Wollinger | Schulze

Handbuch Cybersecurity für die öffentliche Verwaltung

KSV Verwaltungspraxis

Handbuch Cybersecurity für die öffentliche Verwaltung

Herausgegeben von

Prof. Dr. Gina Rosa Wollinger
Hochschule für Polizei und öffentliche Verwaltung Nordrhein-Westfalen

und

Prof. Dr. Anna Schulze
Hochschule des Bundes für öffentliche Verwaltung

KOMMUNAL- UND SCHUL-VERLAG · WIESBADEN

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

Satz: Kumpernatz + Bromann • Schenefeld b. Hamburg

ISBN: 978-3-8293-1606-4
eISBN 978-3-8293-1633-0

Inhalt

Teil 4
Ausblick: Innovationen zur Begegnung von Cyberangriffen

Autorenverzeichnis

Dr. Marie Bergmann
ist Informatikerin. Nach mehrjähriger Tätigkeit in der Prozess- und Strategieberatung mit Schwerpunkt IT-Governance war sie über drei Jahre als IT-Auditorin beim Bundesrechnungshof. Seit 2019 lehrt sie an der Hochschule des Bundes für öffentliche Verwaltung in Brühl.

Prof. Dr. Thomas Deelmann
lehrt Management, Organisation und Strategie an der Hochschule für Polizei und öffentliche Verwaltung NRW in Köln. Vorher war er von 2012 bis 2016 Professor an der BiTS – Business and Information Technology School, Iserlohn.

Arne Dreißigacker
ist Soziologe und seit 2015 als wissenschaftlicher Mitarbeiter am Kriminologischen Forschungsinstitut Niedersachsen e.V. (KFN) tätig. Zu seinen Forschungsschwerpunkten gehören das Kriminalitätsdunkelfeld, Wohnungseinbruchdiebstahl, Vorurteilskriminalität und Cyberkriminalität. Seit Oktober 2018 leitet er das Forschungsprojekt Cyberangriffe gegen Unternehmen am KFN.

Dr. Noella Edelmann
promovierte in öffentlicher Verwaltung an der Ragnar Nurkse School, Technische Universität Tallinn, Estland, und ist leitende Wissenschaftlerin an der Abteilung für E-Governance und Verwaltung an der Donau-Universität, Österreich. Ihre Hauptforschungsinteressen sind digitale

Transformation in der öffentlichen Verwaltung, e-Government und e-Partizipation, Open Access und qualitative Forschungsmethoden. Sie ist Redakteurin des OA eJournal for E-Democracy and Open Government (www.jedem.org), Track Chair bei der IFIP EGOV-Konferenz und derzeit an Projekten zur Digitalisierung des Landes Niederösterreich und der Entwicklung von E-Partizipationsrichtlinien für den österreichischen öffentlichen Sektor beteiligt.

Prof. Dr. Götz Fellrath
ist Wirtschaftsingenieur und Ökonom und war 17 Jahre selbstständig in der Beratung für den öffentlichen Sektor tätig. Seit 2018 hat er eine Professur für Verwaltungsmanagement, Organisation, e-Government, Personal und ÖBWL an der Hochschule für Polizei und öffentliche Verwaltung NRW am Studienort Köln.

RD Dr. Torsten Fischer
ist Mathematiker und Betriebswirt und war als Managementberater bei der BAYER Technologie Service GmbH sowie als IT-Referent beim Bundesministerium für Bildung und Forschung tätig. Seine Forschungsschwerpunkte liegen in den Bereichen IT-gestütztes Prozessmanagement und E-Government. Seit 2014 ist er hauptamtlicher Dozent an der Hochschule für Polizei und öffentliche Verwaltung NRW am Studienort Köln und ist verantwortlich für den Studiengang Verwaltungsinformatik.

Prof. Dr. Lorenz Franck
ist Jurist und war u. a. mehrere Jahre für einen Datenschutzverband tätig. Seit 2014 ist er Lehrbeauftragter für Datenschutzrecht an der TH Köln und seit 2019 hat er eine Professur für IT-Recht an der

Hochschule des Bundes für öffentliche Verwaltung in Brühl inne. Er engagiert sich dort insbesondere in den Studiengängen Verwaltungsinformatik (VIT) und Digital Administration & Cyber Security (DACS).

Prof. Dr. Wilfried Honekamp
ist Informatiker und lehrte ab 2010 an der Hochschule Zittau/Görlitz als Professor für Softwaretechnik und Programmierung. Seit November 2014 ist er Professor für Angewandte Informatik am Fachhochschulbereich der Akademie der Polizei Hamburg. Er forscht u. a. zur Cybersicherheit von Schiffen und Hafenanlagen und zu illegalen Marktplätzen im Darknet. Seit 2016 organisiert er die jährliche Tagung Polizei-Informatik.

Mag. Dr. Edith Huber
ist Kriminalsoziologin, Kriminologin und Sicherheitsforscherin. Sie forscht seit rund 15 Jahren zu den Themen Cybercrime, Cyberstalking, Cybersicherheit und Informationssicherheit an der Donau-Universität Krems. Sie kann auf zahlreiche nationale und internationale Forschungsprojekte und Publikationen zurückblicken. Darüber hinaus ist sie an zahlreichen Studiengängen (Strafrecht, Wirtschaftsstrafrecht und Kriminologie, Security and Safety Management u. v. m.) als Dozentin tätig.

Dr. Lutz Martin Keppeler
ist Fachanwalt für Informationstechnologierecht und Partner der Kanzlei Heuking Kühn Lüer Wojtek. Er berät nationale und internationale Mandanten zu allen Fragen des IT- und Datenschutzrechts und ist in diesen Bereichen sowohl außergerichtlich als auch forensisch tätig. Für die öffentliche Hand hat er eine Vielzahl von IT-Vergaben und IT-Infrastrukturprojekte begleitet. Herr Dr. Keppeler

arbeitet besonders intensiv an der Schnittstelle zwischen Technik und Recht, woraus sich Spezialgebiete wie das IT-Sicherheitsrecht, das Open Source Lizenzrecht, das Datenschutzrecht und das Cyber-Versicherungsrecht ergeben. Zu allen genannten Bereichen hält Herr Dr. Keppeler regelmäßig Vorträge und publiziert hierzu. Seit 2018 hält er eine Vorlesung zum Datenschutzrecht an der TH Köln.

Prof. Dr. Dirk Labudde
ist Forensiker und studierter Physiker. Seit 2009 hat er eine Professur für Bioinformatik und seit 2014 ebenso für den von ihm gegründeten ersten Bachelorstudiengang für Allgemeine und Digitale Forensik an der Hochschule Mittweida. Darüber hinaus ist er als Berater für die Polizei und die Staatsanwaltschaft tätig und seit Anfang 2017 Teil des Fraunhofer Instituts für Sicherheit und Informationstechnologie (SIT) sowie seit 2019 Berater und Dozent an der Hochschule Fresenius.

Dipl.- Psychologin Ivona Matas
arbeitet als (Trauma-)Therapeutin, Trainerin und psychologische Sachverständige in eigener Praxis in Köln. Neben der ‚analogen' Sicherheit befasst sie sich seit 2007 mit Themen der digitalen Sicherheit und ist u. a. verantwortlich für die Durchführung von tiefenpsychologischen Security-Wirkungsanalysen, der Begleitung von Kampagnen mithilfe qualitativer Wirkungsforschung und der Entwicklung neuer Sensibilisierungstools. Sie tritt als Rednerin auf Konferenzen auf, führt Präsenztrainings und Sensibilisierungsmaßnahmen durch und schafft Awareness für die menschlichen Aspekte von Cybersecurity.

Prof. Dr. Katrin Möltgen-Sicking
ist seit 2003 Professorin für Politikwissenschaft und Soziologie an der Hochschule für Polizei und öffentliche Verwaltung NRW (HSPV NRW) sowie seit 2006 Lehrbeauftragte für Projektmanagement im MPA-Studiengang der Universität Kassel. Sie ist Mitglied der Forschungsgruppe Politische Partizipation der HSPV NRW. Zuvor war sie als Beraterin für Kommunal- und Landesverwaltungen tätig, u. a. bei der KGSt consult GmbH Kommunalberatung, PricewaterhouseCoopers und der Deutschen Gesellschaft für Mittelstandsberatung mbH.

Bettina Pospisil, MA
Ist Soziologin und war in den letzten sechs Jahren an verschiedenen Universitäten, wie der Wirtschaftsuniversität Wien und der Alpen Adria Universität Klagenfurt, tätig. Seit 2016 arbeitet sie als wissenschaftliche Mitarbeiterin an der Donau-Universität Krems und ist in dieser Position an verschiedenen drittmittel-finanzierten Forschungsprojekten zu den Themen Cybersicherheit und Technikforschung beteiligt.

Dr. Roman Povalej
ist seit Juli 2015 an der Polizeiakademie Niedersachsen als Professor für Informations- und Kommunikationstechnik und Cybercrime tätig. Seit 2004 betreut er Studierende und hält seit 2006 regelmäßig Informatik-Vorlesungen mit starkem Praxisbezug an diversen Hochschulen und Weiterbildungsinstituten. Er engagiert sich in mehreren Gremien und Arbeitsgruppen bei den Polizeien. Sein besonderes Anliegen ist das Voranbringen der Polizei-Informatik. Die jährliche Fachtagungsreihe Polizei-Informatik wurde 2016 als die erste Fachtagung für Lehrende und/oder Forschende in der Informatik an

Hochschulen und Akademien der Polizeien ins Leben gerufen.

Heiko Rittelmeier
ist „gelernter“ Polizeibeamter und erwarb sich nebenberuflich einen Master of Science in Digitaler Forensik. Er ist als Leiter einer Cybercrime-Organisationseinheit im Bereich der Strafverfolgung tätig. Zusätzlich führt er Schulungen für Ermittler und Forensiker für diverse Behörden durch und arbeitet als freiberuflicher Sachverständiger für Digitale Forensik für Unternehmen und Behörden.

Prof. Dr. Susanne Schulte
ist Professorin für Wirtschaftspsychologie, insbesondere für Arbeits-, Personal- und Organisationspsychologie an der Hochschule Fresenius in Düsseldorf und leitet dort den Masterstudiengang Human Resources Management. Seit 2020 ist sie zudem hauptamtlich für die Hochschule für Polizei und öffentliche Verwaltung tätig und unterrichtet dort Personalmanagement sowie Verwaltungsmanagement und Organisation. Zuvor hat sie hier nebenamtlich das Fach Psychologie unterrichtet. Bis 2020 arbeitete sie über 20 Jahre im Personalbereich der Stadtverwaltung Köln, langjährig im dortigen Institut für Personalentwicklung und Eignungsprüfung sowie als Stabsstelle vorwiegend für die Themenbereiche im Arbeitsfeld der Personalauswahl, Personalentwicklung und Ausbildung.

Prof. Dr. Anna Schulze
ist Mathematikerin und Informatikerin und war sechseinhalb Jahre beim Bundesverwaltungsamt als Referentin und Referatsleiterin im Bereich Softwareentwicklung und Projektmanagement tätig. Seit 2015 hat sie eine Professur für Mathematik und Informatik

an der Hochschule des Bundes für öffentliche Verwaltung in Brühl und ist verantwortlich für die Studiengänge Verwaltungsinformatik und „Digital Administration and Cyber Security (DACS)“.

Mag. Heike Strumpen
ist seit 2004 wissenschaftliche Mitarbeiterin an der Donau-Universität Krems mit den Schwerpunkten Programmkoordination und -entwicklung für Information Security, IT in Healthcare und LifeScience und IT Consulting sowie Qualitätsmanagement. Darüber hinaus ist sie Lehrbeauftragte im Masterprogramm „Professional MSc Management und IT“ und hat an zahlreichen Artikeln zum Thema Informationssicherheit mitgearbeitet.

Fabian Weber
hat neben seinem Master-Abschluss in Technischer Informatik auch die Laufbahnausbildung für den gehobenen technischen Dienst der Verwaltungsinformatik in Bayern absolviert. Kommunale Erfahrung sammelte er in der Stadtverwaltung Regensburg im Amt für Informations- und Kommunikationstechnik bevor er in den Bundesdienst zum Bundesamt für Sicherheit in der Informationstechnik wechselte. Dort war er sieben Jahre im Bereich der Zertifizierung von Software-Produkten tätig. Nach einer Abordnung zum Bundesministerium des Innern wechselte er 2018 an die Hochschule des Bundes, wo er in allen Bereichen der Informationstechnik lehrend tätig ist.

Bennet von Skarczinski
ist Betriebswirt und seit 2015 bei der Unternehmensberatung Pricewaterhouse-Coopers (PwC) im Bereich Cyber Security & Privacy tätig. Seit 2017 promoviert er an der Universität Osnabrück am Fachbereich für Wirtschaftsinformatik und

Unternehmensrechnung. Seine Schwerpunkte sind das betriebliche Management von Informationssicherheit und Cyber-Economics.

Prof. Dr. Gina Rosa Wollinger
ist Soziologin und Kriminologin und war sechs Jahre als wissenschaftliche Mitarbeiterin beim Kriminologischen Forschungsinstitut Niedersachsen e.V. tätig, wo sie u. a. zu den Themengebieten Wohnungseinbruch und Cyberkriminalität geforscht hat. Seit 2018 hat sie eine Professur für Soziologie und Kriminologie an der Hochschule für Polizei und öffentliche Verwaltung NRW am Studienort Köln.

Udo Zaudig
baute 1994 die Abteilung Informationssicherheit des Amtes für Informationsverarbeitung der Stadt Köln auf und ist seit 2003 Informationssicherheitsverantwortlicher/CISO der Stadtverwaltung Köln und der Stadtentwässerungsbetriebe Köln AöR. Daneben leitet er die Arbeitskreise der „Informationssicherheitsbeauftragten des KDN“ und der Arbeitsgruppe „Kritische Infrastrukturen im Kölner Raum“.

Vorwort

Prozesse der Digitalisierung in der Gesellschaft sind weder neu noch auf spezifische Kontexte beschränkt. Vielmehr scheinen nahezu alle Bereiche des alltäglichen Lebens, der Öffentlichkeit und nicht zuletzt der Arbeitswelt durch einen digitalen Wandel geprägt zu sein. Neben den vielen Vorteilen, wie beispielsweise erweiterte Partizipationsmöglichkeiten, Effizienz und sozialer Austausch, sind digitale Entwicklungstendenzen jedoch auch mit unerwünschten Dynamiken verbunden. So schaffen das Arbeiten und Leben mit Informationstechnik und Internet auch neue Möglichkeiten zur Begehung von Straftaten. Der Begriff „Cyberkriminalität“ mag dabei einerseits Assoziationen mit großen IT-Rechenzentren oder spezialisierten und erfolgreichen Unternehmen als Opfer und zurückgezogenen Hackern als Täter andererseits hervorrufen. Das Anliegen des vorliegenden Praxishandbuchs ist es, dies zu ändern. Denn die Komplexität der Digitalisierung spiegelt sich in der Vielfältigkeit von Angriffszielen und -arten sowie Opfern und Tätern im Bereich der Cyberkriminalität wider, was die Relevanz des Themas der Cybersecurity auch für die öffentliche Verwaltung begründet. Dabei sind wir als IT-Nutzer alle gefragt, denn die Aufgabe der Herstellung von Cybersecurity kann nicht an eine IT-Abteilung allein übertragen werden, sondern muss, wie des Weiteren zu zeigen sein wird, gesamtbehördlich geleistet werden.

Die Vielschichtigkeit des Phänomens der Cyberkriminalität und der Herstellung von Cybersecurity in der öffentlichen Verwaltung zeigte sich auch in unserer konzeptionellen

Arbeit an dem vorliegenden Praxishandbuch. Denn schnell wurde deutlich, dass es nicht Informatiker allein sind, die hier das Thema allumfassend beleuchten und Hilfestellungen bieten können. Umso mehr freuen wir uns, dass es uns gelungen ist, eine interdisziplinäre Autorenschaft aus den Bereichen der Kriminologie, Mathematik, Informatik, Psychologie, Soziologie, Politikwissenschaft, Verwaltungswissenschaft, Wirtschaftswissenschaft, Rechtswissenschaft und Digitaler Forensik für das Praxishandbuch zu gewinnen. Diese verschiedenen Disziplinen nehmen jedoch nicht nur verschiedene Blickwinkel auf das Phänomen ein, sondern verfolgen teilweise auch ein unterschiedliches Erkenntnisinteresse und bedienen sich verschiedener Fachsprachen. Umso wichtiger zeigte sich der persönliche Austausch im Rahmen eines Autorenworkshops Anfang des Jahres, um einen Konsens in Bezug auf das Problem zu finden, verschiedene Kompetenzen und Sichtweisen abzustecken sowie Berührungspunkte und Überschneidungen zu erkennen. Im Anschluss wurden Beiträge neu ausgerichtet, einige Autoren haben sich intensiver miteinander abgestimmt und weitere thematische Aspekte wurden in den Band mit aufgenommen. Der persönliche Austausch und die Offenheit für andere Disziplinen ermöglichten uns, die Beiträge aufeinander abzustimmen sowie einen roten Faden im Praxishandbuch zu verankern und sichtbar zu machen.

Mit der vorliegenden ersten Ausgabe des Praxishandbuchs „Cybersecurity für die öffentliche Verwaltung“ wollen wir einen Beitrag dazu liefern, die Bedeutung von Cybersecurity, auch über die Mitarbeiter der IT-Abteilung hinaus, verständlich transportieren zu können sowie Handlungsmöglichkeiten für die öffentliche Verwaltung

aufzuzeigen. Damit ist explizit der Anspruch verbunden, Personen mit verschiedenen beruflichen Hintergründen und Positionen innerhalb der Behörde zu erreichen. Darüber hinaus versteht sich das vorliegende Praxishandbuch jedoch ebenso als Einladung, sich auch zukünftig stärker interdisziplinär mit den Themen der Digitalisierung sowie Cyberkriminalität und Cybersecurity auseinanderzusetzen.

Köln, im September 2020

Die Herausgeberinnen

Einführung: Cybersecurity für die öffentliche Verwaltung

Gina Rosa Wollinger, Anna Schulze

Inhaltsübersicht

Einleitung

Die umfangreichen und vielfältigen Nutzungsmöglichkeiten des Internets sind keine neuen Phänomene und dennoch zeigte sich das Potenzial des Digitalen während der Corona-Krise in einer neuen Dimension. Noch nie wurden in Deutschland zu einer Zeit so viele Daten ausgetauscht, meldet der größte deutsche Internet-Knotenpunkt DE-Cix in Frankfurt[1] und Netflix und YouTube reduzierten die Übertragungsraten, um dazu beizutragen, dass das Netz nicht völlig überlastet[2]. Doch neben der Quantität ist ein Blick auf das, was da qualitativ passiert, interessanter, denn plötzlich geht und passiert (fast) alles online: Sportkurse, Unterricht und sogar Feiern mit dem kleinen Club um die Ecke, sozialer Austausch und Netzwerke zur Unterstützung älterer Menschen und auch politische Abstimmungen und Entscheidungen können nun sowohl

national als auch international in Videokonferenzen erfolgen. Die Corona-Krise bedeutete für etliche Personen aber auch viel freie Zeit zuhause. Gegen die Langeweile bot das Netz Live-Konzerte von Musikern in leeren Hallen, Online-Nähkurse, Einblicke in die kreativen und zum Teil auch skurrilen Beschäftigungen anderer Personen im eigenen Zuhause sowie jede Menge so genannter Corona-Songs. Der digitale Raum, oftmals abgegrenzt vom „realen“ Leben, wurde plötzlich zum Marktplatz der Gesellschaft und schuf soziale Nähe. Daneben ermöglichten das Internet, ein breites Softwareangebot und der eigene Computer aber auch, dass viele Menschen ihre Arbeit von Zuhause aus fortsetzen konnten.

Arbeiten außerhalb des Büros stellt selbstverständlich keine Neuerung durch die Corona-Krise dar. Vielmehr handelt es sich um einen, je nach Branche und Arbeitgeber mehr oder weniger, fest etablierten Bestandteil gegenwärtiger Arbeitsformen, welcher einst als Homeoffice bezeichnet wurde, der Möglichkeit, von Zuhause aus zu arbeiten, dann aber von den Begriffen der mobilen Arbeit und Telearbeit abgelöst wurde. Denn Arbeit findet mittlerweile nicht nur zuhause, sondern „überall“ – wie z. B. im Zug, am Flughafen oder im Café – statt. Die Arbeitswelt befindet sich in einem Prozess der Digitalisierung. Jedoch findet diese nicht allein durch die Entkoppelung von Arbeitsort und räumlicher Arbeitsstelle statt, sondern auch durch die Digitalisierung vieler Arbeitsabläufe, der Speicherung und Nutzung von Informationen, also Daten, und der Kommunikation. Kommunikationsverhältnisse haben sich in den letzten Jahrzehnten dadurch in einer noch die da gewesenen Geschwindigkeit elementar gewandelt.

Zum Präfix „Cyber“

Letztendlich ist diese sich digitalisierende Arbeitswelt jedoch auch mit Gefahren und Risiken verbunden, vor welcher eine neue Form von Sicherheit schützen soll: Informationssicherheit oder auch Cybersecurity genannt. Diese neue Säule in der komplexen Sicherheitsarchitektur moderner Gesellschaften führte auch zum Titel des vorliegenden Praxishandbuchs: „Cybersecurity für die öffentliche Verwaltung“. Noch ein Buch also mit dem Präfix „Cyber“, welchem *Thomas Rid* „unverwüstliche Attraktivität“ (2016, S. 423) bescheinigt. Dabei korrespondiert die wahrgenommene Allgegenwärtigkeit von „Cyber“, man denke nur an Begriffe wie Cyberspace, Cybermobbing, Cybersex, Cyberkrieg, jedoch nicht mit einem einheitlichen Begriffsverständnis oder gar Kenntnis dessen, was „Cyber“ eigentlich bedeutet. Vielmehr dürfte es den meisten Nutzern der genannten Worte sogar schwer fallen, genau zu benennen, was „Cyber“ darin eigentlich meint.

Was heißt „Cyber“? *Thomas Rid* (2016) hat diese Frage, mit der er wiederholt von seinen Studierenden konfrontiert wurde, zu dem Verfassen einer fünfhundertseitigen, sehr empfehlenswerten Abhandlung der Geschichte der Kybernetik, veranlasst. Die Historie der Kybernetik, d. h. einer Theorie der Maschine, kreist um die Fragen nach technischer Steuerung, Kommunikation und Automatisierung. Allerdings geht es dabei „nicht um Mechanik, sondern um Verhalten“ (*Rid,* 2016, S. 87). Die Mathematikerin Alice Mary Hilton beschrieb diese Differenzen in Form von zwei Revolutionen (siehe *Rid,* 2016, S. 133 f.): Während die landwirtschaftliche Revolutionen in Form von Werkzeugen die körperlichen Fähigkeiten der Menschen auf Geräte übertrug und perfektionierte bzw. erweiterte, sieht sie die zweite in der Erweiterung der geistigen Fähigkeiten in Form einer

„Automatisierung der Industrieproduktion“ (ebd.). Die Kybernetik versucht in dem Sinn nicht die Körperkraft, sondern die geistige Kraft des Menschen nachzubilden bzw. zu erweitern und zu verbessern. So wie ein mechanisches Gerät nicht ermüdet und Verschleißerscheinungen größtenteils leichter und einfach behoben werden können als beim menschlichen Körper, so schafft die Kybernetik eine Ausführung geistiger Tätigkeiten wie das Ausführen von Rechenoperationen und das Erinnern bzw. Speichern von Informationen und Daten, nur besser, schneller, komplexer, ohne Flüchtigkeitsfehler und Phänomene wie das des Vergessens und der Ermüdung. Zwei zentrale Revolutionen quasi, in der der Mensch sich selbst, oder man könnte auch sagen, seine Kernkompetenzen neu erschafft in einer überarbeiteten und perfektionierten Version seiner selbst.

Dabei kommt dem Verständnis der geistigen Abläufe des Menschen zentrale Bedeutung zu: *„Das Gehirn ist keine denkende Maschine, es ist eine handelnde Maschine“* wird *Ross Ashby*, der die Idee der Kybernetik mit vorantrieb 1948 zitiert (in *Rid,* 2016, S. 87). Und weiter: *„Es erhält Informationen und unternimmt dann etwas aufgrund dieser Informationen“* (ebd.). Das Gehirn also als geistiger automatisierter Prozess auf Grundlage äußerer Reize und Eindrücke. Nicht die Vorstellung einer von freiem Willen, Spontanität und Kreativität geprägter, *denkender* Entität ist die Grundlage – ein solches Nachzubilden dürfte auch mit enormen Herausforderungen verbunden sein. Den Bezugspunkt bildet vielmehr das Verständnis von einem Gehirn, welches in einer Art und Weise programmiert ist, das automatisierte Prozesse ausführt, je nach Input. Dies bildet die zentrale Idee der Kybernetik: Anders als eine mechanische Maschine, die eine „Bewegung“ ausführt in der Art und Weise, wie sie gebaut ist, reagiert die

kybernetische Maschine auf Informationen aus dem jeweiligen außen und *verhält sich* dementsprechend zu seiner Umwelt. Dabei verlaufen Entscheidungsprozesse in dem Sinn, dass in Situation A anders entschieden und reagiert wird als in Situation B, wobei die kybernetische Maschine erkennen können, welche Situation vorliegt und „auf Veränderungen in seiner Umwelt reagieren“ (*Rid,* 2016, S. 81) muss. Die Grenze zwischen System und Umwelt wird hierbei fraglich, sind doch beide miteinander quasi im Austausch bzw. beziehen sich aufeinander.[3] Im weiteren Sinn beflügelte diese Vorstellung auch Autoren der Belletristik, insofern eine Vielzahl von Werken aufkam, in denen die Verschmelzung von Mensch und Maschine, z. B. in Form von so genannten Cyborgs, das zentrale Narrativ bildet und Science Fiction- und Cyberpunk-Genres prägten (*Rid*, 2016, S. 7 f.; 197 ff.).

Geprägt wurde der Begriff Kybernetik ferner auch von *Norbert Wiener* und seinem Buch „Kybernetik. Regelung und Nachrichtenübertragung im Lebewesen und in der Maschine“ von 1948 (*Rid*, 2016, S. 19). *Wiener* beschäftigte sich im Zusammenhang mit dem Zweiten Weltkrieg mit der Frage, wie der Luftraum kontrolliert werden kann bzw. wie die Luftangriffe der Deutschen abgewehrt werden können (*Rid*, 2016, S. 25-64). Dazu brauchte es Möglichkeiten, Flug- und Abwurfbahnen zu berechnen. Nach intensiver, durch die USA finanzierter wissenschaftlicher Forschung, zu der auch Ingenieure maßgeblich beitrugen, wurde u. a. das Radar entwickelt.

Das Präfix „Cyber“ ist entlehnt aus dem englischen Wort *cybernetics*, auf Deutsch Kybernetik. Kybernetik wiederum stammt von dem griechischem Verb *kyvernó*, was „steuern, lotsen oder herrschen“ (*Rid*, 2016, S. 19) bedeutet, wobei *Thiedeke* auf das griechische Wort *kybernetike* verweist,

was er als „Kunst des Steuermanns“ übersetzt (2004a, S. 124). Der semantische Bezug zum Steuern und zu Kontrolle ist in mehrfacher Hinsicht interessant. Zum einen beschreibt er das, was kybernetische Maschinen vollziehen sollen, nämlich etwas automatisch steuern, etwas kontrollieren. Zum anderen wird jedoch in der öffentlichen Debatte über informationstechnische Systeme oftmals auch die Gefahr des eigenen oder menschlichen Kontrollverlusts im Zusammenhang mit informationstechnischen Systemen oder der so genannten künstlichen Intelligenz diskutiert. Verbunden damit sind Ängste, die Eigenständigkeit von quasi selbst denkenden Maschinen könnte zu der Übernahme der Macht und der Beherrschung der Menschen führen, welche sich auch wiederum in gegenwärtigen Erzählungen und Filmen wiederfindet.[4] Oder, etwas weniger radikal formuliert, aber in seinen Auswirkungen nicht schwächer, die Befürchtung einer totalen Verlagerung des („realen“) Lebens ins Digitale. Das ist im Übrigen nicht eingetreten. Dafür, „dass die Gesellschaft selbst zum Cyberspace wird, gibt es keine Anhaltspunkte“ (*Thiedeke*, 2004b, S. 22). Persönlicher Austausch von Angesicht zu Angesicht findet weiter statt, selbst während der Corona-Krise mussten vielerorts Personen durch das Verhängen von Bußgeldern dazu gebracht werden, sich nicht zu treffen, Menschen reisen, sogar mehr denn je, Regierungschefs begegnen sich bei politischen Gipfeltreffen, Massenansammlungen, -veranstaltungen und -proteste geschehen analog. Hinzufügen könnte man ein „auch“, denn die genannten Austauschprozesse passieren auch digital. Insofern stellt der *Cyberspace* vielmehr eine Erweiterung der Kommunikationsmöglichkeiten und -formen (ebd.) als deren Ersatz oder gar vollständige Auflösung dar. Neben den genannten Befürchtungen sind ebenso viele der

überhöhten Hoffnungen, die mit dem Cyberraum verbunden waren, nicht eingetreten. Die Welt ist nicht zu einem globalen Dorf mutiert, Partizipation und politische Bewegungen werden teilweise durch das Internet unterstützt und mancherorts sicherlich auch überhaupt erst ermöglicht, dennoch kann keine Rede von der Auflösung von etablierten Machtasymmetrien und Verteilungsstrukturen sein.

Und dennoch ergibt sich bezüglich der Frage der Macht der dritte Anknüpfungspunkt an den begrifflichen Bezug zur Kontrolle, denn der Cyberspace ist ein Raum, der von denen kontrolliert wird, die *„seine technische Bedingungen kennen, die verstehen, es zu bedienen“* (*Thiedeke,* 2004a, S. 125). Sicherlich ist es angesichts der Wirkmacht von Facebook, Amazon und Co. nicht ganz unumstritten, wenn *Udo Thiedeke* ausführt, dass durch den Cyberraum Kontrolle *„nicht mehr in den großen institutionalisierten Medienorganisationen der Funkhäuser, Verlage und Sendeanstalten konzentriert sind“* (ebd.). Aber die Kontrolle ist eben nicht nur bei den großen Konzernen, sondern auch bei all denen, die über Wissen verfügen, den Cyberraum für sich zu nutzen. Kennzeichnend dabei ist, dass nicht allein die Hersteller und Anbieter der Maschinen, Webseiten, E-Mail-Programme, digitalen Verwaltungssystemen und dergleichen über diese verfügen können: *„Heute aber können die Maschinen zu Fall gebracht werden. Die Artefakte können gehackt werden. Die Kontrolle kann den Maschinen und natürlich auch den Menschen, die Maschinen als Werkzeuge gebrauchen, entrissen werden“* (*Rid,* 2016, S. 413). Mit anderen Worten, die Datenabläufe und -speicherungen, digitale Kommunikation und Verwaltung kann manipuliert, ausspioniert, zerstört und für vielfältige, schädigende

Zwecke genutzt werden. Der Cyberraum ermöglicht auch die Cyberkriminalität.

Cyberkriminalität

Cyberkriminalität ist ein vielfältiger, nicht klar umgrenzter Deliktsbereich. Hierzu gehören sowohl Taten, bei denen das Internet oder informationstechnische Systeme nur das Tatmittel sind, wie beispielsweise Cybermobbing, Cyberstalking oder Warenbetrug bei Online-Händlern, als auch solche Fälle, bei denen die Hard- oder Software, informationstechnische Systeme, Webseiten usw. selbst manipuliert oder zerstört wurden. Die Bedrohungsformen und Angriffsarten sind demnach sehr vielfältig und unterschiedlich, aber sie sind nicht wirklich neu. Die Grundarten von strafbaren Handlungen, die hinter Delikten aus dem Bereich Cyberkriminalität liegen, sind keine neue Erscheinung, die erst mit technischer Veränderung ermöglicht wurden. Es handelt sich dabei um Diebstahls-, Betrugs- und zum Teil sogar Körperverletzungsdelikte sowie Vandalismus. Dies sind bekannte Straftaten, die wohl in jeder Gesellschaft und zu jeder Zeit, wenn auch in unterschiedlichem Ausmaß, passieren. Und hinsichtlich der Eigentumsdelikte sind sie auch der größte Anteil dessen, was die polizeilich registrierten Straftaten in Deutschland ausmacht (*Bundeskriminalamt*, 2020). Die Taten, die zum Kontext Cyberkriminalität zu fassen sind, sind keine neuartigen Erscheinungen; die Objekte, auf die sich die Taten beziehen bzw. die Tatmittel, stellen die wesentlichen Neuerungen dar.

Hieraus können zwei Schlussfolgerungen getroffen werden. Wenn davon ausgegangen wird, dass die Taten an sich nicht neu sind, bedeutet dies, dass die Motivation, solche Straftaten zu begehen, es auch nicht ist. Täter[5] aus dem

Bereich Cyberkriminalität sind demnach keine Personen, die sich durch sehr spezifische Motive oder Bezüge zur IT stark von anderen Personen, die straffällig auffallen, unterscheiden. Mit Blick auf den oben erwähnten großen Anteil der Straftaten aus dem Bereich der Eigentumsdelikte ist ferner davon auszugehen, dass es viele potenzielle Täter der Cyberkriminalität geben dürfte bzw. in Zukunft auch eine stärkere Verlagerung von vormals „analogen Straftaten“ in den digitalen Raum geben wird. Diese Überlegung wird durch die Tatsache bestärkt, dass zur Ausführung von Straftaten im bzw. mittels des Internets oder informationstechnischer Systeme nicht notwendigerweise auch IT-Kenntnisse vorliegen müssen. Das Internet ermöglicht es dabei, Straftaten bzw. das Ausführen zu kaufen, was auch, dem Dienstleistungsgedanken aufnehmend, *crimeas-a-service* genannt wird.

Zum anderen ist jedoch nicht nur von einer großen Anzahl (potenzieller) Täter auszugehen, sondern auch von vielen (potenziellen) Opfern. Wenn es Tätern aus dem Bereich Cyberkriminalität nicht ausschließlich um sehr spezielle Interessen geht, sondern auch um Schädigungen der Schädigungen willen und das Erlangen von Geld bzw. von Informationen, aus denen mittelbar Geld gewonnen werden kann, ist die Anzahl der (möglichen) Betroffenen hoch. Ferner richten sich viele Angriffe auch nicht an eine bestimmte Person, sondern werden beispielsweise über Mails massenhaft verbreitet, unabhängig davon, ob der Empfänger ein aus Tätersicht vielversprechendes Opfer ist oder nicht. Es kann demnach sogar berechtigterweise die Frage aufgeworfen werden, wer eigentlich nicht betroffen sein kann. Selbst kleine Handwerksbetriebe speichern ihre Kundendaten auf einem Computer und erstellen hiermit Rechnungen. Ebenso kann auch eine normale Arztpraxis in

ihrer Existenz bedroht sein, wenn plötzlich alle Patientendaten verschlüsselt sind und nur durch die Zahlung eines Lösegelds (eventuell) wiedererlangt werden können. Um von einem Cyberangriff betroffen zu werden, ist es keine Voraussetzung, über besonders wertvolle Informationen und Daten zu verfügen, sondern schlichtweg nur eines: einen Computer zu besitzen.

So wurden bislang nicht nur Privatnutzer Opfer von Straftaten aus dem Bereich der Cyberkriminalität (*Bundeskriminalamt,* 2019), sondern auch Unternehmen (*Dreißigacker et al.,* 2020). Ebenso erlebten auch schon etliche kommunale Verwaltungsbehörden Cyberangriffe mit zum Teil starken Auswirkungen auf die Aufrechterhaltung der behördlichen Arbeit.

> *Beispiel: Ein Mitarbeiter der Stadtverwaltung Frankfurt am Main bekam im Dezember 2019 eine E-Mail, die den Anschein machte, von einer anderen städtischen Behörde zu kommen.*[6] *Tatsächlich war dies nur eine Tarnung, um die Schadsoftware Emotet zu verbreiten. Als Sicherheitsmaßnahme ging die Stadtverwaltung für 24 Stunden offline, wodurch zahlreiche Dienstleistungen für die Bürger bis hin zur Ausleihe bei der Stadtbibliothek nicht mehr erreichbar waren. Anders erging es der Universität Gießen: Diese musste aufgrund eines Hacker-Angriffs für zwei Wochen in den Offline-Modus gehen.*[7]

Dies kann auch personelle Konsequenzen nach sich ziehen, wie folgendes Beispiel des Kammergerichts Berlin verdeutlicht.

> *Beispiel: Auch das Kammergericht Berlin wurde im September 2019 Opfer des Computervirus Emotet, welcher sich auf den Rechnern verbreitete.*[8] *Die*

Angreifer hatten damit vollen Zugriff auf alle Daten. Die zögerliche Reaktion auf den Angriff sowie mangelnde Sicherheitsstandards führten letztendlich u. a. dazu, dass der Verantwortliche der Informationstechnik entlassen wurde.[9]

Cyberangriffe auf die öffentliche Verwaltung sind nicht nur eine Unannehmlichkeit, bei welcher der Bürger gegebenenfalls ein wenig länger warten muss, bis sein Anliegen bearbeitet wird. Die Verwaltung verfügt einerseits über hochsensible Daten der Bürger. Andererseits sind das Funktionieren der Verwaltung sowie das Vertrauen des Bürgers darin ein elementarer Bestandteil des Rechtsstaates. Die Bedeutung von Cybersecurity für die öffentliche Verwaltung ist demnach immens, insbesondere in Anbetracht dessen, dass die Digitalisierung in diesem Bereich noch längst nicht abgeschlossen ist und spätestens durch das Onlinezugangsgesetz noch einmal eine neue Dynamik erfahren wird. Der Schutz der öffentlichen Verwaltung vor Cyberangriffen stellt demnach einen zentralen Schutz des Staates und der Gesellschaft dar.

Ziel und Zielgruppe des Praxishandbuchs

Das vorliegende Praxishandbuch will dabei einen Beitrag zur Cybersecurity der öffentlichen Verwaltung in Deutschland geben. Es richtet sich dabei vorwiegend an Mitarbeiter in Leitungspositionen von Behörden, die das Phänomen der Cyberkriminalität verstehen und die Bedrohungslage in Bezug zur behördlichen IT-Struktur einschätzen wollen, um in einem darauf folgenden Schritt die eigene Sicherheitsarchitektur zu überprüfen bzw. die angemessenen Schritte für eine Erhöhung der Cybersecurity einleiten zu können. Sicherlich kann nicht mittels des vorliegenden Praxishandbuchs eins zu eins die

eigene Informationssicherheit hergestellt oder verbessert werden, insofern es sich nicht um einen Umsetzungsplan handelt, den man wie eine Checkliste abarbeiten kann, handelt. Aufgrund der vielfältigen Konstellationen und Unterschiede im Bereich von behördlicher Arbeit und Aufgaben bzw. von Kommunen ist es wohl auch mehr als fraglich, ob hierzu überhaupt ein Buch im Sinne einer Anleitung geschrieben werden kann. Dennoch erhebt das Praxishandbuch den Anspruch, zu Handlungskompetenz zu verhelfen. Um ein IT-Sicherheitskonzept in der eigenen Behörde umzusetzen, bedarf es jedoch zunächst Wissen darüber, welche Gefahren es abzuwehren gilt, welche (auch zukünftigen) Herausforderungen mit einer sich digitalisierenden Kommune verbunden sind, welche Anforderungen, insbesondere rechtlicher Art, an die Behörde gestellt werden und welche Rolle dabei auch die eigenen Mitarbeiter spielen. Erst auf der Grundlage dieses Wissens, bestehend aus Grundlagenwissen und Best-Practice-Beispielen, können die eigenen „Baustellen“ erkannt und weitere Maßnahmen sinnvoll angegangen werden.

Daneben richtet sich das Praxishandbuch aber auch allgemein an Mitarbeiter von kommunalen Behörden, denn wie in mehreren Kapiteln dieses Buchs deutlich wird, ist es für die Cybersecurity unerlässlich, dass jeder Anwender einer Behörde über ein Verständnis von Cyberkriminalität verfügt und ihm die Gefahren im Berufsalltag bewusst sind. Letztendlich richtet sich das Praxishandbuch aber auch an all jene, die sich für Cyberkriminalität und Möglichkeiten seiner Verhinderung mit Bezug zu institutionellen Strukturen, wie sie in Form von Behörden und Unternehmen gegeben sind, interessieren. Es richtet sich explizit nicht an IT-Experten, wobei sicherlich auch der eine oder andere interessante Aspekt für Mitarbeiter von IT-

Abteilungen vorzufinden ist. Vorwiegend soll es jedoch gerade durch die Vermeidung der Verwendung einer IT-Fachsprache das weitläufige Phänomen der Cyberkriminalität und die Möglichkeiten von Sicherheit in dem Bereich einer breiten interessierten Leserschaft zugänglich machen. Denn die Herausforderung im Umgang mit Cyberkriminalität wird nicht allein durch IT-Experten gelöst werden, vielmehr geht sie uns alle an.

Aufbau des Praxishandbuchs

Dem skizzierten Ziel und der anvisierten inhaltlichen Ausrichtung folgt der Aufbau des Praxishandbuchs. Dieses gliedert sich in vier Teile: Phänomen Cyberkriminalität, Digitalisierung und Kommunen, Informationssicherheit für Kommunen und abschließend ein Ausblick auf Innovationen zur Begegnung von Cyberangriffen.

Im ersten Teil **„Phänomen Cyberkriminalität“** wird Grundlagen- und Hintergrundwissen zu Cyberkriminalität vermittelt. Dabei geht es um das Phänomen als solches, was es ist, wie verbreitet es in Deutschland ist und wer die zentralen Akteure in diesem Zusammenhang sind. Hierzu erläutern *Gina Rosa Wollinger, Arne Dreißigacker* und *Bennet von Skarczinski* in Kapitel 1 grundlegende Begriffe aus den Bereichen Sicherheit und Cyber. Dabei werden verschiedene Bedrohungsformen beschrieben und beispielhaft dargestellt. In Kapitel 2 führen *Edith Huber, Noella Edelmann, Bettina Pospisil* und *Heike Strumpen* aus, was über die Täter im Bereich Cyberkriminalität bekannt ist und zu welchen Ergebnissen sie in ihrer Forschung gekommen sind. In Kapitel 3 beschreiben *Arne Dreißigacker* und *Gina Rosa Wollinger* das Ausmaß von Cyberangriffen in Deutschland. Welche Rolle im Zusammenhang mit Cyberkriminalität die Polizei spielt, wie