GRC MANAGEMENT - GOVERNANCE, RISK & COMPLIANCE:

IT-Sicherheit als integrierter Bestandteil eines Compliance-Managements

2. aktualisierte, erweiterte Auflage

Fabian Sachs

Sachs

GRC- Management- Governance, Risk and Compliance: IT- Sicherheit als Bestandteil eines integrierten Compliance-Managements

2. aktualisierte und erweiterte Auflage

Fabian Sachs, LL.M., D.D.F. (Grenoble)

GRC- Management-Governance, Risk and Compliance:

IT- Sicherheit als Bestandteil eines integrierten Compliance-Managements

Theodor-Hoffmann-Platz 15, 56154 Boppard

GRC- Management- Governance, Risk and Compliance: IT- Sicherheit als Bestandteil eines integrierten Compliance- Managements

2. aktualisierte und erweiterte Auflage 2020

Autor: Fabian Sachs
Umschlaggestaltung, Illustration: Huong Tran
Lektorat: Detlef Sachs

Verlag & Druck: tredition GmbH, Halenreie 40-44, 22359 Hamburg

ISBN 978-3-347-18699-6 (Paperback)

ISBN 978-3-347-18700-9 (Hardcover)

ISBN 978-3-347-18701-6 (e-Book)

Bibliografische Information der Deutschen Bibliothek

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

Printed in Germany

Hinweis für die Nutzung des Werkes:

Erkenntnisse in der Informationstechnologie, als auch gesetzliche und nichtgesetzliche Anforderungen unterliegen einem laufenden Wandel durch Forschung und Entwicklung, der Rechtsprechung und Weiterentwicklung des Rechts bzw. einschlägiger Standards und Frameworks. Der Autor hat nach großer Sorgfalt darauf geachtet, dass die im Werk aufgeführten rechtlichen Angaben dem derzeitigen Wissenstand entsprechen. Es entbindet daher dem Nutzer keineswegs von seiner Verpflichtung anhand weiterer Informationsquellen dies zu überprüfen, ob die im Buch gemachten Angaben mit den dortigen gemachten Angaben abweichen. Der Nutzer sollte in eigener Verantwortung seine Entscheidung entsprechend treffen.

Haftungsausschluss für gemachte Internetverweise
In diesem Buch wurden Links (Internetverweise) zu Seiten im Internet hinterlegt. Hierbei gilt für all diese Links, dass der Autor keinerlei Einfluss für die Inhalte oder Gestaltung der verlinkten Seiten hat. Daher kann für diese fremden Inhalte auch keinerlei Gewähr übernommen werden. Es ist für die Inhalte der verlinkten Seiten immer der jeweilige Betreiber oder der Anbieter der Seite verantwortlich. Zum Zeitpunkt der Links wurden diese vom Autor auf etwaige Rechtsverstöße hin überprüft. Dabei waren zu diesem Zeitpunkt keine rechtswidrigen Inhalte erkennbar. Die stetige inhaltliche Kontrolle der in diesem Buch aufgeführten Links zu den entsprechenden Seiteninhalten ist ohne spezifische Anhaltspunkte einer Rechtsverletzung ohnehin nicht zumutbar. Derartige Links werden vom Autor bei Bekanntgabe entsprechend umgehend entfernt. Der Autor distanziert sich daneben ausdrücklich von allen Inhalten aller Seiten, die in diesem Buch aufgeführt sind.

Für meine Eltern

Vorwort

Zielgruppe dieses Buches sind Beschäftigte, Akademiker und Fachkräfte, welche sich mit der IT- Sicherheit und dem Datenschutz auseinandersetzen und in Unternehmen an einem GRC-Management beteiligt sind. Dieses Buch soll Ihnen einen Einblick in das Thema GRC- Management geben, um neben der Schaffung einer höheren Akzeptanz zum Thema Datenschutz und Datensicherheit auf Managementebene auch eine Etablierung im Unternehmen in die Wege leiten zu können. Unter dem Thema GRC-Management: IT- Sicherheit als Bestandteil eines integrierten Compliance- Managements fallen ganz unterschiedliche Disziplinen, wie z.B. die Informationstechnologie, betriebswirtschaftliche Aspekte, als auch nationales, europäisches und internationales Recht. Daneben existieren noch eine Vielzahl an unterschiedlichen Regelungen im nichtgesetzlichen Bereich, die es zu beachten gilt.

Die zweite aktualisierte und erweiterte Auflage wurde vollständig überarbeitet. Aufgrund der entstandenen Praxisrelevanz und aktueller Gesetzgebung wurde das Thema Datenschutz erheblich erweitert. Darüber hinaus wurde das Thema COBIT und das IT-Sicherheitsmanagement ergänzt. Zusätzliche Informationen und Hilfestellungen zum Vertragsmanagement innerhalb der Informationstechnologie runden, ebenso wie die Bereiche Pandemie und Datenschutz, die Aktualisierung ab.

Für die zahlreichen Anregungen und Wünsche der Leserschaft möchte ich mich herzlich Bedanken. Ein ganz besonderer Dank gilt meinem Vater, der sich für dieses doch nun etwas umfangreicheres Werk die Zeit des fachlichen Lektorats genommen hat, als auch meiner Lebensgefährtin Huong Tran, die sich der Gestaltung des Buchumschlages passioniert angenommen hat.

Ich hoffe Ihnen mit diesem Buch einen umfassenden Einblick zu ermöglichen und begrüße Anregungen und konstruktive Kritik sehr. Sie können mir diese gerne mit dem Betreff Buchkritik GRC an fabian_sachs@email.de via E-Mail zukommen lassen.

Abschließend wünsche ich Ihnen viel Freude bei dieser Lektüre.

Fabian Sachs, LL.M., D.D.F. (Grenoble)

Bad Salzig, München November 2020

Inhaltsverzeichnis

d) Folgen bei Nichtbeachtung des Datenschutzes
e) Meldeanforderungen nach DSGVO
f) Datenschutzfolgeabschätzung nach DSGVO
g) Benachrichtigung betroffener Personen nach DSGVO
h) Durchführung von Penetrationstests nach DSGVO
i) Privacy by Design nach DSGVO
j) Privacy by Default nach DSGVO
k) Datenlöschung nach DSGVO
l) Übermittlung zwischen Konzernunternehmen
m) Datennutzung für die Compliancetätigkeiten
    aa) Beteiligung des Betriebsrates
    bb) Kommunikation gegenüber Mitarbeitern
    cc) Nutzung von personenbezogenen Daten bei internen Ermittlungen
n) Planung in datenschutzrechtlicher Hinsicht
    aa) Analyse bereits bestehender Strukturen
    bb) Gap-Analyse
    cc) Verarbeitungsverzeichnis
    dd) Zweckänderung und -festlegung
    ee) Löschkonzepte
    ff) Recht auf Vergessenwerden
    gg) Recht auf Datenübertragbarkeit
    hh) Recht auf Verarbeitungseinschränkung
    ii) Recht auf Auskunft
    jj) Recht auf Berichtigung
    kk) Widerspruchsrecht
    ll) Gemeinsam für die Verarbeitung Verantwortliche
    mm) Auftragsverarbeitung innerhalb der EU und EWR
        aaa) Weitere Auftragsverarbeiter
        bbb) Pflichten des Auftragsverarbeiter
        ccc) Verhaltensregeln
    nn) Auftragsverarbeitung außerhalb der EU und EWR (Drittland)
    oo) Datenschutzfolgeabschätzung

pp) Umgang mit Datenpannen

qq) Datenschutz und Pandemien

o) Anforderungen nach Basel II, III

p) Gesetzliche Behandlung der Korruption in Deutschland

aa) Gesetz über Ordnungswidrigkeiten

bb) Strafgesetz

cc) Einkommenssteuergesetz

q) Gesetzliche Behandlung der Korruption in den USA

r) Gesetzliche Behandlung der Korruption im Vereinigten Königreich

s) Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG)

t) Gesetz zur Unternehmensintegrität und Modernisierung des Anfechtungsrechts (UMAG)

u) Aktiengesetz (AktG)

v) Lizenzmanagement

w) Lizenzen und Urheberrecht

1.2 Regelungen im nichtgesetzlichen Bereich

a) IDW-Standards

b) Deutscher Corporate Governance Kodex (DCGK)

c) OECD Principles of Corporate Governance

d) Framework in der IT- Governance (ISACA, ITGI)

e) ISO/IEC 2700x

aa) Management in der Informationssicherheit gem. ISO/IEC 27001 (ISMS)

bb) Code of Practice gem. ISO/IEC 27002

cc) Risikomanagement in der Informationssicherheit gem. ISO/IEC 27005

dd) Datenschutz gem. ISO/IEC 27018

f) IT- Grundschutzkatalog des BSI

g) CobiT Framework im IT-Bereich der strategischunternehmerischen Managementebene

h) COSO

i) Val IT

j) IT-Grundsätze (Policies) und deren praxisgerechte Implementierung

2. Risk

2.1 Akteure

2.2 Risiken in der Informationstechnologie

2.3 Risikobestimmung

a) Potenzielle Risiken und Risikoarten

b) Datendiebstahl

aa) Datendiebstahl von Microsoft Windows-Systemen

bb) Datendiebstahl von Linux-Systemen

cc) Hacking

dd) Malware

ee) Botnetze

ff) Denail of Service (DoS)

gg) Phising

hh) Social Media

ii) Keylogger

jj) Risiko USB-Schnittstelle

kk) Risiko WLAN

ll) Risiko bei SCADA- Systemen

c) Eintrittswahrscheinlichkeit und deren Konsequenzen

d) Probleme bei subjektiver Einschätzung der Risiken und deren Bewertung

2.4 Grundlagenmethoden des Risikomanagements

a) Berechnungsverfahrungen zur Analyse und Darstellung der Risiken

aa) Risiko- und Risikobewertungsmatrix

bb) Risikoportfolio und die Kriterien zur Einstufung des möglichen Schadens

cc) Risikokatalog

b) Bestimmungen zur Ausführung von Informationen

2.5 Methoden im Bereich des IT-Risikomanagements

a) Analyse von Schwachstellen

b) Ergreifung von Maßnahmen

aa) Maßnahmen zum Schutz personenbezogener Daten

bb) Schutz der Beschäftigtendaten

bb) Patchmanagement und Virenschutz

cc) Netzwerkmonitoring

dd) EDV-Sicherungen

ee) E-Mail und Internetnutzung

ff) Technische Vorgaben zum Lizenzmanagement

gg) Überprüfung der umgesetzten Maßnahmen

hh) Methodendidaktik CRAMM

ii) Fehlermöglichkeits- und Einflussanalyse

2.6 Risiko Korruption

2.7 Moralische Risiken

3. Compliance

3.1 Sicherheitskonzepte bei unternehmerischer Infrastruktur

3.2 Notfallplan

a) Business Continuity Management (BCM)

b) Umsetzung des BCM

3.3 Präventive Schadensminimierung durch Vertragsmanagement

II. Praktische Anwendung des GRC

1. Unternehmensbezogener Lösungsansatz am Praxisbeispiel SAP

2. Outsourcing

2.1 Cloud Computing

Abkürzungsverzeichnis

A.a.O.	am angegebenen Ort
Abb.	Abbildung
Abs.	Absatz
AES	Advanced Encryption Standard
AEUV	Vertrag über die Arbeitsweise der Europäischen Union
AG	Aktiengesellschaft
AG*	Amtsgericht
AGG	Allgemeines Gleichbehandlungsgesetz
AktG	Aktiengesetz
Anm.	Anmerkung
AO	Abgabenordnung
APT	Advanced Persistent Threat
ArbGG	Arbeitsgerichtsgesetz
Az.	Aktenzeichen
BAG	Bundesarbeitsgericht
BayLDA	Bayerischen Landesamtes für Datenschutzaufsicht
BCM	Business Continuity Management
BCR	Binding Corporate Rules

Bd.	Band
BetrVG	Betriebsverfassungsgesetz
BeckOK	Beck’scher Online-Kommentar
BGB	Bürgerliches Gesetzbuch
BGH	Bundesgerichtshof
BSA	Business Software Alliance
BSI	Bundesamt für Sicherheit in der Informationstechnik
bzgl.	bezüglich
bzw.	beziehungsweise
BDSG	Bundesdatenschutzgesetz
BIA	Business Impact Analyse
BITKOM	Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V.
BIOS	Basic Input Output System
BZRG	Bundeszentralregistergesetz
ca.	circa
CD	Compact Disc
CDs	Compact Discs
CEO	Chief Executive Officer
CIIP	Critical Information Infrastructure Protection
CIP	Critical Infrastructure Protection

CMOS- SRAM	Complementary Metal Oxide Semiconductor-Static Random- Access Memory
CNLI	Commission nationale de l'informatique et des libertés
CobiT	Control Objectives for Information and related Technology
COSO	Committee of Sponsoring Organizations of the Treadway Commission
CR	COMPUTER UND RECHT
CRAMM	Centre for Information Systems Risk Analysis and Management Method
CIA	Central Intelligence Agency
CRO	Chief Risk Officer
DAkkS	Deutsche Akkreditierungsstelle
DB	Der Betrieb
DCGK	Deutsche Corporate Governance Kodex
DIN	Deutsches Institut für Normung
DSG	Datenschutzgesetz
DSS	Data Security Standard
DoS	Denial of Service
DIN	Deutsches Institut für Normung
DSFA	Datenschutzfolgeabschätzung
DSK	Datenschutzkonferenz

DuD	Datenschutz und Datensicherheit
DVBl	Deutsches Verwaltungsblatt
DVDs	Digital Versatile Discs
EDSA	Europäische Datenschutzausschuss
EDV	Elektronische Datenverarbeitung
EG	Europäische Gemeinschaft
EN	Europäische Norm
ENISA	European Network and Information Security Agency
E.O.	Executive Order
ERP	Enterprise resource planning
EStG	Einkommensteuergesetz
et al.	et alii
etc.	et cetera
EU	Europäische Union
e.V.	eingetragener Verein
evtl.	eventuell
EWR	Europäischer Wirtschaftsraum
FAQ	Frequently Asked Questions
FBI	Federal Bureau of Investigation
FCPA	Foreign Corrupt Practices Act
FISA	Foreign Intelligence Surveillance Act

FMEA	Fehlermöglichkeits- und Einflussanalyse
ff.	fortfolgende
GDPdU	Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen
GDPR	General Data Protection Regulation
GDV	Deutschen Versicherungswirtschaft e.V.
gem	gemäß
GenG	Genossenschaftsgesetz
GeschGehG	Gesetz zum Schutz von Geschäftsgeheimnissen
GG	Grundgesetz
GewO	Gewerbeordnung
GRCh	Charta der Grundrechte der Europäischen Union
GoBS	Grundsätzen ordnungsgemäßer Datenverarbeitungsgestützter Buchführungssysteme
GmbH	Gesellschaft mit beschränkter Haftung
GmbH & Co. KG	Gesellschaft mit beschränkter Haftung & Compagnie Kommanditgesellschaft
GRC	Government, Risk and Compliance
GRU	Glawnoje Raswedywatelnoje Uprawlenije
GRUR	Gewerblicher Rechtsschutz und Urheberrecht

GG	Grundgesetz
GRUB	Grand Unified Bootloader
HIPAA	Health Insurance Portability and Accountability Act
HMD	Handbuch der maschinellen Datenverarbeitung
HPM	High Power Microwave
Hrsg.	Herausgeber
IDS	Intrusion Detection System
ICS-CERT	Industrial Control Systems Cyber Emergency Response Team
IEC	International Electrotechnical Commission
i.d.R.	in der Regel
IDW	Institut der Wirtschaftsprüfer
IKS	internes Kontrollsystem
IPMA	International Project Management Association
ISACA	Information Systems Audit and Control Association
ISMS	Informationssicherheitsmanagementsystem
ITGI	IT- Governance Institute
ITIL	IT Infrastructure Library
IPSec	Internet Protocol Security
ISO	International Organization for

	Standardization
ISPRAT	Interdisziplinäre Studien zu Politik, Recht, Administration und Technologie e.V.
i.V.m.	in Verbindung mit
inkl.	inklusive
insb.	Insbesondere
ISMS	Information Security Management System
IT	Informationstechnologie
KG	Kommanditgesellschaft
KGaA	Kommanditgesellschaft auf Aktien
KMU	kleine und mittlere Unternehmen
KonTraG	Gesetz zur Kontrolle und Transparenz im Unternehmensbereich
KPMG	Klynfeld, Peat, Marwick und Goerdeler
LAG	Landesarbeitsgericht
LfDI BW	Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Baden-Württemberg
Linux	Linus torvalds unix
MBR	Master Boot Record
mbH	mit beschränkter Haftung
MIR	Medien Internet und Recht
MMR	Multimedia und Recht

m.w.N.	mit weiteren Nennungen
NATO	North Atlantic Treaty Organization
NDR	Norddeutscher Rundfunk
NIFIS	Nationale Initiative für Informations- und Internet-Sicherheit e.V.
NJW	Neue Juristische Wochenschrift
NSA	National Security Agency
NZA	Neue Zeitschrift für Arbeitsrecht
NZA-RR	Neue Zeitschrift für Arbeitsrecht-Rechtsprechungs-Report Arbeitsrecht
OECD	Organisation for Economic Co-operation and Development
OHG	offene Handelsgesellschaft
OLG	Oberlandesgericht
OSS	One Stop Shop
OWiG	Gesetz über Ordnungswidrigkeiten
PaaS	Platform as a Service
PC	Personal Computer
PCCIP	President´s Commission on Critical Infrastructure Protection
PCI	Payment Card Industry
PDCA	Plan-Do-Check-Act
PHP	Personal Home Page Tools

PINs	Personal Identification Numbers
PMBOK	Project Management Body of Knowledge
POST	Power On Self Test
PPD	Presidential Policy Directive
PPTP	Point-to-Point Tunneling Protocol
PIA	Privacy Impact assessment
pwc	PricewaterhouseCoopers (pwc)
Q&R	Questions & Answers
RAID	Redundant Array of Independant
Rn.	Randnummer
SaaS	Software as a Service
SARS-CoV-2	severe acute respiratory syndrome coronavirus 2
SCADA	Supervisory Control and Data Acquisition
SDM	Standard-Datenschutzmodell
SEC	Securities and Exchange Commission
SLA	Service Level Agreement
SMS	Short Message Service
SOX	Sarbanes-Oxley Act
sog.	sogenannten
SSL	Secure Sockets Layer
StGB	Strafgesetzbuch

SZ	Süddeutsche Zeitung
TAN	Transaktionsnummer
TKG	Telekommunikationsgesetzes
TKModG	Telekommunikationsmodernisierungsgesetz
TMG	Telemediengesetz
TNS Emid	Taylor Nelson Sofres Erforschung der öffentlichen Meinung, Marktforschung, Nachrichten, Informationen und Dienstleistungen
TTDSG	Telekommunikations-Telemedien-Datenschutz-Gesetz
UrhG	Urheberrechtsgesetz
UMAG	Gesetz zur Unternehmensintegrität und Modernisierung des Anfechtungsrechts
URL	Uniform Resource Locator
USA	United States of America
U.S.C.	United States Code
USB	Universal Serial Bus
UStG	Umsatzsteuer
Vgl.	Vergleiche
VDG	Vertrauensdienstegesetz
VDI	Verein Deutscher Ingenieure
VoIP	Voice over IP
VPN	Virtual Private Network

VwVfG	Verwaltungsverfahrensgesetz
WDR	Westdeutscher Rundfunk Köln
WHO	World Health Organization
Wi-Fi	Wireless Fidelity
WLAN	Wireless Local Area Network
WPA	Wi-Fi Protected Access
WPA2	Wi-Fi Protected Access 2
z.B.	zum Beispiel

A. Entwicklung von IT- Bedrohungen

Die immer stärker ausgeprägte Implementierung der Informationstechnik (IT) in kleinen, mittelständischen Unternehmen und Konzernen und die seit Jahren wachsende Anzahl potenzieller Bedrohungen im Bereich der Wirtschaftskriminalität sowie der zum Teil äußerst fahrlässige Umgang innerhalb der Datenverarbeitung und -speicherung steigern den Bedarf an möglichen Lösungsansätzen im Bereich des GRC- Managements, vor allem in Hinblick auf die IT-Sicherheit als Bestandteil eines integrierten Compliance-Managements. Nach einer Studie der Wirtschaftsprüfungsgesellschaft KPMG befürchten weit über drei Viertel (87 Prozent) der Unternehmen potenzielle Opfer von Datenmissbrauch oder Datendiebstahl zu werden. Tatsächlich wurde bereits jedes dritte Unternehmen in den Jahren 2012 und 2013 Opfer von Wirtschaftskriminalität. Obwohl von einer potenziell steigenden Gefahr in diesem Bereich ausgegangen werden kann und bereits 55 Prozent der Täter wirtschaftskrimineller Handlungen innerhalb des Unternehmens anzutreffen sind sowie 45 Prozent der deliktischen Handlungen von Personen aus dem unternehmensexternen Umfeld erfolgen,[1] stufen 70 Prozent der befragten Unternehmen in Deutschland das eigene Risiko in Hinblick auf Handlungen im Bereich der Wirtschaftskriminalität als gering ein.[2] Deutsche Unternehmen verkennen die steigende Anzahl potenziell organisierter Cyberkriminalität und Wirtschaftsspionage, als auch die Risiken der eigenen Mitarbeiter. Dies kann für die Unternehmen massive rechtliche und finanzielle Folgen haben. Der Schaden durch Wirtschaftsspionage wird nach

dem Verein Deutscher Ingenieure (VDI) in Deutschland jährlich auf 100 Milliarden Euro geschätzt.[3] Unternehmen, insbesondere kleine, mittelständische Unternehmen (KMU), rücken vermehrt in den Fokus von Cyberkriminellen. Dabei sind diese häufig Opfer von Erpressung, Wirtschaftsspionage und Abgreifen von Know- How durch Konkurrenzunternehmen.[4] Es existieren in der Informationstechnologie unterschiedliche Risikoakteure bzw. Angreifertypologien (versierte und weniger versierte Hacker, politische Gruppierungen oder Innentäter,[5] als auch Nachrichtendienste). Seit den Jahren 2013 und 2014 ist das technische Verständnis und Wissen über nachrichtendienstliche Aktivitäten gewachsen.[6]

In den folgenden Seiten wird ein Einblick in das Thema „GRC-Management- Governance, Risk and Compliance: IT-Sicherheit als Bestandteil eines integrierten Compliance-Managements" gegeben und Lösungsansätze aufgezeigt.

I. Industrie 4.0

Die Industrie 4.0 wurde aufgrund einer Hightech-Strategie der Bundesregierung und des gleichnamigen Projektes ins Leben gerufen. Unter diesen Begriff fällt die Vernetzung der Produktion mit modernster Kommunikations- und Informationstechnik.[7]

Industrie 4.0 bezieht sich auf die vorherigen drei industriellen Revolutionen (Dampfmaschine (1.0), Fließband (1.0), Elektronik und IT (3.0) Die Produktion mittels Industrie 4.0 bedeutet die Nutzung intelligenter Fabriken- smart factories durch digital vernetzte, intelligente Systeme, um eine effiziente und flexible Produktion zu ermöglichen. Es soll die individuelle Produktion ebenso ermöglichen, wie

auch die damit verbunden Produkte maßgeschneidert an den Kunden zu bringen.[8]

Hierbei müssen Normen Standards für einzelne Industriesektoren entwickelt, der Datenschutz und die IT-Sicherheit ebenso beachtet werden, als auch die Veränderungen in der Arbeitsorganisation.[9]

II. Folgen der Vernetzung

Im Mai 2015 erfolgte ein Hackerangriff auf den Bundestag.[10] Hierbei wurden 50 Gigabyte Daten[11] durch den Angriff entwendet. Zu diesem Zeitpunkt war noch nicht abschließend geklärt, welche Informationen abgeflossen sind.[12] Anfang Juli 2015 erklärte ein Mitarbeiter des Bundesamtes für Sicherheit in der Informationstechnologie (BSI), dass auf das folgende Wochenende des 7. Mai 2015 Täter in der Lage gewesen seien, sich frei im Bundestag-Netzwerk bewegen zu können. Es sei den Angreifen, so der Mitarbeiter des BSI möglich gewesen, fünf von sechs der Domainadministratoraccounts der Bundestagsverwaltung zu kompromittieren und nutzen zu können. Beängstigend ist, dass Hinweise von Nutzern bei der IT- Abteilung des Bundestages nicht ernst genommen worden waren und man erst mit der Meldung des Verfassungsschutzes am 12. Mai 2015 den Ernst der Lage erkannte. Noch dazu wurde das Bundesamt für Verfassungsschutz (BfV) über ein britisches Unternehmen darüber informiert, dass ein Kunde des Unternehmens die übertragenen Daten des Bundestages auf dessen Server hatte und sich darüber „wunderte“. In der Sommerpause des Bundestages 2015 erfolgte eine viertägige Netzabschaltung, die darin gipfelte, dass nur mit Hilfe des BSI, des BfV und durch externe Unternehmen der

Angriff nun abgewehrt werden konnte.[13] Die Linkspartei weigerte sich aufgrund der Überwachung der Partei durch das BfV bei deren Mitwirkung.[14] Laut dem Abschlussberichts des BSI vom 03. November 2015 wurde die methodische Einordnung des Cyber-Angriffs festgestellt. Es handelte sich hierbei um ein klassisches Advanced Persistent Threat (APT)- Muster,[15] welches durch gängige Methoden und für die Öffentlichkeit verfügbare Programme durchgeführt worden ist. Die Analyse ergab, dass die Angreifer drei Wochen Zeit hatten, um die Daten entsprechend abgreifen zu können. Ende Mai 2015 sei, so laut BSI, das IT- System vom Bundestag wieder vollständig abgesichert. Anfang 2016 teilte das BfV mit, dass davon auszugehen sei, dass es sich bei dem Hackerangriff auf den Bundestag um einen geheimdienstlich gesteuerten Angriff gehalten haben könnte. Die Bundesanwaltschaft nahm daraufhin Mitte Januar 2016 förmliche Ermittlungen wegen des Verdachts von geheimdienstlicher Agententätigkeit gegen unbekannt auf.[16]

Anfang Mai 2020 hat die Bundesanwaltschaft laut Informationen des Westdeutschen Rundfunks (WDR), der Süddeutschen Zeitung (SZ) und des Norddeutschen Rundfunks gegen einen möglichen Mitarbeiter des russischen Militärgeheimdienstes Glawnoje Raswedywatelnoje Uprawlenije (GRU) Haftbefehl erlassen. Der Mitarbeiter steht in Verdacht, an dem Hackerangriff auf den Bundestag beteiligt gewesen zu sein.[17] Hierbei wurde bei der niederländischen Spionageabwehr im Jahr 2018 durch Abfangen des PKW von vier russischen Diplomaten und dem sichergestellten Material die Beweislage zum Haftbefehl geschaffen.[18]

Ein weiteres Beispiel ist der am 12. Mai 2017 „WannaCry“ Trojaner,[19] der innerhalb von wenigen Stunden mehr als 7.000 Rechner befallen hatte und dazu führte, dass Automobilunternehmen ihre Produktion stoppten und britische Krankenhäuser Operationen verschoben haben. Daneben waren 450 Rechner der Deutschen Bahn, deren Befall sich durch nicht mehr funktionierende Anzeigetafeln und Videoüberwachungssysteme an den Bahnhöfen äußerte, betroffen.[20]

Die Vernetzung unterschiedlicher Systeme führt zu einer immer weiteren potenziellen Bedrohung von IT- Systemen.

---

1 Die Prozentzahlen beziehen sich auf Fälle, bei denen der oder die Täter ermittelt werden konnten, vgl. *KPMG AG Wirtschaftsprüfungsgesellschaft,* Studie Wirtschaftskriminalität in Deutschland 2014, URL 1.

2 Vgl. *KPMG AG Wirtschaftsprüfungsgesellschaft,* Studie Wirtschaftskriminalität in Deutschland 2014, URL 1.

3 Vgl. *Nationale Initiative für Informations- und Internet-Sicherheit e.V. (NIFIS),* Mangelnde IT-Sicherheit: Unternehmen unterschätzen rechtliche Konsequenzen, URL 2.

4 Vgl. *Kraft, Weyert,* Network Hacking: Professionelle Angriffs- und Verteidigungstechniken gegen Hacker und Datendiebe, 2014, S. 5.

5 Als Innentäter werden Täter bezeichnet, die über entsprechendes internes Fachwissen verfügen. Innentäter können neben Sabotage auch unternehmensinterne bzw. vertrauliche Informationen abschöpfen, vgl. *Bundesamt für Sicherheit in der Informationstechnik,* Die Lage der IT-Sicherheit in Deutschland 2014, URL 3, S. 25.

6 Vgl. *Bundesamt für Sicherheit in der Informationstechnik,* Die Lage der IT-Sicherheit in Deutschland 2014, URL 3, S. 22.

7 Vgl. Bundesministerium für Bildung und Forschung: Digitale Wirtschaft und Gesellschaft, Industrie 4.0, URL 4.

8 Vgl. Plattform Industrie 4.0- Was ist Industrie 4.0?, URL 5.

9 Vgl. a.a.O.

10 Vgl. *Evers,* Was tun im Fall der Fälle? Risiko- und Notfallmanagement in der IT für die eigene Behörde in Behörden Spiegel, Ausgabe Juli 2015, S. 36.

11 Diese Datenmenge entspricht mehrere Millionen DIN- A4 Seiten, vgl. *Henke,* Ist die Attacke ein NATO- Verteidigungsfall? Cyber-Angriff auf den