Rechtshandbuch Cyber-Security

IT-Sicherheit, Datenschutz, Gesellschaftsrecht, Compliance, M&A, Versicherungen, Aufsichtsrecht, Arbeitsrecht, Litigation

Herausgegeben von

Dr. Detlev Gabel
Rechtsanwalt, Frankfurt am Main

Dr. Tobias A. Heinrich, LL.M. (London)
Rechtsanwalt, Frankfurt am Main

und

Dr. Alexander Kiefner
Rechtsanwalt, Frankfurt am Main

Bearbeitet von

Steven Chabinsky; Melody Chan; Denise Cheung; Dr. Detlev Gabel; Tobias Gans; Dr. Tobias A. Heinrich, LL.M. (London); Dr. Justus Herrlinger; Dr. Alexander Kiefner; Markus Langen, LL.M. (Sydney); Aurora Leung; David Markoff; Robert Mechler; Dr. Lars Ole Petersen; F. Paul Pittman; Prof. Dr. Igor Podebrad; Hendrik Röger; Dr. Dominik Stier; Douglas Tan; John Timmons; Dr. Philip Trillmich; Dr. Andreas Wieland; Mark Williams; Prof. Dr. Norbert Wimmer; Christian Wirth; Karl-Jörg Xylander

Fachmedien Recht und Wirtschaft | dfv Mediengruppe | Frankfurt am Main

Bibliografische Information der Deutschen Nationalbibliothek

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

ISBN 978-3-8005-0012-3

dfv Mediengruppe

Satzkonvertierung: Lichtsatz Michael Glaese GmbH, 69502 Hemsbach

Druck und Verarbeitung: WIRmachenDRUCK GmbH, 71522 Backnang

Printed in Germany

Kapitel 1
Einleitung

Prof. Dr. Igor Podebrad/Dr. Detlev Gabel

Übersicht

I. Top-Thema „Cyber-Security“

Kein Geschäft ohne Risiko – das war schon immer so. Welche Risiken für Unternehmen besonders relevant sind, ändert sich jedoch in regelmäßigen Abständen. Für Top-Manager auf der ganzen Welt steht mittlerweile ein Risiko an der Spitze, das noch vor ein paar Jahren kaum jemand beachtet hatte: **Cyber-Attacken**. Dies meldet das World Economic Forum als ein Kernergebnis seines „Regional Risks for Doing Business Report 2018“ mit einem **1**

Hinweis darauf, dass Cyber-Attacken inzwischen als **Risiko Nummer eins** in Märkten gelten, die 50 % zum globalen Bruttoinlandsprodukt beitragen.[1]

2 Alarmiert ist jedoch nicht nur das Management, sondern laut „Allianz Risk Barometer 2019" auch die Riege der Risikoexperten. Aus Sicht der weltweit befragten Spezialisten stehen die Geschäftsrisiken „Betriebsunterbrechungen" und „Cyber-Vorfälle" an der Spitze drohender Gefahren.[2] Als Auslöser für Betriebsunterbrechungen und Hauptursache für entsprechende wirtschaftliche Schäden fürchten sie passenderweise in erster Linie Cyber-Vorfälle.[3]

3 Wie sieht die **Lage in Deutschland** aus? Diese Frage beantwortet zum Beispiel der Digitalverband Bitkom mit seiner regelmäßig aufgelegten Studie zum Thema „Wirtschaftsschutz". Im Studienreport 2018 ist zu lesen: „68 Prozent der Industrieunternehmen gaben an, in den vergangenen zwei Jahren Opfer von Datendiebstahl, Industriespionage oder Sabotage gewesen zu sein." Der Studie zufolge waren vermutlich weitere 19 % der Teilnehmer von entsprechenden Vorfällen betroffen – denn ob Daten abgeflossen sind, lässt sich nicht immer zweifelsfrei feststellen, und nicht alle Angriffe werden auch entdeckt.[4]

4 Bitkom sieht die deutsche Industrie insgesamt „**unter digitalem Dauerbeschuss**" durch Kleinkriminelle genauso wie durch organisierte Kriminalität und Hacker im Staatsauftrag.[5] Und von „Dauerbeschuss" kann man durchaus sprechen: 2018 waren in Deutschland über 800 Mio. Schadprogramme im Umlauf, wobei pro Tag ca. 390.000 Programmvarianten entdeckt werden konnten, wie der Lagebericht 2018 des Bundesamtes für Sicherheit in der Informationstechnik (BSI) warnend belegt.[6]

---

1 World Economic Forum, Pressemitteilung, 12.11.2018, https://www.weforum.org/press/2018/11/from-unemployment-to-growing-cyber-risk-business-executives-in-different-regions-have-different-worries/ (zuletzt abgerufen: 20.2.2019).

2 Allianz, Allianz Risk Barometer 2019, S. 8, https://www.agcs.allianz.com/assets/PDFs/Reports/Allianz_Risk_Barometer_2019.pdf (zuletzt abgerufen: 20.2.2019).

3 Allianz, Allianz Risk Barometer 2019, S. 10.

4 Bitkom, Spionage, Sabotage und Datendiebstahl – Wirtschaftsschutz in der Industrie, 2018, S. 14, https://www.bitkom.org/sites/default/files/file/import/181008-Bitkom-Studie-Wirtschaftsschutz-2018-NEU.pdf (zuletzt abgerufen: 20.2.2019).

5 Bitkom, Pressemitteilung, 11.10.2018, https://www.bitkom.org/Presse/Presseinformation/Cyberattacken-auf-deutsche-Industrie-nehmen-stark-zu.html (zuletzt abgerufen: 20.2.2019).

6 Bundesamt für Sicherheit in der Informationstechnik, Die Lage der IT-Sicherheit in Deutschland 2018, S. 50, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2018.pdf (zuletzt abgerufen: 20.2.2019).

Auch das Bundeskriminalamt (BKA) zeigt sich besorgt: Es hält die Cyber-Kriminalität gleich nach dem islamistischen Terrorismus für die derzeit größte Herausforderung für seine Arbeit.[7] Das BKA weist darauf hin: „Die Qualität der Angriffe nimmt weiter zu.“[8] Die Gefahr ist immens, Opfer von Cyber-Angriffen zu werden. Im Fadenkreuz stehen mittlerweile **Unternehmen jeder Größe**, auch und nicht zuletzt der **deutsche Mittelstand** mit seinen zahlreichen Weltmarktführern. Betroffen waren in letzter Zeit laut Bitkom vor allem die Chemie- und Pharmabranche, der Automobilbau, der Maschinen- und Anlagenbau und die Hersteller von Kommunikations- und Elektrotechnik.[9] Doch in Sicherheit wiegen darf sich keine Branche – und das weltweit. **5**

Eine Zahl lässt dabei aufhorchen: McKinsey hat ermittelt, dass nur 16 % der Manager ihr Unternehmen auf Cyber-Risiken gut vorbereitet sehen.[10] Diese **kritische Einschätzung** ist faktisch begründet. Der Cyber-Raum ist nicht ohne Risiken, und die Unternehmen richten sich hier zunehmend ein. Sie digitalisieren und vernetzen ihre Wertschöpfungsprozesse, arbeiten mit immer größeren Datenmengen aus unterschiedlichen Quellen und binden immer mehr Kunden, Lieferanten und Dienstleister in ihre IT-Landschaft ein. Produktionssysteme werden dadurch genauso gefährdet wie geistiges Eigentum, Kundendaten und andere Assets. **6**

Eine Entwicklung hat besondere Sprengkraft: die zunehmende Verbreitung des „**Internet of Things“ (IoT)**, das die physische und die virtuelle Welt hochgradig miteinander verbindet. McKinsey hat berechnet, dass bis 2020 46 % aller Internetverbindungen zwischen Maschinen bestehen werden, Tendenz steigend.[11] So öffnen sich viele Einfallstore für Cyber-Kriminelle, und diese sind eng und vielfältig miteinander verbunden. **7**

---

7 *Falk Steiner*, Tagung des BKA: Cyberkriminalität – eine der größten Herausforderungen, https://www.deutschlandfunk.de/tagung-des-bka-cyberkriminalitaet-eine-der-grossten.1783.de.html?dram:article_id=385265 (zuletzt abgerufen: 20.2.2019).

8 Bundeskriminalamt, Pressemitteilung, 27.9.2018, https://www.bka.de/SharedDocs/Pressemitteilungen/DE/Presse_2018/pm180927_BundeslagebildCybercrime.html (zuletzt abgerufen: 20.2.2019).

9 Bitkom, Spionage, Sabotage und Datendiebstahl – Wirtschaftsschutz in der Industrie, 2018, S. 17.

10 McKinsey, A new posture for cybersecurity in a networked world, S. 2, https://www.mckinsey.com/business-functions/risk/our-insights/a-new-posture-for-cybersecurity-in-a-networked-world (zuletzt abgerufen: 20.2.2019).

11 McKinsey, A new posture for cybersecurity in a networked world, S. 3.

II. Gängige Formen von Cyber-Attacken

8 Cyber-Kriminelle sind nicht nur technisch versiert und oft mit enormen Ressourcen ausgestattet, sie sind auch kreativ und finden immer wieder neue Wege, um Unternehmen in Bedrängnis zu bringen. Zu den gängigen Formen von Cyber-Attacke zählen die Folgenden:

1. Erpressung durch Computersabotage – Ransomware

9 Vielen Cyber-Kriminellen geht es schlichtweg darum, Geld zu erpressen. Sie suchen ihre Opfer entweder gezielt aus oder setzen bei ihrem Angriff auf Streuwirkung. Ein besonders prominentes Beispiel für einen breit gestreuten Angriff war die Attacke auf Unternehmen, Institutionen und Privatpersonen mit der **Ransomware „WannaCry“** im Mai 2017. Betroffen waren davon schätzungsweise über 230.000 Systeme in über 150 Ländern.[12] Generell gilt es zwei Arten von Ransomware zu unterscheiden: die eine versperrt den Zugriff auf ein System, die andere, wesentlich gefährlichere, verschlüsselt die Daten der infizierten Systeme. In beiden Fällen können Unternehmen nicht mehr mit ihren Rechnern arbeiten, der Zugriff auf Daten und Anwendungen ist verwehrt. Die betroffenen Unternehmen werden dann aufgefordert, ein „Lösegeld“, meist in Form digitaler Bitcoins, auf angegebene Konten zu überweisen, um wieder freizukommen.

2. Computersabotage um der Sabotage willen – Malware

10 Es geht nicht immer um Geld. Tatmotive sind oft auch die Zerstörung von Daten oder die Sabotage von Betriebsabläufen. Die Opfer werden mit Hilfe von **Schadsoftware (Malware)** attackiert, um ihre Wettbewerbskraft zu schwächen und ihre Reputation zu beschädigen. Im Juni 2017 sorgte etwa die Malware „NotPetya“ weltweit für Furore. In Deutschland wurden vor allem Unternehmen aus den Branchen Logistik, Finanzen und Gesundheit angegriffen.[13] Laut BKA hat „NotPetya“ dabei enorme Schäden angerichtet, weil die Malware die infizierten Systeme in wesentlichen Teilen auch dauerhaft unbrauchbar gemacht hat.[14]

---

12 Bundeskriminalamt, Bundeslagebild Cybercrime 2017, S. 12, https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2017.html (zuletzt abgerufen: 20.2.2019).

13 Bundeskriminalamt, Bundeslagebild Cybercrime 2017, S. 14.

14 Bundeskriminalamt, Bundeslagebild Cybercrime 2017, S. 14.

3. Überlastung von Infrastrukturen – DDoS-Attacken

Unternehmen können auch durch sog. **„Distributed Denial of Service"-Attacken (DDoS-Attacken)** wirkungsvoll angegriffen werden. Die Angreifer überlasten dabei die Systeme ihrer Opfer durch massive Anfragen an deren Server. Das BKA sieht darin die am häufigsten beobachteten Sicherheitsvorfälle im Cyber-Raum.[15] Entsprechende Attacken können außerordentlich wettbewerbsschädigend sein – etwa weil IT-basierte Arbeitsabläufe gestört werden oder Unternehmenswebsites nicht mehr erreichbar sind. Dies ist vor allem für Betreiber von Online-Shops oder anderer Kundenportale fatal. **11**

4. Gezielter dauerhafter Zugriff auf IT-Systeme – Advanced Persistent Threat (APT-Angriff)

Erpressungen, sabotierte Systeme oder überlastete Server werden in der Regel schnell erkannt. Hingegen bleibt es oft lange unentdeckt, wenn ein Unternehmen **ausspioniert** wird. Den Tätern kommt es darauf an, dauerhaft unerkannt zu bleiben, um sich möglichst viele Informationen bzw. Daten beschaffen zu können. Ihre Spionage-Software schleusen sie häufig über sog. Spear-Phishing-Mails in das Zielunternehmen.[16] Diese E-Mails werden gezielt eingesetzt, d. h. personalisiert und mit einem vertrauenswürdig wirkenden Absender an ausgewählte Mitarbeiter verschickt. Die Adressaten werden mit vermeintlich relevanten Botschaften dazu eingeladen, bestimmte Websites aufzusuchen oder Anhänge herunterzuladen, die jeweils mit Schadcode versehen sind. Die Schadsoftware kann sich dann auf den betreffenden Rechnern installieren und sich im Hintergrund im Unternehmen ausbreiten. Das BSI weist u. a. auf eine bei Cyber-Spionen zunehmend beliebte Methode hin: Infiziert werden dabei die Websites und Software-Archive von Software-Herstellern; wenn Mitarbeiter eines Unternehmens nach einem Update für bestimmte Programme suchen und diese installieren, holen sie sich den digitalen Spion mit ins Haus.[17] Wie auch immer die APT-Angriffe erfolgen – den Tätern kann es gelingen, in den Besitz umfangreicher sensibler Kundendaten zu gelangen oder einen anderen gravierenden Schaden anzurichten. **12**

---

15 Bundeskriminalamt, Bundeslagebild Cybercrime 2017, S. 17.

16 Bundeskriminalamt, Bundeslagebild Cybercrime 2017, S. 18.

17 Bundesamt für Sicherheit in der Informationstechnik, Die Lage der IT-Sicherheit in Deutschland 2018, S. 23.

5. Die Chef-Masche – CEO-Fraud

13 Ein besonders dreistes Vorgehen von Cyber-Kriminellen ist schließlich der sog. „**CEO-Fraud**“.[18] Die Täter fordern dabei relevante Mitarbeiter eines Unternehmens etwa per E-Mail dazu auf, einen größeren Geldbetrag ins Ausland zu überweisen. Nicht selten haben sie damit Erfolg. Denn sie geben sich als CEO oder als eine andere Führungskraft des betreffenden Unternehmens aus und können so Druck machen, auch ohne weiter hinterfragt zu werden. Vorab haben sie sich etwa mit Hilfe von Unternehmenspublikationen, Wirtschaftsnachrichten und Quellen wie dem Handelsregister über Projekte, Geschäftspartner und geplante Investitionen informiert und sich auf dieser Basis eine glaubwürdige „Story“ für ihre Aufforderung zurechtgelegt. Geeignete „Ansprechpartner“ mit deren Dialogdaten lassen sich häufig durch einfache Recherchen herausfinden – auch Social-Media-Plattformen oder Online-Netzwerke sind dafür wahre Fundgruben.

III. Kosten

14 Bereits diese grob skizzierte Bedrohungslage lässt erkennen: Bei Cyber-Crime geht es nicht um Delikte, die Unternehmen auf die leichte Schulter nehmen sollten, sondern um Angriffe, die sie im Kern treffen können. Ausdruck findet diese Relevanz in den Kosten, die Unternehmen im Zuge von Cyber-Attacken entstehen.

15 Das Ponemon Institute hat im Auftrag von IBM Security Zahlen ermittelt:[19] Die Ergebnisse sind beeindruckend. So betragen laut der Penomenon Studie „**Cost of a Data Breach 2018**“ weltweit die durchschnittlichen Kosten eines Datenlecks („data breach“) 3,86 Mio. USD. Verglichen mit der entsprechenden Studie aus dem Vorjahr ist das ein Kostenanstieg um 6,4 %. Sogenannte Mega-Breaches, bei denen zwischen 1 Mio. und 50 Mio. Datensätze („records“) abgeflossen sind, schlagen noch höher zu Buche: Die Kosten liegen hier zwischen 40 Mio. USD und 350 Mio. USD.

16 Für **Deutschland** verweist der Studienbericht von Bitkom aus dem Jahr **2018** ebenfalls auf signifikante Kosten, die Industrieunternehmen innerhalb von zwei Jahren durch Wirtschaftsspionage, Sabotage oder Datendiebstahl

---

18 Bundeskriminalamt, Flyer Warnhinweis CEO-Fraud, https://www.bka.de/SharedDocs/Downloads/DE/IhreSicherheit/CEOFraud.html (zuletzt abgerufen: 20.2.2019).

19 IBM, Pressemitteilung, 11.7.2018, https://newsroom.ibm.com/2018-07-11-IBM-Study-Hidden-Costs-of-Data-Breaches-Increase-Expenses-for-Businesses (zuletzt abgerufen: 20.2.2019).