kapitel 20.3 Digitaler Verbraucherschutz durch Security Updates und IT-Kennzeichen

Kapitel 20.4 Schutz der Meinungs- und Willensbildung vor technologiegestützten Interventionen

Kapitel 21. Internationaler Rahmen

Kapitel 21.1 Rechtsrahmen in der Europäischen Union

Kapitel 21.2 US-amerikanische Regulierung der IT-Sicherheit

Kapitel 21.3 Japanisches Cyber-Sicherheitsrecht

Kapitel 21.4 Cybersecurity-Regulierung in Israel

Kapitel 21.5 Korea's Cybersecurity Regulations and Enforcement related to Security Incidents

Kapitel 21.6 Cybersecurity Regulation in China

Kapitel 21.7 Cybersecurity in Russia

Kapitel 21.8 Cybersecurity Law and Policy in India

Kapitel 22. Völkerrechtliche Aspekte, Cyberwarfare

Kapitel 23. Anwendungsszenarien

Inhaltsverzeichnis

Kapitel 9. IT-Vertragsrecht

Kapitel 10. Ziviles Haftungsrecht

Kapitel 11. Urheber- und Lauterkeitsrecht, Know-How-Schutz

Kapitel 12. Arbeitsrecht und IT-Sicherheit

Kapitel 13. Prozessuale Durchsetzung

Kapitel 14. Kritische Infrastrukturen

Kapitel 15. Verwaltung

Kapitel 15.1. Cybersicherheitsarchitektur des Bundes

Kapitel 15.2. Kompetenzen und Arbeit des BSI

Kapitel 15.3. IT-Sicherheitsrecht der (Bundes)Länder

Kapitel 15.4. Sichere elektronische Identitäten und sichere Identifizierung im E-Government

Kapitel 16. Gesundheit und Soziales

Kapitel 17. Gefahrenabwehr und Sanktionierung

Kapitel 18. Nachrichtendienstrecht

Kapitel 19. IT-Sicherheitsforschung

Kapitel 20.2 Blockchain, Smart Contracts und Künstliche Intelligenz

Kapitel 20.3 Digitaler Verbraucherschutz durch Security Updates und IT-Kennzeichen

Kapitel 20.4 Schutz der Meinungs- und Willensbildung vor technologiegestützten Interventionen

Kapitel 21. Internationaler Rahmen

Kapitel 21.1 Rechtsrahmen in der Europäischen Union

Kapitel 21.2 US-amerikanische Regulierung der IT-Sicherheit

Kapitel 21.3 Japanisches Cyber-Sicherheitsrecht

Kapitel 21.7 Cybersecurity in Russia

Kapitel 21.8 Cybersecurity Law and Policy in India

Kapitel 22. Völkerrechtliche Aspekte, Cyberwarfare

Kapitel 23. Anwendungsszenarien