Rechtliche Implikationen von Cybersicherheitsvorfällen in der kommunalen Verwaltung

Linda Schreiber[1]

Abstract: Einrichtungen der kommunalen Verwaltung sind zunehmend von IT-Sicherheitsvorfällen betroffen, mit zum Teil weitreichenden Auswirkungen. Diese Vorfälle können sich auf die Verfügbarkeit von IT-Systemen und damit wichtiger kommunaler Leistungen im Bereich der Daseinsvorsorge auswirken sowie auf die Vertraulichkeit und Integrität von Daten und Systemen der kommunalen Verwaltung. Der Beitrag skizziert Beispiele von Cybersicherheitsvorfällen im kommunalen Bereich sowie Anknüpfungspunkte für rechtliche Implikationen und identifiziert weitere Forschungsfragen.

Keywords: Cybersicherheit, öffentliche Verwaltung, Datenschutz, Regulierung, Geheimschutz, Kommunen, Verfassungsrecht

1 Die Rolle kommunaler Einrichtungen

Kommunale Einrichtungen nehmen eine Vielzahl öffentlicher Aufgaben wahr, also Aufgaben „an deren Erfüllung ein gesteigertes Interesse der Gemeinschaft besteht“ [Bu74]. Im Rahmen der kommunalen Selbstverwaltung regeln Kommunen alle Angelegenheiten ihrer örtlichen Gemeinschaft in eigener Verantwortung (Art. 28 Abs. 2 GG). Neben den Aufgaben der kommunalen Daseinsvorsorge erfüllen Kommunen ihnen durch Gesetze übertragene Aufgaben, wie beispielsweise bei der Durchführung von Bundestagswahlen (§9 BWahlG), im Bereich der Sozialhilfe (§ 6 SGB II) oder des Baurechts (§ 1 BauGB). Für BürgerInnen, ansässige Unternehmen und den Staat besteht demnach vielfach eine besondere Abhängigkeit von der Erbringung der Aufgaben und Verfügbarkeit der Dienstleistungen der kommunalen Verwaltung. Besorgniserregend ist vor diesem Hintergrund, dass sich Berichte von Cybersicherheitsvorfällen in kommunalen Einrichtungen häufen.

Der Beitrag zeigt Beispiele für verschiedene Arten von Cybersicherheitsvorfällen in kommunalen Einrichtungen sowie deren Auswirkungen. Zudem werden rechtliche Rahmenbedingungen, die im kommunalen Bereich für die Prävention von und den

[1] Fraunhofer-Institut für Sichere Informationstechnologie SIT | Nationales Forschungszentrum für angewandte Cybersicherheit ATHENE, Rheinstr. 75, 64295 Darmstadt, Deutschland, linda.schreiber@sit.fraunhofer.de.
Diese Forschungsarbeit wurde vom Bundesministerium für Bildung und Forschung (BMBF) und vom Hessischen Ministerium für Wissenschaft und Kunst (HMWK) im Rahmen ihrer gemeinsamen Förderung für das Nationale Forschungszentrum für angewandte Cybersicherheit ATHENE unterstützt.

doi:10.18420/inf2022_22

Umgang mit Cybersicherheitsvorfällen anwendbar sind, skizziert, wobei ein weiterer Forschungsbedarf identifiziert wird.

2 Cybersicherheitsvorfälle in der kommunalen Verwaltung

2.1 Definition Cybersicherheitsvorfälle und Schutzziele

Der Begriff der Cybersicherheit und der damit verbundene Schutz von Informationen und Systemen bestimmt sich über die Bewahrung beziehungsweise die Einhaltung der Schutzziele der Vertraulichkeit, Integrität und Verfügbarkeit von Informationen. Dementsprechend sind *Cybersicherheitsvorfälle* ungewollte oder unerwartete Ereignisse, wie Angriffe oder unautorisierte Zugriffe, die nachteilige Auswirkungen haben, in dem sie eines oder mehrere ebendieser Schutzziele beeinträchtigen (Art. 4 Nr. 2 und 7 NIS Richtline). Die *Vertraulichkeit* von Informationen und Systemen bedeutet, dass nur ein jeweils definierter Kreis an befugten Personen Zugriff auf diese haben bzw. Informationen nur gegenüber diesen offengelegt werden. Die *Verfügbarkeit* von Informationen und IT-Systemen bezieht sich auf deren Eigenschaft, dass sie wie vorgesehen zugänglich und nutzbar bzw. betriebsbereit sind. *Integrität* bezieht sich auf die Korrektheit und Unverfälschtheit von Daten bzw. die korrekte Funktionsweise von IT-Systemen, also den Schutz vor einer unbefugten Manipulation. Daneben gibt es noch eine Reihe weiterer, untergeordneter Schutzziele bzw. Spezialfälle der Dreien, wie die *Authentizität*, *Unverkettbarkeit*, oder *Nachweisbarkeit* [BA10]. Viele Cybersicherheitsvorfälle sind gezielte Angriffe, also eine vorsätzliche Gefährdung der Cybersicherheit durch einen Angreifer mit dem Ziel, sich oder einem anderen Vorteile zu verschaffen [BS22].

2.2 Beispiele zu Cybersicherheitsvorfällen auf kommunaler Ebene

In Einrichtungen der kommunalen Verwaltung haben sich in den vergangenen Jahren zahlreiche Cybersicherheitsvorfälle unterschiedlichen Ausmaßes ereignet. Im Folgenden wird anhand einer Auswahl von Beispielen aus der Praxis die Bandbreite an Cybersicherheitsvorfällen und Beeinträchtigungen der jeweiligen Schutzziele aufgezeigt sowie die praktischen Auswirkungen.

Ransomware Angriffe

Eine häufige Form von Schadsoftware, die von Angreifern bei einer Vielzahl von Cybersicherheitsvorfällen im öffentlichen Bereich verwendet wird, ist Ransomware. Bei Ransomwareangriffen werden Daten und Systeme von Anwendern verschlüsselt und somit der Zugriff verhindert. Angreifer fordern die Zahlung eines Lösegelds, damit die Daten wieder entschlüsselt werden. Betroffen sind bei Kommunen häufig in umfassender Weise verschiedene Ämter, Bereiche und Standorte. Insbesondere wenn Backups der Systeme nicht vorhanden sind, ebenfalls verschlüsselt wurden, veraltet oder in Folge des

Angriffs nicht mehr vertrauenswürdig sind, kann die Wiederherstellung bis zu mehreren Monaten dauern [SK20] [BS22]. Ransomware richtet sich in erster Linie gegen das Schutzziel der Verfügbarkeit. Die Nicht-Verfügbarkeit von Daten und IT-Anwendungen auf technischer Ebene führt dazu, dass viele öffentliche Aufgaben und Dienste, die darauf basieren, nicht erbracht werden können. Dies führt beispielsweise dazu, dass allgemein die Kommunikation mit den verschiedenen Bereichen der öffentlichen Verwaltung eingeschränkt ist, aber auch dazu, dass beispielsweise Sozialhilfe- oder Unterhaltszahlungen nicht erfolgen, neue Kraftfahrzeuge nicht zugelassen oder Personalausweise und Pässe nicht ausgestellt werden [St21] [Sc21].

Neben der Verfügbarkeit kann es auch zu Beeinträchtigungen des Schutzziels der Vertraulichkeit kommen, wenn es während des Angriffs gleichzeitig zum Abfluss von Daten kommt. So gibt es Fälle, bei denen personenbezogene Daten von BürgerInnen, VerwaltungsmitarbeiterInnen und Abgeordneten nach einem Ransomware-Angriff im Darknet veröffentlicht wurden [He21] [St21].

Distributed Denial of Service

„Denial of Service“ (DoS) Angriffe sind Angriffe, die zu einer gezielten Überlastung von Diensten, Systemen oder Webseiten führen und sich somit gegen das Schutzziel der Verfügbarkeit richten. Dies geschieht häufig in der Form von verteilten “Distributed Denial of Service” (DDoS) Angriffen, bei denen der Angriff durch Anfragen von vielen Rechnern gleichzeitig erfolgt. Häufig haben Angreifer hierfür zuvor die Kontrolle über eine Vielzahl an Rechnern im Netz mittels Schadsoftware übernommen und damit ein sog. Botnetz erstellt, womit ein entsprechender Angriff durchgeführt wird [GW21] [SK20]. Im öffentlichen Bereich konnte man diese Angriffsart zuletzt insbesondere gegen Schul- und Lernplattformen beobachten, aber bspw. auch gegen ein Portal zur Vergabe von Impfterminen [Sä20] [Sp21] [BS21]. DDoS-Angriffe führen dazu, dass betroffene Systeme und Dienste zeitweise nicht oder nur eingeschränkt für die Nutzenden erreichbar sind.

Phishing

Phishing ist eine Form des Social Engineerings und beschreibt eine Methode, bei der mittels gefälschter bzw. manipulierter E-Mails oder Webseiten, in denen sich der Angreifer als vertrauensvolle, bekannte Quelle ausgibt, Nutzer zu einer bestimmten Handlung verleitet werden. Dies kann etwa die Eingabe von Daten und Passwörtern sein, oder das Öffnen eines Anhangs, was zur unbemerkten Ausführung eines Schadprogramms führt [We22] [BS22]. Bei Phishing-Vorfällen, die öffentliche Stellen involvieren, sind diese nicht immer das Opfer: In Nordrhein-Westfalen haben Betrüger das Portal für Corona-Nothilfen des Wirtschaftsministeriums kopiert und darüber Daten von Selbstständigen und Kleinunternehmen erlangt, womit sie wiederum die Nothilfen selbst beantragt haben [Ko20]. Phishing-Angriffe, die sich gegen öffentliche Einrichtungen selbst richten, können unterschiedlichste Auswirkungen haben. Sie können als Angriffsvektor zur Ausführung von Malware genutzt werden und damit beispielsweise zu oben genannten Ransomware-Angriffen führen [SN21].

Technische Schwachstellen

Neben gezielten Cyberangriffen kommt es auch zu Cybersicherheitsvorfällen, die nicht durch Angreifer vorsätzlich initiiert wurden, sondern durch technisch bedingte Schwachstellen, die durch Angreifer ausgenutzt werden können. Technische Schwachstellen sind sicherheitsrelevante Fehler in IT-Systemen, die das jeweilige System bzw. die einsetzende Einrichtung anfällig für Bedrohungen und Cyberangriffe machen [BS22]. In diesem Zusammenhang wird auch der Begriff der Sicherheitslücke für die Eigenschaft von IT-Systemen verwendet, bei denen es durch Ausnutzung möglich ist, dass sich Dritte gegen den Willen des Berechtigten Zugang zum jeweiligen System verschaffen oder die Funktion des jeweiligen Systems beeinflussen können (§ 2 Abs. 6 BSIG). Sicherheitslücken wurden im öffentlichen Bereich bspw. in einer App für Rettungskräfte sowie in Software zur Wahlauswertung entdeckt. Hierbei verletzten die Sicherheitslücken das Schutzziel der Vertraulichkeit, durch die Möglichkeit der Einsichtnahme von Patienten- und Einsatzdaten, bzw. das Schutzziel der Integrität, durch die Möglichkeit der Manipulation von Wahlergebnissen [Do18] [Go20].

3 Rechtliche Implikationen

Es zeigt sich, dass die Auswirkungen von Cybersicherheitsvorfällen in kommunalen Einrichtungen unterschiedlichster Art und Tragweite sein können. Bestehende Handreichungen, wie beispielsweise das „IT-Grundschutz-Profil Basis-Absicherung Kommunalverwaltung“ [DD22] und die „Handreichung zur Ausgestaltung der Informationssicherheitsleitlinie in Kommunalverwaltungen“ [Ko17] bieten für das spezifische Umfeld von Kommunen praktische Hilfestellung zur Implementierung technischer und organisatorischer Maßnahmen sowie der Errichtung eines Informationssicherheits-Managementsystems. Allerdings fehlt es bislang an einer umfassenden systematischen Analyse der rechtlichen Rahmenbedingungen, die im kommunalen Bereich für die Prävention von und den Umgang mit Cybersicherheitsvorfällen anwendbar sind und welcher cybersicherheitsrechtliche Handlungsbedarf sich aus diesen ergibt. Mögliche Anknüpfungspunkte für künftige Forschung sind die folgenden Bereiche:

Datenschutzrecht

In vielen Fällen führen Cybersicherheitsvorfälle zu Datenschutzverletzungen (Art. 4 Nr. 12 DSGVO). Durch die verschiedenen Einrichtungen der kommunalen Verwaltung werden vielfach personenbezogene Daten in einem besonderen Umfang, Detailgrad, Bandbreite und Schutzbedarf verarbeitet.

Zudem gelten im kommunalen Bereich zum Teil bereichsspezifische datenschutzrechtliche Regelungen, wie beispielsweise zum Steuergeheimnis für Amtsträger in Finanzbehörden (§ 30 AO) oder dem Sozialgeheimnis für Sozialleistungsträger (§ 35 SGB I, § 67 SGB X).

Hier gilt es beispielsweise spezifische Kriterien für die bei Datenschutzverletzungen durchzuführende Risikobewertung zu analysieren [Ar18] [Eu21]. Für die Feststellung der Betroffenheit von Personen sowie der Bewertung des sich für diese jeweils aus der Datenschutzverletzung ergebenden Risikos wird in diesen Fällen oftmals ein kontinuierliches Monitoring über längere Zeiträume notwendig sein. Dies ist insbesondere bei komplexen, unübersichtlichen Cybersicherheitsvorfällen wie Ransomwareangriffen der Fall, wenn zum Beispiel nicht klar ist, ob und welche Daten während eines Angriffs abgeflossen sind und wozu die Angreifer diese verwenden.

Geheimschutz

Zudem ergibt sich ein besonderer Schutzbedarf für Verschlusssachen nachdem Sicherheitsüberprüfungsgesetz (SÜG) sowie den entsprechenden landesrechtlichen Regelungen. Verschlusssachen sind im öffentlichen Interesse, insbesondere zum Schutz des Wohles des Bundes oder eines Landes, geheimhaltungsbedürftigen Tatsachen, Gegenstände oder Erkenntnisse (§ 4 Abs. 1 S. 1 SÜG). Verschlusssachen werden entsprechend ihrer Schutzbedürftigkeit, also dem Schaden den eine unbefugte Kenntnisnahme erzeugen kann, eingestuft (§ 4 Abs. 2 SÜG).

Onlinezugangsgesetz

Durch das Onlinezugangsgesetz (OZG) werden Bund, Länder und Kommunen dazu verpflichtet bestimmte Verwaltungsleistungen auch digital über Verwaltungsportale anzubieten, die Verwaltungsportale werden zu einem Portalverbund verknüpft (§ 1 OZG). Für die IT-Sicherheit der an den Portalverbund angebundenen IT-Komponenten sind verbindliche Maßnahmen und Standards durch die IT-Sicherheitsverordnung Portalverbund (ITSiV-PV) definiert. Dazu zählen beispielsweise Technische Richtlinien, die durch das BSI herausgegeben werden sowie verbindliche Penetrationstests und Webchecks (§ 2 Abs. 2 und 6 ITSiV-PV). Kritik im Zusammenhang mit der IT-Sicherheitsverordnung Portalverbund gab es in Bezug auf die späte Veröffentlichung des Standards zu einem Zeitpunkt, zu dem entsprechende Software bereits entwickelt war und Anforderungen nachträglich umzusetzen sind. Zudem sehen Kommunen Probleme bei der konkreten Umsetzung der Richtlinie sowie dem entstehenden finanziellen Aufwand [Pu22].

BSI-Gesetz und Richtlinie zur Netz- und Informationssicherheit

Zum Teil sind kommunale Einrichtungen der Kritischen Infrastruktur (KRITIS) nach § 2 Abs. 10 BSIG zu zuordnen, sofern bspw. kommunale Eigenbetriebe Aufgaben im Bereich der KRITIS Sektoren, wie Wasser oder Energie übernehmen und die entsprechenden Schwellenwerte erreichen (Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz). Für Betreiber Kritischer Infrastrukturen gelten besondere Anforderungen an die technischen und organisatorischen Vorkehrungen zur Vermeidung von Cybersicherheitsvorfällen sowie zur Meldung von Störungen (§§ 8a ff. BSIG).

Auf europäischer Ebene definiert die Richtlinie (EU) 2016/1148 zur Gewährleistung einer hohen Netzwerk- und Informationssicherheit (NIS-Richtlinie) einheitliche Anforderungen an die Mitgliedsstaaten sowie Betreiber Kritischer Infrastrukturen. Die Europäische Kommission hatte im Dezember 2020 einen Vorschlag für eine überarbeitete NIS-Richtlinie (NIS-2-Richtlinie) vorgelegt [Eu20]. Im Mai 2022 wurde eine vorläufige, bislang unveröffentlichte Einigung erzielt, die noch angenommen werden muss. Grundsätzlich sieht die NIS-2-Richtlinie einen wesentlich breiteren Anwendungsbereich vor. Ein wesentlicher Diskussionspunkt in den Verhandlungen war die Frage, welche Ebenen der öffentlichen Verwaltung von den Regelungen erfasst werden sollen. Die Einigung sieht eine grundsätzliche Einbeziehung der öffentlichen Verwaltung vor, räumt den Mitgliedsstaaten aber Spielraum bei der Beurteilung ein, inwiefern Einrichtungen auf lokaler Ebene erfasst werden [Be22] [Rh22]. Ein wichtiger Gesichtspunkt künftiger Forschungsarbeiten wird die Analyse der NIS-2-Regelungen und der Umsetzung in Deutschland sein sowie die Auswirkungen hiervon im spezifischen Umfeld der föderalen Verwaltungsstrukturen in Deutschland.

Verfassungsrechtliche Anforderungen

Ein Forschungsbedarf lässt sich zudem bei der Untersuchung verfassungsrechtlicher Anforderungen an die Cybersicherheit der kommunalen Verwaltung erkennen sowie bei der Frage, ob bestehende und künftige gesetzliche Regelungen diesen Anforderungen entsprechen. Im Hinblick auf die zunehmende Bedeutung der Nutzung informationstechnischer Systeme hat das Bundesverfassungsgericht 2008 erstmals ein grundrechtlich erhebliches Schutzbedürfnis festgestellt und das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität von IT-Systemen als Ausprägung des allgemeinen Persönlichkeitsrechts beschrieben [Bu08]. Der Gewährleistungsgehalt von Grundrechten beschränkt sich nicht auf deren Abwehrfunktion, sondern kann auch staatliche Schutzpflichten begründen, also eine konkrete Pflicht des Staates dazu beizutragen, dass die Cybersicherheit von IT-Systemen geschützt wird [Bu21].

4 Ausblick

In Anbetracht des hohen Maßes an gesellschaftlicher, wirtschaftlicher und staatsorganisatorischer Abhängigkeit von der Verfügbarkeit kommunaler Leistungen sowie der Vertraulichkeit von Daten im kommunalen Wirkbereich wird die Untersuchung der rechtlichen Rahmenbedingungen und Anforderungen an die Cybersicherheit im spezifischen Umfeld der kommunalen Verwaltung in Zukunft wichtiger Forschungsgegenstand sein. Die skizzierten rechtlichen Anknüpfungspunkte sind nicht abschließend und lassen sich insbesondere hinsichtlich konkreter Handlungsbedarfe sowie ihrer Angemessenheit weiter untersuchen. Dabei sind insbesondere auch praktische Herausforderungen im Kontext der kommunalen Selbstverwaltung, der Organisationsstrukturen sowie der finanziellen und personellen Umsetzbarkeit von Anforderungen zu analysieren.

5 Literaturverzeichnis

[Ar18] Artikel-29-Datenschutzgruppe, Leitlinien für die Meldung von Verletzungen des Schutzes personenbezogener Daten, zuletzt überarbeitet und angenommen am 06.02.2018.

[BA10] Bedner, M.; Ackermann, T.: Schutzziele der IT-Sicherheit, DuD 2010, S. 323-328.

[Be22] Bertuzzi, Luca: NIS-2 kommt – und nun?, Tagesspiegel Background, https://background.tagesspiegel.de/cybersecurity/nis-2-kommt-und-nun, 16.05.2022.

[BS21] Bundesamt für Sicherheit in der Informationstechnik, Die Lage der IT-Sicherheit in Deutschland 2021

[BS22] Bundesamt für Sicherheit in der Informationstechnik, Glossar der Cybersicherheit, https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Glossar-der-Cyber-Sicherheit/glossar-der-cyber-sicherheit_node.html, Stand: 28.04.2022.

[Bu21] Bundesverfassungsgericht, Beschluss vom 08.06.2021, 1 BvR 2771/18.

[Bu08] Bundesverfassungsgericht, Urteil vom 27.02.2008, 1 BvR 370/07 u. 595/07.

[Bu74] Bundesverfassungsgericht, Beschluss vom 18.12.1974, 1 BvR 430/65 u. 259/66.

[DD22] Deutscher Städtetag, Deutscher Landkreistag, Deutscher Städte- und Gemeindebund: IT-Grundschutz-Profil Basis-Absicherung Kommunalverwaltung, 31.03.2022.

[Do18] Does S.: Security-Notruf – Sicherheitslücke in Notfall-App legt Einsatzdaten offen, c't 7/2018, S.60.

[Eu20] European Commission, Proposal for a Directive on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148, 16.12.2020.

[Eu21] Europäischer Datenschutzausschuss, Guidelines 01/2021 on Examples regarding Personal Data Breach Notification, Version 2.0, Stand 14.12.2021.

[Go20] Golem, Schwere Sicherheitslücken in bayerischer Wahlsoftware, https://www.golem.de/news/ok-vote-schwere-sicherheitsluecken-in-bayerischer-wahlsoftware-2012-153062.html, Stand: 28.04.2022.

[GW21] Grimm, R.; Waidner. M.: IT-Sicherheit aus technischer Sicht. In (Hornung, G.; Schallbruch, M., Hrsg): IT-Sicherheitsrecht Praxishandbuch. Nomos, Baden-Baden, 1.Auflage, S. 33-62, 2021.

[He21] Heise online, Witten: Bei Cyberangriff erbeutete Daten im Darknet veröffentlicht, https://www.heise.de/news/Hacker-veroeffentlichen-Wittener-Daten-Buergermeister-warnt-6269952.html, Stand: 28.04.2022.

[Ko20] Kommunal, So schützen sich Behörden von Cyber-Kriminellen, https://kommunal.de/schuetzen-vor-cyber-kriminellen.

[Ko17] Kommunale Spitzenverbänden, Handreichung zur Ausgestaltung der Informationssicherheitsleitlinie in Kommunalverwaltungen, Februar 2017.

[Pu22] Punz, Matthias: OZG: Kritik an Verordnung zu IT-Sicherheit, Tagesspiegel Background, https://background.tagesspiegel.de/smart-city/ozg-kritik-an-verordnung-zu-it-sicherheit, 25.01.2022.

[Rh22] Rheinland-Pfalz Landesvertretung Brüssel, Rat und Parlament erzielen Einigung über EU-Cybersicherheits-niveau, https://europa.rlp.de/de/aktuelles/detail/news/News/detail/rat-und-parlament-erzielen-einigung-ueber-eu-cybersicherheits-niveau/, 20.05.2022.

[Sä20] Sächsisches Staatsministerium für Kultus, Cyberangriff legt LernSax lahm, https://www.bildung.sachsen.de/blog/index.php/2020/12/15/cyberangriff-legt-lernsax-lahm/.

[Sc21] Landeshauptstadt Schwerin, IT-Störungsmeldung, https://www.schwerin.de/it-stoerungsmeldung/, Stand: 28.04.2022.

[SK20] Sohr, K.; Kemmerich, T.: Technische Grundlagen der IT-Sicherheit. In (Kipker, D.-K., Hrsg): Cybersecurity Rechtshandbuch, 1. Auflage, C.H. Beck München, S. 23-82, 2020.

[Sp21] Spiegel Online, Cyberangriff auf Schulplattform, https://www.spiegel.de/netzwelt/web/rheinland-pfalz-14-jaehriger-stoerte-von-schulen-genutztes-konferenzsystem-a-664fa36a-c962-42a8-bca6-529342b81c79.

[St21] Stiftung Neue Verantwortung, Transkript zum Hintergrundgespräch: "Cyberkriminelle erpressen Anhalt-Bitterfeld - Was können wir daraus lernen?", https://www.stiftung-nv.de/de/publikation/transkript-zum-hintergrundgespraech-cyberkriminelle-erpressen-anhalt-bitterfeld-was#collapse-newsletter_banner_bottom, Stand 28.04.2022.

[We22] Weidemann, M.: Lexikon des Strafrechts – Computerkriminalität. In (Heintschel-Heinegg, B., Hrsg): BeckOK StGB, 52. Edition, C.H. Beck, München, 2022.