Strafrechtliche Relevanz von Datensicherheit und Datenschutz im Unternehmen

Carsten Momsen

Inhaltsverzeichnis

C. Momsen (✉)
Freie Universität Berlin, Fachbereich Rechtswissenschaft, Berlin, Deutschland
E-Mail: carsten.momsen@fu-berlin.de

W. Frenz (Hrsg.), *Handbuch Industrie 4.0: Recht, Technik, Gesellschaft*,
https://doi.org/10.1007/978-3-662-58474-3_4

1 Einleitung

Unternehmen können durch eine Vielzahl klassischer sog. „**IT-Delikte**“ betroffen werden. Sie können Opfer von Hacking-Angriffen werden, ebenso, wie Mitarbeiter sich der Ressourcen des Unternehmens bedienen können, um eigene Straftaten zu begehen. Dasselbe gilt auch für die Versendung inkriminierter, etwa kinderpornographischer, rassistischer oder volksverhetzender Inhalte. Auch können im Bereich des Kapitalmarktstrafrechts die Infrastrukturen von Unternehmen genutzt werden, um Straftaten zu begehen. Das Gleiche gilt im Bereich der Ausspähung von Betriebsgeheimnissen, auch hier können Unternehmen auf der Täter- (Mitarbeiter) oder Opferseite stehen. Diese und andere Erscheinungsformen sind jedoch nicht im eigentlichen Sinne unternehmens- oder industriespezifisch.

Spezifisch für Unternehmen ist jedoch die Situation, in einem Schnittfeld teilweise nicht ohne weiteres kompatibler Interessen und Pflichten zu stehen. Treffen beispielsweise Anforderungen des Datenschutzes mit solchen der Kooperation mit Ermittlungsbehörden aufeinander, können Unternehmen sowohl erhebliche Geldbußen (und den leitenden Mitarbeiter∗innen strafrechtliche Verfolgung) drohen, als auch dann, wenn zu wenig Informationen freigegeben werden. Die Probleme verschärfen sich im Bereich internationaler tätiger Unternehmen.

Daher werden nachfolgend Bereiche dargestellt, die spezifische Risiken bzw. Pflichten für Unternehmen begründen können. Diese sind ganz zentral mit dem Schutz der eigenen Daten und Infrastrukturen sowie möglichen Abwehrmaßnahmen gegen entsprechende Angriffe verbunden. Zudem müssen Unternehmen Vorsorge treffen, sowohl dagegen, Opfer von vermeidbaren Angriffen zu werden, als auch davor, dass aus ihrem Bereich heraus Straftaten begangen werden. Damit ist der Bereich der Prävention und Compliance angesprochen.

Werden Unternehmen dennoch in Strafverfahren verwickelt, so treffen sie Nachweispflichten und ggf. Mitwirkungspflichten. Sie können auch Gegenstand von Ermittlungsmaßnahmen im Online-Bereich werden. Auf der anderen Seite stehen aber auch Rechte zum Schutz eigener sensibler Informationen und Interessen. Wichtig ist hier in jedem Fall eine Dokumentation aller relevanten Vorgänge.

Folgende Themen stehen im Mittelpunkt des Beitrags: Datenschutz und Strafrecht, eigene Verpflichtungen zum Datenschutz, bspw. nach § 203 StGB, die strafrechtliche Relevanz möglicher Abwehrmaßnamen, Online-Ermittlungen gegen Unternehmen, Prävention, Digital Compliance, digitale Beweise und die Standards der „Forensic Readiness“.

2 Datenschutz und Strafrecht

2.1 Verletzung des Betriebs- und Geschäftsgeheimnisses, strafrechtliche Verpflichtung zum Schutz personenbezogener Daten im Unternehmen

Betriebsgeheimnisse und personenbezogene Daten stehen in verschiedener Hinsicht unter strafrechtlichem Schutz, § 203 StGB. In jedem Fall bedeutet dies für Unternehmen die rechtliche Verpflichtung zu besonderer Sorgfalt bei Erhebung, Verarbeitung, Speicherung und insbesondere bei der Weitergabe solcher Daten. Nachfolgend werden der Schutz solcher Daten durch bestimmte Berufe und die daraus folgenden **Konsequenzen für Dienstleister** beleuchtet, d. h. solche Unternehmen deren Geschäftszweck in der Erbringung von datenbezogenen Dienstleistungen liegt (dieser Abschnitt folgt in Teilen Grosskopf und Momsen 2018, S. 98 ff., sowie Momsen und Savic 2017, S. 301 ff.).

Exemplarisch für ein aktuelles deutlich erweitertes Schutzkonzept ist die Novelle des § 203 StGB. Durch dessen Neufassung und die verbundene Anpassung berufs- (ordnungs-) rechtlicher Vorschriften müssen Berufsgeheimnisträger und deren Diensteanbieter ihre bisherigen betrieblichen Abläufe neu justieren, wozu sie auch die Datenschutz-Grundverordnung (DSGVO) zwingt, die am 25.05.2018 in Kraft getreten ist.

Berufs- und andere Geheimnisträger nutzen häufig externe Dienstleister, weil sie zeitlich oder technisch, aber auch aus kommerziellen Gründen nicht in der Lage sind, alle für den Kanzleialltag notwendigen Dienstleistungen durch Angestellte zu erbringen. Die externen Dienstleister kommen mit den häufig hochsensiblen Daten der Mandanten/Patienten/Kunden und anderer Personen in Kontakt. Sie unterlagen aber nicht per se dem Berufsgeheimnisschutz. § 203 StGB n.F. in Verbindung mit den einschlägigen berufs-(ordnungs-) rechtlichen Normen soll jetzt einen umfassenden Geheimnisschutz sicherstellen. Einhergehend mit der Reform im vergangenen Herbst werden den Berufsgeheimnisträgern aber gleichzeitig erheblich weitergehende Pflichten aufgebürdet, die sich als eine umfassende Kanzlei-Compliance darstellen. Diese Pflichten werden durch die **Datenschutzgrundverordnung** (DGSVO) nochmals erweitert und teilweise konkretisiert.

Interne und vor allem externe Systemadministratoren sind faktisch gezwungen, alle Daten – darunter auch personenbezogene – in Augenschein zu nehmen, die mit den von ihnen angebotenen Programmen bearbeitet werden, um ein Problem zu beseitigen. Dementsprechend verfügen sie zwangsläufig über sehr viel „Insiderwissen“. Dies betrifft einmal die verarbeiteten Daten, aber genauso diejenigen Metadaten, welche vom Charakter her Verkehrsdaten sind, also bspw. wer wann wie lange mit welchen Programmen und welchen Inhalten arbeitet. Systemadministratoren und vergleichbare Mitarbeiter sind daher nicht nur innerhalb von Unternehmen besondere Geheimnisträger, sondern auch dann, wenn sie als selbstständige Dienstleister tätig sind oder die IT eines Unternehmens bei einem Cloud-Anbieter betreuen (Managed Services). Sind außenstehende Systembetreuer bspw. für Anwalts-,

Notars-, Patentanwalts-, Steuerberater- oder Wirtschaftsprüferkanzleien tätig, also Kanzleien, auf deren Speichermedien sich unzählige Geheimnisse ihrer Auftraggeber befinden, werden sie natürlich angehalten, den Datenschutz und das Mandantengeheimnis zu beachten. Ungeachtet der seit langem davon unbeeindruckten Praxis war rechtlich fraglich, ob insbesondere Berufsgeheimnisträger überhaupt externen Systembetreuern Zugang zu den fremden Geheimnissen gewähren dürfen, die ihnen in ihrer beruflichen Eigenschaft anvertraut oder bekannt geworden sind. Mit der Änderung des § 203 Abs. 3 und Abs. 4 des Strafgesetzbuches (StGB) wurde nun der Weg für eine klarere Regelung eines Graubereichs bei der Auslagerung von Dienstleistungen auch für Unternehmen der privaten Kranken-, Unfall- oder Lebensversicherung sowie Verrechnungsstellen eröffnet werden (Gesetz zu Neuregelung des Schutzes von Geheimnissen bei der Mitwirkung Dritter an der Berufsausübung schweigepflichtiger Personen, Gesetzesmaterialien abrufbar unter https://www.bundesrat.de/SharedDocs/beratungsvorgaenge/2017/0601-0700/0608-17.html). Das heißt, alle Unternehmen, welche IT-Dienste u. a. für diese Berufsgruppen (also auch für Krankenhäuser und Verwaltungs- und Justizbehörden, in denen Angehörige der genannten Berufe mit Geheimnissen in Berührung kommen) anbieten, sind von dem neuen Schutzkonzept betroffen.

§ 203 StGB stellt den Schutz von Geheimnissen vor unbefugter Offenbarung sicher, die (Berufs-) Geheimnisträgern im Rahmen ihrer beruflichen Tätigkeit anvertraut werden. Durch das „Gesetz zur Neuregelung des Schutzes von Geheimnissen bei der Mitwirkung Dritter an der Berufsausübung schweigepflichtiger Personen“ (BT-Drs. 18/11936, S. 36) wird § 203 StGB sowie das verbundene Verfahrens- und Berufsordnungsrecht umgestaltet, wodurch ein Geheimnisschutz auch im Zeitalter des – nicht nur digitalen – Outsourcing sichergestellt werden soll. Die Gesetzesänderung soll bereits vielfältig praktizierte Formen des Outsourcings mit den Bedürfnissen eines strafrechtlich wirksamen Geheimnisschutzes in Einklang bringen. Dabei geht es nicht nur um IT-Outsourcing und die Übertragung von konkreten fachlichen Aufgaben durch Legal Information Management oder Legal Project Management auf Dritte, sondern auch um sonstige Tätigkeiten wie Aktenvernichtung, Schreib-, Übersetzungs- oder Rechnungsarbeiten und Telefonservice. Die neu geregelten straf- und die damit einhergehenden strafverfahrensrechtlichen Normen stellen im Zusammenspiel mit der Datenschutzgrundverordnung (DSGVO, Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27.04.2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG, Abl L 119/1 vom 04.05.2016) explizierte und teilweise weitreichende Anforderungen an die **Compliance** für Berufsgeheimnisträger, aber auch für Dienstleister auf.[1]

Externe Dienstleister werden als Gehilfen qualifiziert und somit in den Kreis der Verpflichteten neu aufgenommen, wenn sie in irgendeiner Art und Weise in deren

[1] Diese Geheimhaltungspflicht wird durch § 29 Abs. 3 BDSG (neu) flankiert. Im Geltungsbereich des § 203 StGB dürfen die Aufsichtsbehörden nicht die Herausgabe von Daten verlangen bzw. veranlassen. Erhalten sie dennoch Zugriff auf entsprechend geschützte Daten, so erweitert sich der Anwendungsbereich des § 203 StGB automatisch auf die Aufsichtsbehörde.

berufliche Tätigkeit eingebunden sind und dazu Beiträge leisten. Die mit der Einschaltung dritter Personen verbundene Verringerung des Geheimnisschutzes wird kompensiert, indem mitwirkende Personen in die Strafbarkeit nach § 203 StGB einbezogen werden, die bei der ordnungsgemäßen Durchführung ihrer Tätigkeit die Möglichkeit erhalten, von geschützten Geheimnissen Kenntnis zu erlangen. Jetzt machen sich also alle an der Berufsausübung mitwirkenden Personen strafbar, wenn sie ein Geheimnis offenbaren, das ihnen bei ihrer Tätigkeit bekannt geworden ist. Die (Berufs-) Geheimnisträger sind deshalb auch zur Belehrung der mitwirkenden Personen über die jetzt bestehende Strafbarkeit verpflichtet (§ 203 Abs. 4 Nr. 2 StGB). Sie dürfen aber dennoch nicht generell Zugang zu den Geheimnissen gewähren, sondern nur soweit dies zur Inanspruchnahme der Dienstleistung erforderlich ist (§ 203 Abs. 3 Satz 2 StGB).

Der Kunde hat bei der Einbeziehung **externer Personen** in die Berufsausübung für eine Verpflichtung zur Geheimhaltung Sorge zu tragen (§ 203 Abs. 4 Nr. 2 StGB). Diese Pflicht gilt unabhängig von berufsrechtlichen oder sonstigen rechtlichen Vorgaben. Die Verletzung dieser Pflicht ist für alle (Berufs-) Geheimnisträger strafbewehrt, wenn die einbezogene Person unbefugt ein Geheimnis offenbart hat (§ 203 Abs. 4 Nr. 2 StGB). Eine Beauftragung durch Zuruf etwa bei einem IT-Sicherheitsvorfall ist also nicht möglich, bei dem in der Regel nur durch rasches Handeln größerer Schaden verhindert werden kann. Im Rahmen der Erstellung der auch nach § 64 Abs. 3 Nr. 9 BDSG (neu) geforderten Kontinuitäts- und Wiederherstellungspläne muss daher im **Notfallhandbuch** eine Musterbelehrung aufgenommen werden, damit an die Belehrung bei IT-Notfällen erinnert wird.[2] Neben der Geheimhaltungsbelehrung ist aber auch eine datenschutzrechtliche Belehrung erforderlich, die bis zum 24.05.2018 in Schriftform erfolgen muss (§ 4a Abs. 1 Satz 3 BDSG alt). Gleiches gilt in mehrstufigen Auftragsverhältnissen in denen nur der Auftragnehmer zu verpflichten ist, auch die Subunternehmer zu belehren.

Die Prüfung der fachlichen Eignung soll anhand von **Zertifizierungen** und sonstige Qualifikationsnachweise erfolgen. Datenschutzrechtliche Zertifikate dürfen gem. Art. 42 Abs. 5 DSGVO nur von den Aufsichtsbehörden oder akkreditierten Zertifizierungsstellen ausgestellt werden. Solche datenschutzrechtlichen Zertifikate gibt es derzeit jedoch noch nicht,[3] da die EU-Datenschutz-Richtlinie 95/46/EG Zertifizierungen nicht als Beweise für Compliance ansah, weshalb sich auch das „Datenschutz-Gütesiegel“ des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein (s. https://www.datenschutzzentrum.de/guetesiegel/register/) und europäische Zertifikate wie das „European Privacy Seal (EuroPriSe – s. https://

[2] Ein komplettes Notfallmanagement ist auf der Webseite des Bundesamtes für Sicherheit in der Informationstechnik (BSI) beschrieben im BSI-Standard 100-4. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/ITGrundschutzstandards/BSI-Standard_1004.html. Zugegriffen am 01.10.2019.

[3] S. etwa das Forschungsprojekt für eine „European Cloud Service Data Protection Certification (Auditor)“ abrufbar unter http://auditor-cert.de und European Union Agency for Network and Information Security (ENISA), Recommendations on European Data Protection Certification, Version 1.0 November 2017. https://www.enisa.europa.eu/publications/recommendations-on-european-data-protection-certification/at_download/fullReport. Zugegriffen am 01.10.2019.

www.datenschutzzentrum.de/guetesiegel/register/)“ nicht am Markt durchgesetzt haben (s. ENISA, Annex A: Analyse der vorhandenen Zertifizierungen im Überblick, S. 32 ff.). Andere praxistaugliche Zertifizierungsverfahren müssen erst entwickelt werden.[4] Wie auch bzgl. der Zuverlässigkeit, werden die Dienstleistungsunternehmen hier selbst entsprechende Standards anbieten und garantieren müssen (§ 3 BZRG). Als Maßstab für die notwendige Überprüfung können die nach dem Geldwäschegesetz (GwG) vorzunehmenden „Pre-Employment-Screening“ und „In-Employment-Screening“ herangezogen werden.[5] Für die Beurteilung der Zuverlässigkeit ist maßgeblich, ob ein Dienstleister unter Berücksichtigung aller in Betracht kommenden Umstände des Einzelfalls eine ordnungsgemäße und vertragsgerechte Ausführung der zu erbringenden Leistung und vor allen Dingen die gebotene Geheimhaltung erwarten lässt. Der Auftragnehmer muss konkrete technische, organisatorische und personelle Maßnahmen ergriffen, mithin **ein Compliance-Managementsystem** eingerichtet und auch die Compliance-Anforderungen umgesetzt haben. Besondere Bedeutung erlangen diese Anforderungen beim Einsatz von Fernwartungssystemen.[6] Auch können im **Ausland** erbrachte Dienstleistungen genutzt werden. Voraussetzung ist aber ein mit dem Inland vergleichbares Schutzniveau, das nach der Gesetzesbegründung in allen EU-Mitgliedstaaten gegeben sein soll (BT-Drs. 18/11936, S. 35 unter Verweis auf die Schlussanträge der Generalan-

[4] S. etwa Vorschlag für eine EU-Verordnung „on ENISA, the „EU Cybersecurity Agency“, and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification („Cybersecurity Act“), COM(2017) 477 final/2 und auch ENISA, Overview of the practices of ICT Certification Laboratories in Europe“, Version 1.1, Januar 2018. https://www.enisa.europa.eu/publications/overview-of-the-practices-of-ict-certification-laboratories-in-europe/at_download/fullReport. Zugegriffen am 01.10.2019. S. dazu auch die „Draft Opinion“ von Seiten des Ausschusses für bürgerliche Freiheiten, Justiz und Inneres des Europäischen Parlaments (Berichterstatter Jan Philipp Albrecht), 2017/0225(COD). http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+COMPARL+PE-615.394+02+DOC+PDF+V0//EN. Zugegriffen am 01.10.2019.

[5] S. Bundesamt für Verfassungsschutz/Bundesamt für Sicherheit in der Informationstechnik/Bundesverband Allianz für Sicherheit in der Wirtschaft e.V., Wirtschaftsgrundschutz, Baustein MA2 Bewerberprüfung, Stand Juli 2017. https://www.wirtschaftsschutz.info/DE/Aktuelles/Wirtschaftsgrundschutz/Bausteine/Bewerberpruefung.pdf. Zugegriffen am 01.10.2019.

[6] Vor dem Einsatz einer Fernwartung ist zu überprüfen, ob die Fernwartungssoftware eine verschlüsselte Übermittlung ermöglicht und welche Verschlüsselung verwendet wird, usw. Bei der Inanspruchnahme von Cloud-Plattformen wie Dropbox, Google Drive, Microsoft OneDrive etc., also dem Speichern von Geheimnissen auf fremden Servern, muss neben der Transportverschlüsselung auch eine benutzer- oder gruppenbasierte Verschlüsselung auf Dateiebene im Unternehmen des Geheimnisträgers stattfinden, denn dann kann die Dienstleistung ohne Kenntnis von Geheimnissen erbracht werden.

Gleiches gilt bei Infrastructure as a Service (IaaS), bei der ganze Rechner (Server) gemietet werden, oder bei Platform as a Service (PaaS), bei der vom Anbieter nur eine Laufzeitumgebungen bereitstellt wird, innerhalb derer Anwender ihre eigene Software laufen lassen können. Bei „Software as a Service“ (SaaS) bietet der Dienstleister spezielle Software an, die auf den Ressourcen des Anbieters läuft und die dem Anwender online zugänglich gemacht wird, wobei der Dienstleister auch die Pflege durch Updates und Upgrades übernimmt, wie etwa bei Microsoft Office 365 und bei Google Docs, Sheets, Slides und Forms. Näher *Fechtner* und *Haßdenteufel*, CR 2017, S. 355, 357 f.

wältin Juliane Kokott vom 29.04.2010, Rechtssache C-550/07 P – Akzo Nobel, ECLI:EU:C:2010:229). Für das übrige Ausland muss im Einzelfall geprüft werden, ob der erforderliche Schutz gewährleistet ist, es sei denn der Schutz der Geheimnisse gebietet keinen vergleichbaren Schutz (§ 43e Abs. 4 BRAO; § 26a Abs. 4 BNotO; § 39c Abs. 4 PAO; § 62a Abs. 4 StBerG; § 50a Abs. 4 WiPrO).

Da die bisher gelebte Praxis nach der Gesetzesnovelle und dem Inkrafttreten der DSGVO keine legitimierende Wirkung mehr haben kann, bestehen die Pflicht zur Vertraulichkeit und die Pflicht zur Wahrung des Berufsgeheimnisses für alle bei den (Berufs-) Geheimnisträgern anfallenden Informationen (ausf. zu den möglichen Tatbestandsausschlüssen durch Sozialadäquanz: Roxin 2006 § 10 Rn. 36 ff.; Rosenau 2018 vor §§ 32 ff. Rn. 61 f.). Dies geschieht aber etwa beim Versand von unverschlüsselten eMails nach der wohl (noch) herrschenden Meinung der Literatur (s. Degen 2016, § 66 Rn. 109 ff.; Eisele und Lenckner 2014, § 203 Rn. 19; von Lewinski 2004, S. 12; Härting 2005, S. 1248; Sassenberg 2006, S. 196; a.A. Koch 2014, S. 691), obwohl die Kenntnisnahme der eMails Dritten ohne weiteres möglich ist und eMail-Provider ohne jeden Zweifel Outsourcingdienstleister sind (Gesetzesbegründung, BT-Drs. 18/11936, S. 8; vgl. auch Dix 2014, § 1 Rn. 170 m.w.N.). Zudem wird der Geheimnisschutz zukünftig durch den technischen und organisatorischen Datenschutz gem. Art. 5 Abs. 1f. und Art. 32 DSGVO flankiert und ein Verstoß mit Geldbußen geahndet (Art. 83 DSGVO).[7] Auch kann die Verarbeitung von personenbezogenen Daten ohne entsprechende Einwilligung der Betroffenen einen Wettbewerbsverstoß darstellen (LG Hamburg, Urt. v. 02.03.2017 – 327 O 148/16, BeckRS 2017, 117352). Schließlich fordert § 203 Abs. 4 Satz 2 StGB nicht nur eine sorgfältige Auswahl von Dienstleistern und eine Verpflichtung zur Geheimhaltung, sondern ausdrücklich auch eine Überwachung ihrer Tätigkeit.[8] Ausdrücklich muss die Zusammenarbeit beendet werden, wenn sich der Dienstleister Kenntnis von fremden Geheimnissen verschafft, die nicht zur Vertragserfüllung erforderlich sind (§ 43e Abs. 3 Nr. 2 BRAO; § 26a Abs. 3 Nr. 2 BNotO; § 39c Abs. 3 Nr. 2 PAO; § 62a Abs. 3 Nr. 2 StBerG; § 50a Abs. 3 Nr. 2 WiPrO). Ob sich der Dienstleister solche Kenntnisse verschafft, kann nur durch ständige Überwachung seiner Tätigkeit erfolgen. Eine solche Überwachung erfordert ein „**Managementsystem für Geheimnisschutz**“, also zunächst die Aufstellung von Verfahren und Regeln, welches dazu dienen sollen, den Geheimnisschutz zu definieren und zu steuern (Jahn und Palm 2011, S. 620 zu den Vorgaben für ein Anwaltssekretariats außerhalb der Kanzlei, speziell zum Telefonservice). Die Umsetzung dieses Systems durch den Dienstleister muss dann kontrolliert und fortlaufend verbessert werden. Der Dienstleister

[7] S. Stellungnahme des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit zur Geschäftsnummer D42/2017/1114 vom 08.01. 2018. https://www.datenschutzbeauftragter-info.de/wp-content/uploads/2018/02/schreiben-der-aufsichtsbehoerde.pdf. Zugegriffen am 01.10.2019. und 8. Tätigkeitsbericht des Sächsischen Datenschutzbeauftragten, vorgelegt zum 31.03.2017, S. 138.

[8] S. S. 4 des Referentenentwurfs des BMJV zu einem Gesetz zur Neuregelung des Schutzes von Geheimnissen bei der Mitwirkung Dritter an der Berufsausübung schweigepflichtiger Personen. https://www.bmjv.de/SharedDocs/Gesetzgebungsverfahren/Dokumente/RefE_Neuregelung_Schutzes_von_Geheimnissen_bei_Mitwirkung_Dritter_an_der_Berufsausuebung_schweigepflichtiger_Personen.pdf. Zugegriffen am 01.10.2019.

muss also angehalten werden, seine Dienstleistung nach dem „Stand der Technik“ zu erbringen, also nach dem Entwicklungsstand fortschrittlicher Verfahren, Einrichtungen oder Betriebsweisen, der die praktische Eignung einer Maßnahme oder Vorgehensweise zum Schutz der Geheimnisse gesichert erscheinen lässt (zur Folgenabschätzung Art. 35 DSGVO). Für die digitale Archivierung ist der Stand der Technik niedergelegt in den „Technischen Richtlinien“ des BSI (s. BSI TR-03138 Ersetzendes Scannen (RESISCAN), abzurufen unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03138/TR-03138.pdf). Auch bei der **Fernwartung** sind die Vorgaben des BSI einzuhalten (s. BSI, IT-Grundschutz, M 5.33 Absicherung von Fernwartung, abzurufen unter https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m05/m05033.html). Für die Akten- und Datenträgervernichtung beschreibt bei (Berufs-) Geheimnisträgern als Stand der Technik die in der DIN 66399 beschriebene höchste Schutzklasse 3 für besonders vertrauliche und geheime Daten und mindestens die Sicherheitsstufe 4 (besonders sensible Daten – Reproduktion mit außergewöhnlichem Aufwand). Beim Schreib-, Übersetzungs- und Rechnungsarbeiten sowie natürlich auch bei der Fernwartung ist vom Dienstleister dessen eigene IT-Infrastruktur nach dem Stand der Technik zu schützen, also nach den BSI Anforderungskatalog M 1 (s. BSI, IT-Grundschutz, abzurufen unter https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m01/m01.html). Diese Anforderungen gelten nach § 13 Abs. 7 Telemediengesetz (TMG) bei online angebotenen Diensten (u. a. Gehrmann und Voigt 2017, S. 93; Michaelis 2016, S. 118). Für den Telefonservice gibt es keinen von unabhängigen Stellen vorgegebenen Stand der Technik (s. Jahn und Palm 2011, S. 613). Es ist daher fraglich, nach welchen Standards sich Anbieter richten müssen. Zudem werden Verträge mit Dienstleistern und Auftraggebern neu gefasst oder zumindest angepasst werden müssen. Eine pauschale Risikoabwälzung wird aber in praktisch keiner Richtung mehr stattfinden können.

2.2 Hacking gegen das Unternehmen: Die strafrechtliche Relevanz eigener Abwehrmaßnahmen gegen Angriffe auf die Unternehmens-IT

Die Einhaltung entsprechender Sicherheitsstandards ist nicht nur für die oben in Bezug genommenen IT-Dienstleister und Diensteanbieter essenziell, sondern für jedes Unternehmen. Gleichwohl kann es zu Angriffen auf die Unternehmens-IT kommen, die den Verlust von relevanten Daten und geschützten Geheimnissen befürchten lassen. Wie weit darf sich ein Unternehmen gegen derartige Angriffe verteidigen? In welcher Form kann **technische Prävention** betrieben werden?

Aufgrund der Struktur moderner IT-Angriffe kann eine Verteidigung nur dann erfolgreich sein, wenn sie so früh wie möglich ansetzt und den Abfluss von Daten verhindert. Präventive oder aktive **Verteidigungsstrategien** sind allerdings zum

größten Teil nach deutschem Recht ihrerseits mit der Begehung von Straftaten verbunden. Wer Opfer eines Angriffs auf Datenbestände oder Hardware geworden ist, wird versuchen, den Angriff möglichst schnell und nachhaltig zu beenden. Dies bedeutet, dass es in der Regel zu ineffektiv ist, staatliche Hilfe in Anspruch zu nehmen, also bspw. eine Strafanzeige zu stellen und darauf zu warten, dass der Angreifer ermittelt und verurteilt wird. Neben der Frage der Schnelligkeit und Effektivität polizeilicher Maßnahmen liegt ein weiteres Problem darin, dass Angriffe häufig mit Auslandsbezug erfolgen, staatliche Ermittlungen daher auf den zähen Weg der Rechtshilfe durch andere Staaten verwiesen sind. Eine nachhaltige Verteidigung wird am besten durch eigene „**Active Defense**“ sichergestellt, dem aktiven Vorgehen gegen Angreifer mit dem Ziel deren Infrastruktur zu zerstören und weitere Angriffe zu unterbinden. Darin liegt aber zugleich eine eigene, strafrechtlich erfassbare Angriffshandlung begründet, die nur unter bestimmten Bedingungen und in engen Grenzen als Notwehr gerechtfertigt sein kann. Ist der Angriff durch staatliche Stellen veranlasst, schrumpft der Freiraum für „Active Defense“ noch weiter.

Betrachtet man die Masse der Hacking-Versuche auf Unternehmensseiten, so lassen sich Angriffe grob strukturieren:

- Das Remote-System (RS) ist im Besitz der Angreifer und führt einen aktiven Angriff auf das System des Unternehmens durch.
- Das RS befindet sich nicht im Besitz der Angreifer, diese sind aktive „Nutzer“ auf dem RS.
- Das RS hat eine Schwäche, die der Angreifer ausnutzt und es aus der Ferne kontrolliert.
- Das RS wird für Durchführung des Angriffs ausgenutzt, der Angriff erfolgt automatisiert.

Bei Planung eines „Counter-Strike“, fragt sich, welche Rückwirkungen in jedem dieser Szenarien für das angegriffene Unternehmen selbst entstehen. Aufgrund der Struktur strafrechtlicher Verhaltenspflichten kann eine Selbstverteidigung im Sinne der Active-Defense nur in Ausnahmefällen gerechtfertigt sein. Zumindest muss der ursprüngliche Angriff rechtswidrig sein und es muss einen guten Grund für die ausnahmsweise Gestattung dieser Form von Selbstverteidigung geben.

Der hier einschlägige Rechtfertigungsgrund der **Notwehr** (§ 32 StGB) erfordert zunächst einen rechtswidrigen und gegenwärtigen Angriff auf geschützte Interessen. Die auf den Angriff folgende Verteidigungshandlung muss erforderlich und geeignet sein. Grundsätzlich darf eine Verteidigung daher nur gegen den Angreifer stattfinden, jedoch gab es in der Vergangenheit auch Fälle in denen von diesem Grundsatz Ausnahmen gemacht wurden, indem man auch gegen Dritten gehörende Gegenstände etc. vorgehen durfte, sofern diese beim Angriff benutzt wurden. Das Maß der erforderlichen Verteidigung richtet sich nach der Intensität des Eingriffs. Grundsätzlich ist unter mehreren gleichermaßen geeigneten Verteidigungsoptionen die mildeste zu wählen, die den Angreifer am wenigsten belastet. Eine weitere Einschränkung des Notwehrrechts erfolgt nach dem Kriterium der Angemessenheit. Man spricht hier auch von sog. „sozial-ethischen Einschränkungen“ des ansonsten sehr weit reichenden Notwehrrechts. Bspw. wird ein Ausweichen den Angreifer idR

nicht seinerseits verletzen, so dass vom Angegriffenen eine solche passive Schutzreaktion erwartet wird, soweit sie zumutbar ist. Weitere Einschränkungen können sich bei einem krassen **Missverhältnis** zwischen dem Erhaltungsgut und dem Eingriffsgut ergeben.

Für die Legitimation von Active-Defense Maßnahmen sind diese Einschränkungen ersichtlich von großer Bedeutung. Darf bspw. angesichts des Verlusts relativ unbedeutender Daten im Active-Defense-Modus die gesamte Infrastruktur des Angreifers zerstört werden? Was gilt, wenn sich der wahre Angreifer widerrechtlich der Infrastruktur eines Dritten bedient? Da die aufgezeigten Konstellationen sich häufig einer abstrakten rechtlichen Bewertung entziehen, kommt es vielfach zu interessenabwägenden Entscheidungen. Hier kann die Berücksichtigung ethischer Wertentscheidungen sehr hilfreich sein. Beispielsweise sind unbeteiligte Dritte, die der Angreifer sich nur zunutze macht, nach Möglichkeit zu schonen. Dies kann sich aber anders darstellen, wenn der Unbeteiligte zwar mit dem Angreifer nichts gemein hat, aber gerade dadurch, dass er ihm – in gutem Glauben – Ressourcen bereitstellt, Gewinne macht.

Um die Abwägung vornehmen zu können sind die verschiedenen Grundformen von Hackings welche mittels Active-Defense Maßnahmen bekämpft werden sollen, zu identifizieren. Sodann ist zu überprüfen, ob das Hacking einen Angriff darstellt, gegen welche eine Ausübung des Notwehrrechts überhaupt in Betracht kommen kann. In einem zweiten Schritt ist (ggf.) zu bewerten, ob die Active-Defense-Maßnahme eine zulässige Notwehrhandlung im strafrechtlichen Sinn darstellen kann. Angriffe richten sich grundsätzlich gegen Lücken im System des Angegriffenen, die in jedem System massenhaft vorhanden sind.

Es werden mindestens drei verschiedene Arten von Angriffen unterschieden:

2.2.1 Domain-Name-System

Vergleichbar mit der Situation, dass jemand anonym einen Katalog unter falschen Namen an jemand anderen schickt.

A (Angreifer) schickt eine Anfrage an B los, mit der Information, die Antwort an D zu schicken A kann frei auswählen, an wen die Antwort geschickt werden soll). B schickt Anfrage weiter an C. C schickt Antwort an B, der diese an D (Angegriffener) schickt. D wird also direkt von B angegriffen, eigentlich jedoch von A (das sog. „**Attributionsproblem**“).

2.2.2 Angriff zur Industriespionage

Häufig erfolgen auf Spionage gerichtete Angriffe in der Weise, dass ein Virus in der Hardware (Tastatur) eingespeist wird. Von dort aus fragt dieser regelmäßig Daten vom Rechner ab. Hier gibt es kaum Möglichkeiten, den Angriff zu entdecken. Manchmal hinterlässt der Angreifer auch eine Art „Hintertür“, über die er sich immer wieder unbemerkt Zugriff auf das System verschaffen kann.

2.2.3 Drive-by-downloads

Gleiches gilt bei der Infektion mit einem Virus der die gesamte Festplatte verschlüsselt, während ein Programm downloaded.

2.2.4 Angriffe über Back-ups oder USB-Sticks

USB-Sticks mit Virus werden beispielsweise mit der Aufschrift „Urlaubsbilder" auf Firmenparkplatz/im Büro liegen gelassen. Sobald eingestöpselt, installiert sich der Virus.

2.2.5 Angriffs- und Verteidigungsformen

Im Fall des Hackings können Daten betroffen sein, die sowohl dem Eigentum und Vermögen als auch dem Persönlichkeitsrecht unterfallen. Dabei kann als Auslegungshilfe dienen, dass die §§ 202a ff. StGB gegen Daten gerichtete Verhaltensweisen (Ausspähen, Abfangen, Vorbereitungshandlungen, Verrat von Privat und Geschäftsgeheimnissen) explizit unter Strafe stellen. Die Vorschriften schützen weitreichendes Interesse an der Geheimhaltung von Daten, die nicht unmittelbar wahrnehmbar gespeichert sind oder übermittelt werden (so Heger 2018, Rn. 1 ff.; Lenckner und Winkelbauer 1986, S. 485; Schmölzer 2011, S. 724; Haß 1993, S. 480 Rn. 20; Jessen 2014 S. 37; Schulze-Heiming 1995, S. 37; Schreibauer und Hessel 2007, S. 616; Schumann 2007, S. 675, 676; Eisele 2013, S. 6/1; krit. Hilgendorf 2015 S. 8/49–54; aM Haft 1987, S. 9). Die Berechtigung an der Speicherung und Nutzung von Daten ist daher ein notwehrfähiges Rechtsgut. Man kann damit von einem umfassenden strafrechtlich geschützten Bereich gespeicherter Daten sprechen. Sofern Ziel des Angriffs Daten sind, die bei einem externen Anbieter, etwa einem Cloud-Provider, gespeichert sind, wären diese im Wege der Nothilfe ggf. auch vom Unternehmen, als Dritten zu verteidigen.

Grundsätzlich kann das Eindringen in einen anderen Computer mittels eines dafür eigens hergestellten Programms als Angriff bewertet werden. Denn um spionieren oder sabotieren zu können, muss man faktisch zunächst bestimmte Schutzvorrichtungen des Computers, den man „angreift", umgehen. Technisch betrachtet, könnte man bereits dieses „Umgehen" als eine Art „Angriff" sehen. Auch die Voraussetzung, dass der Angriff durch menschliches Verhalten erfolgen muss, lässt sich in der Mehrzahl der Fälle bejahen. Denn bspw. die Erstellung eines Programms, mit dem man im Endeffekt seinen Angriff verüben möchte, bedarf ja immer eines gewissen menschlichen Verhaltens (Erstellung/Eingabe eines Codes etc.). Zudem muss zu einem bestimmten Zeitpunkt die Aktivierungssequenz ausgelöst werden.

Problematisch ist, dass Notwehr nur gegen „gegenwärtige", also gerade stattfindende Angriffe zulässig ist (BGH NJW 1979, 2053). Aufgrund der Schnelligkeit des Datenverlusts bei Angriffen auf die Unternehmens-IT ist einerseits die Frage von besonderer Relevanz, wann ein Angriff in der Weise bevorsteht, dass er „schon" gegenwärtig ist. Entscheidend ist, ob durch weiteres Zuwarten die Chancen zur

Erhaltung des Gutes (erheblich) verschlechtert werden. Ausgehend davon, dass bei vielen Angriffen trotzdem eine Reaktion erst auf das bereits erfolgte Eindringen möglich ist, muss auch geklärt werden, ob der Angriff noch andauert, d. h. „noch" gegenwärtig ist, da ansonsten das Rechtsgut nicht mehr gerettet, sondern allenfalls wiederhergestellt werden könnte. Ein Angriff ist zudem solange nicht beendet, wie sich der Angriffserfolg vergrößert, intensiviert oder eine Wiederholung zu befürchten ist. Beendet ist ein Angriff nicht nur, wenn er endgültig durchgeführt wurde, sondern auch, wenn er fehlgeschlagen ist, oder aufgegeben ist. Wird ein ehemaliger, bereits auf dem Rückzug befindlicher Angreifer attackiert, so kann im Gegenteil ein Angriff gegen diesen vorliegen, der von diesem seinerseits durch Notwehr abgewendet werden darf. Sofern das Opfer über eine Art „**automatisches Rückschlagprogramm**" verfügt, das einen Gegenschlag auslöst, dies aber erst nach einer „Aufklärungsphase" tut, wird es demgemäß schwierig, noch von einer „Gegenwärtigkeit" auszugehen. Es kommt also fallabhängig darauf an, wie lange typischerweise eine Aufklärungsphase andauert und ob bzw. welche technischen Möglichkeiten bestehen, diese „schnell" (also in unmittelbaren zeitlichen Zusammenhang zu dem Angriff) durchzuführen.

2.2.6 Fehlattribution

Vor dem Hintergrund des sog. „Attributionsproblems", also in strafrechtliche Kategorien übersetzt, der Schwierigkeit, den Angriff bspw. eine DDoS-Attacke dem wirklichen Veranlasser zuzurechnen, wird insbesondere die Erforderlichkeit der Verteidigung zu einem erheblichen Problem (Momsen und Savic 2018, § 32 Rn. 25–25.3). Häufig ist es nicht möglich genau zu identifizieren, woher ein Hackerangriff kommt, sofern dieser dadurch seine Spuren verwischt, dass er andere Systeme für den eigentlichen Angriff nutzt. Das bedeutet im Umkehrschluss, dass es unter Umständen keine geeignete Maßnahme gibt, mit denen man aktiv gegen einen Angriff vorgehen kann. Dann wären lediglich passive Maßnahmen, wie bspw. die Einrichtung einer Firewall zulässig. Während die Geeignetheit hier damit eine eher von technischen Parametern geprägte Frage darstellt, kommt in den verbleibenden Fällen der Auswahl des Verteidigungsmittels eine besondere Bedeutung zu, wenn nicht ausgeschlossen oder sogar wahrscheinlich ist, dass die Active-Defense die Infrastruktur eines unbeteiligten oder bestenfalls fahrlässig unterstützenden Dritten beschädigt. Das „Attributionsproblem" führt (insbesondere bei professionellen Angriffen) zu einem Identifikationsproblem. Der Angegriffene kann lediglich den kompromittierten Rechner als Angreifer identifizieren, nicht aber, wo der Angriff, der sich schon gegen den angreifenden Rechner richtete, seinen Ursprung hatte.

2.2.7 Automatische Reaktion auf Angriffe

Problematisch ist, dass automatische Programme, die aktiv abwehren sollen, häufig erst aktiv bzw. effektiv werden können, nachdem der Angriff schon vorüber ist. Zudem sind die Angriffe sehr spezifisch – es ist (mathematisch) nicht möglich ein Programm

zu schreiben, dass auf jegliche Angriffe vorbereitet ist. Durch genaue Beobachtung ist es lediglich möglich herauszufinden, dass sich das System verändert hat. Ob diese Veränderung dann durch einen Angriff oder lediglich durch einen Systemfehler verursacht wurde, ist dann zusätzlich zu untersuchen. Dies führt u. a. dazu, dass die Angriffe erst viel zu spät bemerkt werden. Wenn der Angriff dann aber abgeschlossen ist, sieht man lediglich noch die Lücke, aber nicht, ob und welche Daten gestohlen wurden.

2.2.8 Sog. „Honeypot“ Methode

Erfolgversprechend ist daher die Möglichkeit auf dem eigenen System Software zu installieren, die „verseucht“ ist, so dass man auf das System des Hackers, der diese kopiert und auf seinem System öffnet, über die „remote shell“ Methode zuzugreifen und diesen identifizieren kann. Dabei besteht beispielsweise die Möglichkeit die Kamera und das Mikrofon des Hackerrechners (GPS Koordinaten etc.) zu nutzen. Problematisch an dieser Methode ist zum einen, dass der Angriff überhaupt erst mal bemerkt werden muss. Zum anderen kennen gerade professionelle Hacker diese Vorgehensweise und können sich wiederum dagegen abschirmen.

2.2.9 Zusammenfassung

Sofern die Active Defense Maßnahme lediglich die Infrastruktur des kompromittierten Systems stört, stellt sich die Frage der Geeignetheit. Ist der Angriff im Wesentlichen abgeschlossen und kann er jederzeit über einen anderen kompromittierten Rechner wiederholt werden, wird die Active Defense mangels Eignung zur Abwehr nicht rechtfertigend. Die Maßnahme wäre dann ihrerseits rechtswidriger Angriff und könnte bestraft werden. Im Rahmen der Verpflichtung zur Wahl eines angemessenen Verteidigungsmittels sind die bereits dargelegten Erwägungen im Hinblick darauf anzustellen, ob und in welcher Form der Betreiber des kompromittierten Rechners dafür (mit-) verantwortlich ist, dass sein Rechner für den Angriff ausgenutzt wurde.

Ein krasses, zum Ausschluss der Notwehr durch Active Defense führendes Missverhältnis könnte schließlich vorliegen, wenn zur Abwehr eines Diebstahls unbedeutender Daten eine komplexe Infrastruktur ggf. von allgemeiner Bedeutung zerstört wird.

3 Staatliches Hacking – Neue Online-Ermittlungsinstrumente

Zu einer anderen Form des Hackings der Unternehmens-IT kann es im Rahmen strafrechtlicher Ermittlung kommen, wenn gegen das Unternehmen selbst oder einzelne Mitarbeiter in Verdacht geraten und die Strafverfolgungsbehörden Gebrauch von den 2017 eingeführten neuen Online-Ermittlungsmethoden, der Quellen TKÜ und der Online Durchsuchung, machen.

3.1 Quellen-TKÜ

Während die herkömmliche Telekommunikationsüberwachung (TKÜ) nach § 100a Abs. 1 S. 1 StPO, soweit es um das Abhören von Telefonaten, das Mitlesen von SMS und dergleichen geht, grundsätzlich völlig ausreicht, stoßen die Behörden derzeit im Bereich der Messenger-Kommunikation über soziale Netzwerke oder auch der Internet-Telefonie schnell an seine Grenzen (so auch BT-Drs. 18/12785, S. 51), die nach dem Stand der Technik auch von Strafverfolgungsbehörden nicht umgangen werden kann. Hier kommt die sog. „Quellen-TKÜ" ins Spiel: Anders als die herkömmliche TKÜ ermöglicht sie es, **Kommunikationsinhalte** abzufangen und auszuleiten, *bevor* sie vom informationstechnischen Gerät ihres Absenders verschlüsselt und verschickt werden. Gleiches gilt für das Gerät des Empfängers, wo die Kommunikationsinhalte wieder entschlüsselt dargestellt und gespeichert werden. Ungeachtet aller Verschlüsselungsbemühungen sind für die Ermittlungsbehörden dadurch sämtliche Inhalte darstell- und abgreifbar.

Allerdings tangiert dieser Eingriff nicht lediglich das **Fernmeldegeheimnis** gem. Art. 10 GG tangiert (vgl. Schiemann 2017, S. 341), sondern infiltriert das informationstechnische System des Betroffenen und greift somit in sein Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme gem. Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG (vgl. BVerfGE 120, 274) ein. Schwer zu leugnen ist zudem ein Widerspruch zwischen der etwa in § 3 Abs. 1 S. 1 BSIG niedergelegten Verpflichtung des Staates, auf die Förderung der Sicherheit informationstechnischer Systeme hinzuwirken, und seinem in Konsequenz strafverfolgungsbehördlicher Kompetenzen wie der Quellen-TKÜ notwendig gegebenen Interesse daran, **Sicherheitslücken** in ebendiesen Systemen offenzuhalten, die behördliche Infiltration erst ermöglichen (Roggan 2017, S. 829).

Gem. § 100a Abs. 1 S. 2 StPO ist die die Quellen-TKÜ zulässig, wenn bestimmte Tatsachen den Verdacht einer schweren Straftat i.S.d. Abs. 2 begründen, die auch im Einzelfall schwer wiegt, und die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsorts des Beschuldigten auf andere Weise wesentlich erschwert oder aussichtslos wäre. Die Qualifikation einer Tat als „schwer" i.S.d. § 100a Abs. 2 StPO sieht das BVerfG mit Blick auf die mittels des jeweiligen Straftatbestands geschützten Rechtsgüter wie etwa die Funktionsfähigkeit des Staates oder seiner Einrichtungen als vom Gestaltungsspielraum des Gesetzgebers umfasst (BVerfG NJW 2011, 833, 836). Unter Verweis auf das Fehlen einer plausiblen dogmatischen Struktur wird der Anlasstatenkatalog nichtsdestoweniger teils als „partiell unverhältnismäßig" bezeichnet (Eschelbach 2017, § 100a Rn. 10).

Zur Anordnung der Quellen-TKÜ ist gem. § 100e Abs. 1 S. 1 StPO grundsätzlich nur das zuständige Gericht, gem. Abs. 1 S. 2 bei Gefahr im Verzug jedoch auch die Staatsanwaltschaft befugt. Jede geschaffene Zugriffsmöglichkeit ist gem. § 100a Abs. 5 S. 1 StPO so zu beschränken, dass nur die kommunikationsbezogenen Inhalte erfasst werden *können*, die nach der Ratio des § 100a StPO erfasst werden *sollen*. Vorgenommene Änderungen sind nach Beendigung der Maßnahme – soweit technisch möglich – automatisiert wieder rückgängig zu machen. Ebenso auf den

state of the art beschränkt ist die von Abs. 5 S. 2 statuierte Pflicht zum Schutz des eingesetzten Programms gegen unbefugte Nutzung und Kenntnisnahme durch Dritte. Schon die Formulierung „nach dem Stand des technisch Möglichen" erkennt dabei an, dass geöffnete Sicherheitslücken den Betroffenen unter Umständen durchaus auch dem erhöhten Risiko eines solchen unbefugten Eindringens – bspw. durch Kriminelle – aussetzen können.

3.2 Online-Durchsuchung

2017 wurde auch die Online-Durchsuchung mit § 100b StPO § 100b n.F. eingeführt. Nach der Legaldefinition des § 100b Abs. 1 S. 1 erfolgt sie durch Eingriff in ein und Datenentnahme aus einem informationstechnischen System mit technischen Mitteln ohne Wissen des Betroffenen. Über den auf kommunikationsbezogene Inhalte beschränkten Rahmen der Quellen-TKÜ geht sie bei technisch nahezu identischem Vorgehen hinaus und erfasst „alle auf einem IT-System gespeicherten Inhalte", also „gespeicherte Mails unabhängig vom Zeitpunkt ihres Empfangs, SMS- und WhatsApp-Nachrichten, Fotodateien, Social-Media-Kontakte etc." (Roggan 2017, S. 825).

Die materiellen Eingriffsvoraussetzungen des § 100b Abs. 1 entsprechen denen der Quellen-TKÜ. Den Anlasstatenkatalog des § 100b Abs. 2 indes teilt die Online-Durchsuchung gem. § 100c Abs. 1 Nr. 1 mit dem großen Lauschangriff, der akustischen Wohnraumüberwachung. Diese Parallelität erklärt sich daraus, dass die Online-Durchsuchung in das **Grundrecht des Betroffenen auf Integrität und Vertraulichkeit informationstechnischer Systeme** gem. Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG eingreift (Graf 2018, § 100b Rn. 8) und in ihrer Eingriffsintensität insofern der Wohnraumüberwachung gleichkommt (BT-Drs. 18/12785, S. 54 unter Verweis auf BVerfG, Urt. v. 27.02.2008 – 1 BvR 370/07, Rn. 200; Eschelbach 2017, § 100b Rn. 3). Der Anlasstaten-Katalog setzt sich dabei zusammen aus Taten, die mit Blick auf betroffenes Rechtsgut und angedrohte Strafe besonders schwer wiegen, aber auch aus solchen, deren Verfolgung typischerweise größeren Schwierigkeiten in der Beschaffung belastbarer Beweise begegnet (Eschelbach 2017 § 100b Rn. 11). Die Online-Durchsuchung ist technisch zu beschränken und zu protokollieren.

Wenngleich sich die Online-Durchsuchung gem. § 100b Abs. 3 S. 1 nur gegen den Beschuldigten richten darf, können auch hier Dritte betroffen sein. Dies zum einen, wenn bestimmte Tatsachen nahelegen, dass der Beschuldigte ein ihnen gehörendes informationstechnisches System nutzt oder ein Eingriff in dessen informationstechnisches System nicht ausreicht (Abs. 3 S. 2). Zum anderen aber können Dritte im Rahmen einer zulässigen Maßnahme gem. § 100b Abs. 3 S. 3 auch betroffen sein, wenn dies „unvermeidbar" ist. Wenngleich die Unvermeidbarkeit im Einzelfall zu prüfen ist (Graf 2018, § 100b Rn. 24), kann die Online-Durchsuchung daher auch Informationen vollständig unbeteiligter Dritter erfassen, die mit einem Beschuldigten in Kontakt stehen (Soiné 2018, S. 502). Richtet sich die Maßnahme gegen einen Mitarbeiter des Unternehmens, können bspw. Inhaltsinformationen aus

der Kommunikation mit anderen Mitarbeitern, Kunden und Geschäftspartnern betroffen sein.

Technisch ohne weiteres möglich ist es zudem, mittels eines nun ebenfalls rechtlich zulässigerweise einsetzbaren „**Keyloggers**“ (sog. „Bundestrojaner“) die ggf. erforderlichen Passwörter auszuspähen, um ohne Kenntnis des Betroffenen dessen Kommunikation zu übernehmen. Für Kommunikationspartner gibt es dabei – abgesehen vom Rückgriff auf klassische analoge Techniken wie den Einsatz von Sprachcodes o. ä. – praktisch keine Möglichkeit, festzustellen, mit wem sie wirklich kommunizieren. Für Unternehmen entsteht damit ein Spannungsverhältnis gegenüber der Verpflichtung, personenbezogene Daten und geheimhaltungsbedürftige Informationen wirksam zu schützen.

4 Digitale Beweise

Wenn Unternehmen auf Beschuldigten- oder Verletztenseite Gegenstand einer strafrechtlichen Ermittlung werden, wird es wichtig, digitale Informationen in einer beweisfähigen Form speichern. Sowohl wenn diese zur Entlastung dienen sollen, als auch dann, wenn sie (i. d. R. nach vorheriger unternehmensinterner Untersuchung) den Ermittlungsbehörden zur Verfügung gestellt werden sollen, um im Wege der Kooperation eine Milderung von drohenden Sanktionen zu erreichen (Momsen 2015, S. 1234 ff.; Momsen und Tween 2015, S. 1027 ff.; Momsen und Savic, 2017; Momsen und Grützner, 2017, S. 242 ff.). Zudem müssen die digitalen Informationen so gespeichert und gesichert werden, dass die Geschäftstätigkeit auch für den Fall der Beschlagnahme von Teilen der IT-Infrastruktur und Datenträgern möglichst weitergeführt werden kann.

4.1 Charakteristika digitaler Beweise

Digitale Daten können in diesem Sinne nicht unmittelbar als Beweis erhoben werden, da der durch sie verkörperte Inhalt nicht unmittelbar wahrnehmbar ist. Sie lassen sich auch nicht mit dem Urkundenbeweis vergleichen. Da sie anders als Schriftsprache nicht für jedermann verständliche Chiffren darstellen, bedürfen sie der Vermittlung. Dies aber begründet das Risiko einer Informationsselektion und damit zugleich der Interpretation und Reduktion.

Der für digitale Daten notwendige **Umwandlungsprozess** in ein prozessual verwendbares Beweismittel birgt ein ganz vergleichbares **Interpretations- und Reduktionspotenzial**. Erfolgt die Umwandlung zum Beweismittel durch automatisierte Prozesse, so steht das Reduktionsproblem im Vordergrund, der drohende Beweisverlust. Erfolgt die Umwandlung durch menschliche Interpretationsprozesse, so überwiegt das Risiko der Manipulation des Beweisinhalts. Dies gilt für einerseits für die Behandlung zu Beweiszwecken gesicherter digitaler Daten durch die Strafverfol-

gungsbehörden. Andererseits können wie vorstehend beschrieben zu Beweiszwecken gesicherte Daten ohne weiteres Ziel von Hacking-Attacken werden.

4.2 Bedeutung digitaler Beweismittel

Digitale Beweismittel werden bereits gegenwärtig wohl in der Mehrzahl aller nicht auf Zeugenaussagen hinauslaufenden Beweisantritte verwendet (vgl. bereits Endicott-Popovsky und Frincke 2007, S. 364 ff.). Inhalte und Informationen werden zusätzlich, zunehmend aber auch ausschließlich, digital erstellt und verbreitet. Geschäfte werden online getätigt; EDV-Systeme finden sich in nahezu allen Unternehmen. Textdokumente sowie Foto-, Video- und Audioaufnahmen werden mittlerweile überwiegend digital erstellt und gespeichert. Dabei kommt es zu einem erheblichen Anschwellen des Datenvolumens wie auch der an dem Informationsaustausch beteiligten Geräte. Das „Internet der Dinge", also die Einbindung vieler nicht primär zur Kommunikation dienender Geräte, wie bspw. Autos oder „smarte" Haushaltsgeräte, führen zu einer unübersehbaren Zahl und Verschiedenheit möglicher Informationsquellen über das Verhalten individueller Personen. Diese Informationsflut muss über algorithmenbasierte sog. „Big Data" – Konzepte gefiltert und effektiv handhabbar gemacht werden. Zudem führen Cloudspeicherkonzepte dazu, dass auf Daten von diversen Endgeräten ggf. diverser Nutzer zugegriffen werden kann, d. h. auch Veränderungen vorgenommen werden können. Die Zunahme digitaler Informationen geht zwangsläufig einher mit der steigenden Bedeutung digitaler Beweismittel. Alibis können verifiziert oder falsifiziert werden, Beweggründe lassen sich möglicherweise nachvollziehen und Verbindungen zwischen Personen können ebenfalls nachvollzogen werden.

Digitale Daten besitzen ein erhebliches Potenzial, verschiedene Kommunikationsformen zu verändern (dazu mit diversen Beispielen: Rudolph 2013). Da der Strafprozess natürlich nichts anderes als eine spezifische Kommunikationsplattform darstellt (Wassermann 1996, Einl. II, Rn. 10 ff.), wirken sich diese Veränderungen auch hier aus. Nicht nur in komplexeren Strafverfahren ist einerseits die Auswertung von E-Mails und Kommunikationsdaten sog. „social networks" zum zentralen Gegenstand der Beweisaufnahme geworden und andererseits erfolgt in erheblichem Umfang die erstmalige Erhebung derartiger Beweise nicht durch die Strafverfolgungsbehörden selbst sondern im Rahmen interner Ermittlungen durch die betroffenen Unternehmen nach den Vorgaben ihrer IT-/Data-Compliance (Die Polizei Hannover hat bspw. ein Pilotprojekt „Facebook-Fahndung" gestartet, http://www.handelsblatt.com/politik/deutschland/pilotprojekt-wie-die-polizei-in-hannover-nach-zeugen-sucht/7382618.html). Die Auswertung der gesicherten Daten wird ebenfalls mangels eigener Ressourcen nicht selten auf private Dienstleister ausgelagert.

Gleichwohl wird man sich aus der Perspektive des Verfahrensrechts dieselben grundlegenden Fragen stellen müssen, wie bei nicht-digitalen (Das Gegenstück zu digitalen Beweismitteln sind insoweit nicht allein die analogen Beweismittel, sondern auch alle weiteren Beweismittel, denen keine Perpetuierung von Informationen

zugrunde liegt (Zeugen, sonstige Einlassungen von natürlichen Personen)) Beweismitteln. Neben den rechtlichen Rahmenbedingungen der Beweiserhebung und Beweisverwertung sind dies namentlich Fragen nach Wert und Qualität des Beweismittels sowie die Reichweite des Beweises. Wie ein DNA-Identifizierungsmuster kann auch eine Funkzellenortung nur bestimmte Fakten belegen: Ein Endgerät war in einem bestimmten Bezirk zu einer bestimmten Zeit aktiv.

4.3 Kontextualisierung und Fehlinterpretation

Gleichwohl weisen digitale Beweismittel einige Besonderheiten auf, die im Strafverfahren zu berücksichtigen sind. Bedingt durch die digitale Form der gespeicherten Informationen besteht die Möglichkeit, diese relativ einfach und in vielerlei Hinsicht zu verändern (Gercke 2012, S. 713). Es ist jedermann ohne größere Schwierigkeiten möglich, mit einem Computer erstellte Texte zu verändern oder Bilder und Videos zu bearbeiten. Die entsprechenden Programme sind zum Teil kostenlos erhältlich und bieten Möglichkeiten der nachträglichen Veränderung, die bei einem handschriftlich erstellten Dokument oder einem von einem Negativ entwickelten Foto jedenfalls nicht so einfach möglich wären. Damit entsteht ein spezifischer Unsicherheitsfaktor in Bezug auf die Richtigkeit einer Tatsache, die mit der jeweiligen Datei nachgewiesen werden soll. Probleme kann auch die Zuordnung digitaler Informationen zu einer Person bereiten.

Wird beispielsweise ein zur Begehung eines Cybercrimes verwendeter Computer in einem Unternehmen von mehreren Mitarbeitern benutzt, bereitet die Beantwortung der Frage nach der Täterschaft unter Umständen erhebliche Schwierigkeiten (vgl. Casey 2002, S. 2; Chaski 2005, S. 1 ff.). Richtigerweise gründet die Rechtsprechung bei Delikten mit Internetbezug einen hinreichenden Tatverdacht gegen den Anschlussinhaber nicht allein auf die Zuordnung zu seiner IP-Adresse. Denn die konkrete Täterschaft einer bestimmten Person kann so gerade nicht festgestellt werden (vgl. LG Karlsruhe MMR 2010, 68; LG Köln, Beschl. v. 20.10 2008 – 106-5/08, juris; MMR 2009, 291; LG Saarbrücken K&R 2008, 320; zumeist Akteneinsichtsgesuche betreffende Fälle). Die Schwierigkeiten erhöhen sich nochmals, wenn die Nutzer eine unter dem Aspekt der IT-Sicherheit vielfach und dringend angeratene Anonymisierungssoftware verwenden (s.o. 1), was eine systematische Entwertung des digitalen Beweismittels zur Folge haben kann (Meier 2012, S. 198).

Weiterhin liegt die erstmalige Beweiserhebung, teilweise sogar die „Schaffung" des digitalen Beweismittels (zum Vorgang der **Beweisschaffung** (evidence creation/fabricating the evidence) Marshall 2008, S. 55 ff.) häufig nicht in der Hand der Strafverfolgungsbehörden. Das begründet ein komplexeres und weniger offensichtliches, gleichwohl aber signifikant erhöhtes Risiko im Hinblick auf Manipulation und Verlust von beweisrelevanten Informationen, als bei den meisten herkömmlichen Beweismitteln (vgl. dazu Geschonneck 2004, S. 243 ff.). In der Auswirkung vergleichbar besteht das Problem, dass die Verfahrensbeteiligten im Bereich der digitalen Beweismittel häufig mit einem so hohen Datenvolumen konfrontiert werden, dass bereits früh im Ermittlungsverfahren ein Selektionsvorgang im Sinne einer

Reduktion auf verfahrenswesentliche Informationen stattfinden muss, in der Regel auf Seiten der Ermittlungsbehörden. Dieser Schritt muss für die übrigen Verfahrensbeteiligten, soweit Ihnen ein Akteneinsichtsrecht zusteht, nachvollziehbar und überprüfbar sein. Freilich scheitert dies in der Praxis häufig an zwei Umständen: Das Volumen der Rohdaten kann die Datenverarbeitungskapazitäten der Verteidigung überfordern. Auch die Ermittlungsbehörden selbst stehen vor erheblichen Schwierigkeiten. Bislang gibt es auf Seiten der Ermittlungsbehörden auch kaum elaborierte und nachvollziehbare Instrumente zum Umgang mit „Big Data", die Auswahl erfolgt i.d.R. nach subjektiven Kriterien, was eine Rekonstruktion dieses für die Beweisaufnahme konstitutiven Vorgangs stark erschwert.

Eine weitere Besonderheit besteht in dem bereits angesprochenen Umstand, dass die digitale Datei, wie auch bereits das digitale Datum selbst, von ganz wenigen besonderen Konstellationen abgesehen, ein für den nach den Prinzipien der Mündlichkeit und Unmittelbarkeit zu führenden Strafprozess völlig untaugliches Beweismittel ist. Denn digitale Daten müssen zwingend im Wege eines Transformations- und Bearbeitungsprozesses visualisierbar oder auf andere Weise wahrnehmbar gemacht werden. Dieser Bearbeitungsprozess ist evident ein für ein Beweismittel äußert kritischer Umstand. Denn Bearbeitung ist nichts anderes als Manipulation (in einem wertneutralen Sinne); u. U. könnte man sogar von der „Herstellung" des Beweismittels i.e.S. sprechen. Beide Begriffe sind aus der Perspektive des Verfahrensrechts im Zusammenhang mit Beweismitteln außerordentlich problematische Begriffe.

4.4 Digitale Daten und Beweismittelstandards

Die beschlagnahmte DVD oder Festplatte ist lediglich ein Augenscheinsobjekt und hat keinen über das Faktum seiner Existenz hinausgehend Beweiswert. Selbst die Umstände seiner Auffindung sind i.d.R. dem Zeugenbeweis vorbehalten. Die digitalisierte bzw. digital gespeicherte Information bedarf der Bearbeitung, um als Beweismittel im Strafprozess verwendbar zu sein (s.o. 2.2). Für das digitale Beweismittel weist dieser Bearbeitungsvorgang jedoch eine entscheidende Besonderheit auf: Die verwertbar gemachte Information verbleibt stets im Kontext ihrer digitalen Speicherung.

Als Beispiel: Die ausgedruckte E-Mail ähnelt dem herkömmlich entwickelten Foto darin, dass in beiden Fällen durch einen technischen Prozess ein Augenscheinsobjekt (ggf. eine Urkunde) entsteht. Bzgl. der Authentizität des Beweismittels kommt es primär darauf an, dass der Umwandlungsprozess (digitale Daten zu lesbarerem Text, Negativ zu belichtungs- und farbgetreuem Bild (dargestellt mit Manipulations- bzw. Verzerrungsgefahren bei Marshall 2008, 75 ff.)) technisch einwandfrei abläuft. Zum Beweis dafür wäre die Person, welche die Verarbeitung vorgenommen hat, als Zeuge, ggf. auch ein Sachverständiger heranzuziehen. Im Falle der Textdatei jedoch stehen bei regulären Abläufen weiterhin die Roh- und Metadaten zur Verfügung (folgend vereinfachend als „Kontextdaten" bezeichnet (angelehnt an „data context", vgl. Marshall 2008, S. 83 in Abgrenzung zu den Daten selbst bzw. dem durch sie verkörperten Informationsgehalt („data content", a.a.O. S. 69 ff.)).

Ohne diese ist ein aussagekräftiger Authentizitätsnachweis nicht zu führen. Sie müssen also gleichsam immer im Hintergrund der „wahrnehmbar“ gemachten Information, welche das Beweismittel i.e.S. darstellt, mit erhoben werden. Damit entsteht ein Bedürfnis nach Standards der Beweiseignung auch für diese Kontextdaten (Überblick bei Casey 2002, S. 25 ff.; Geschonneck 2004, S. 64 ff.; Rowlingson 2014, S. 11 ff.); dazu sogleich. Wenn die Kontextdaten aber ihrerseits mittelbar beweisrelevant sind, fragt sich weitergehend, ob und wie weit deren Authentizität überprüfbar ist bzw. sein muss.

5 „Forensic Readiness“ und Digital Compliance

5.1 Begriff

Der im Common Law verwendete Begriff der „Forensic Readiness“ deckt sich zwar in der Übersetzung (Gerichts- oder Prozessbereitschaft) nicht vollständig, dürfte aber im hier relevanten Kontext mit „Beweiseignung und -qualität“ zutreffend erfasst sein. „Forensic Readiness“ hat einen weitergehenden, proaktiven Gehalt in dem Sinne, dass Informationen so erstellt, gesammelt, archiviert und dokumentiert werden, dass sie im hypothetischen Falle eines späteren Verfahrens verwertbar sind. Hintergrund ist u.a. das Bestreben der mit diesem Vorgang befassten Personen oder Institutionen, sicherzustellen, dass die ihnen obliegenden Sorgfaltspflichten bei der Implementierung von Prozessabläufen eingehalten wurden und insoweit keine Verantwortlichkeit für Fehler besteht. „Forensic Readiness is defined as the ability of an organisation to maximise its potential to use digital evidence whilst minimising the costs of an investigation“.[9] „Forensic Readiness“ passt damit primär in den Rahmen der präventiven Compliance, die eng mit strafverfahrensrechtlichen Aspekten verknüpft ist (ausf. zu den Zielsetzungen von Compliance Bock 2011, S. 19 ff.; Rotsch 2013, 3 ff.).

5.2 Standards des Beweiswerts

Wenn auch in einem nicht strafverfahrensspezifischen Rahmen, werden mit „Forensic Readiness“ Voraussetzungen festgelegt, deren Einhaltung den Beweiswert der präsentierten Informationen deutlich erhöht. Auch für deutsche Strafverfahren hilfreich sind die im Common Law maßgeblichen sog. „Daubert-Criteria“ (Daubert v.

[9] Rowlingson 2014, 1: „A forensic investigation of digital evidence is commonly employed as a post event response to a serious information security incident. In fact, there are many circumstances where a organization may benefit from an ability to gather and preserve digital evidence before an incident occurs“ (a.a.O.). Tan (Fn.1), S. 1 definiert wie folgt: „Forensic Readiness“ has two objectives: „Maximalizing an environments ability to collect credible digital evidence; and 2. Minimalizing the costs of forensics in an incident response“.

Merrell Dow Pharmaceuticals, Inc., 509 U.S. 579 (1993), zum Fall in National Research Council 2009, S. 90): In Ermangelung eines spezifisches Tests, der verwendet werden könne, um zu bestimmen, ob (digitale) Beweise die erforderliche wissenschaftliche Qualität aufweisen, schlug der US Supreme-Court 1993 in der Daubert-Entscheidung (Daubert v. Merrell Dow Pharmaceuticals, Inc., 509 U.S. 579 (1993), S. 593 ff.) vor, dass jeweils mehrere Faktoren berücksichtigt (Casey 2002, S. 73 ff.; Ryan und Shpantzer 2008, S. 2) werden sollten, um falsch positive Ergebnisse zu vermeiden (Ausführliche Analyse bei National Research Council 2009, S. 90 ff. mit Verweis auf die Kommentierung zur Fed. R. Evid. 702 Verweis auf General Electric, 522 U.S. (at 146): „that there is simply too great an analytical gap between the data and the opinion proffered"):

Diese Faktoren sind nicht erschöpfend und stellen keine Checkliste oder abschließenden Bewertungsmaßstab im Sinne eines „endgültigen Tests" dar (Daubert v. Merrell Dow Pharmaceuticals, Inc., 509 U.S. 579 (1993), S. 593 ff.). Die Daubert-Rechtsprechung stellt sich als Weiterentwicklung der tradierten Frye-Entscheidung des „District of Columbia Court of Appeals" aus dem Jahr 1923 zum Umgang mit „scientific evidence" dar, welche die Anforderungen an wissenschaftliche Sachverständige bis heute umreißt[10] (Erfahrung, Ausbildung, Verankerung in allgemein anerkannten Methoden und Verfahren; vgl. Frye v. United States, 54 App. D. C. 46, 293 F. 1013 (1923)). Diese Kriterien lassen sich ohne weiteres mit den Grundsätzen des Sachverständigenbeweises in § 244 Abs. 4 StPO in Einklang bringen (vgl. Meyer-Goßner 2018, § 244 Rn. 75).

Im Strafverfahren können diese Kriterien in zweifacher Hinsicht relevant werden. Zum einen könnte das digitale Beweismittel so präsentiert werden, dass bereits bei seiner Einführung in das Verfahren dargelegt wird, dass die Datenerhebung den genannten Voraussetzungen entsprechend erfolgte. Das wäre die mit „Forensic Readiness" verbundene Idealvorstellung. Um ein digitales Beweismittel effektiv auf seinen Beweiswert überprüfen zu können, ist es allerdings unumgänglich, die potenziellen Schwachstellen zu kennen. Denn der entsprechende Beweisantrag muss den Voraussetzungen des § 219 S. 1 StPO sowie der höchstrichterlichen Rechtsprechung genügend konkretisiert werden (BGHSt 1, 29 (31); 6, 128 (129); StV 2000, 180; Meyer-Goßner 2018, § 244 Rn. 18 ff.; Sättele 2017, § 244 Rn. 82 ff.).

Angesichts der oben dargelegten Spezifika digitaler Beweismittel ist zunächst einmal die Entstehungsgeschichte des Beweises von Interesse. Strafprozessual relevante Beweise entstehen i.d.R. im Zusammenhang mit Vorfällen, also jeder – auch firmeninternen – Straftat. Nach einem entsprechenden Vorfall entstehen Beweise häufig an verschiedenen Orten und in unterschiedlichen Formen. Nur einige Orte sind zu Beginn der Ermittlungen bekannt. Digitale Beweise können bspw. in verschiedenen Medien gespeichert sein, seien dies körperliche Speichermedien wie

[10] National Research Council 2009, 93 (m.w.N.) – „… that an expert´s testimony is reliable where the discipline itself lacks reliability (…)". Dies ist mit Blick auf die Zulassung von Sachverständigen angesichts der sich rasch entwickelnden Bereiche der „Digitalen Forensik" von nicht zu unterschätzender Bedeutung. Ggf. wird hierin ein Grund für einen weiteren Sachverständigen i.S. § 244 Abs. 4 StPO liegen können.

DVDs oder Festplatten oder unkörperliche, wie soziale Netzwerke oder die Cloudspeicherung. Häufig setzt sich das vollständige Bild erst bei einem Abgleich verschiedener Speicherorte einer Information zusammen (ausführlich mit Bsp. Marshall 2008, S. 19 ff., 85 ff.).

5.3 Integrität, Authentizität, Reproduzierbarkeit

Abhängig vom Ort der Speicherung sowie dem Wissen um mögliche weitere Speicherorte lassen sich Aussagen zur Integrität und Authentizität des digitalen Beweismittels treffen. „Integrität" bedeutet, dass Beweise „unverändert" sein und bleiben müssen. Der Integritätsgrad sollte so hoch wie möglich sein. Zweifel können sich zum Beispiel ergeben, wenn die Beweiserhebung nicht von Strafverfolgungsbehörden durchgeführt wurde oder wenn die Datenmenge drastisch reduziert wurde (Marshall 2008, S. 19 ff., 43 ff.). In beiden Fällen stellt sich die Frage nach der Vorlage der Rohdaten um überprüfen zu können, ob eine Korruption oder Kontamination der Daten erfolgt sein kann (Marshall 2008, S. 40 ff.). Authentizität bedeutet, dass das Beweismittel unmittelbar das(selbe) ist, welches ursprünglich gewonnen wurde. Hier können Probleme auftreten, wenn digitale Daten vor oder auch nach der Beweisgewinnung auf andere Medien oder an andere Orte umgespeichert wurden. Zwar verliert das Beweismittel damit nicht zwangsläufig an Qualität, jedoch wird man häufig Kontextdaten (Meta- oder Rohdaten) im o.g. Sinn heranziehen müssen, um die Authentizität gewährleisten zu können. Geht die Integrität verloren oder der unterschreitet der Grad der Integrität ein bestimmtes Niveau, so sind Schlussfolgerungen nur noch sehr beschränkt möglich. Ähnliches gilt für die Authentizität; auch die Gewährleistung dieses Kriteriums hängt von der Möglichkeit ab, die Herkunft von Informationen zu identifizieren. Dies macht die Auswertung derivativer Informationen bzw. kontextualen Daten notwendig. Bestehen bspw. Anhaltspunkte dafür, dass eine Festplatte „gesäubert" wurde, so wird neben der Kopie der Festplatte auch der Flash-Speicher-Cache auf der Festplatte beweiserheblich sein.

Weiterhin muss das digitale Beweismittel reproduzierbar sein. „Reproduzierbarkeit" meint Nachvollziehbarkeit im Sinne einer ableitbaren logischen Kette komplexer Beweise bzw. Informationen aus einfacheren Beweisen bzw. Daten. In enger Verbindung hierzu steht die Überprüfbarkeit i.S. der internen Konsistenz des digitalen Beweismittels: Beweisstücke, die ihrer Natur nach manipulationsanfällig sind (wie viele gespeicherte Daten), erlangen einen höheren Beweiswert, wenn parallele Beweisstränge vorhanden sind, die insgesamt im Einklang miteinander stehen. Ist eine Information bspw. an verschiedenen voneinander unabhängigen Speicherorten identisch gespeichert, so spricht dies für einen hohen Beweiswert, da es unwahrscheinlich ist, dass alle Speicherorte gleichzeitig manipuliert worden sind. Nimmt man als Beispiel ein Dokument, welches auf einer Plattform von mehreren Nutzern gleichzeitig bearbeitet werden konnte (bspw. „Google-Drive") so steigt der Beweiswert, wenn verschiedene Nutzer das Dokument in identischer Weise auf ihren Endgeräten abgespeichert haben. Zu berücksichtigen sind weiterhin mögliche End-

nutzungen durch Geräte oder Personen (Entities), die Umgebung, Beschränkungen und Kontrollen (Environment), Organisation der relevanten IT (Organisation), Infrastruktur von Gebäuden, Netzwerken etc. (Infrastructure), Arbeitsabläufe (Activities), (Daten-) Verarbeitungsprozesse (Procedures) und die Daten (Data) selbst (anhand des „Seven-Element Security Models“ von Marshall, 2008, S. 56 ff.).

Der durch die vorgenannten Kriterien umschriebene Beweiswert lässt sich relativ gut in Kategorien einteilen, wie dies bspw. *Casey* mit den von ihm entwickelten „Levels of Certainty“ aufgezeigt hat (Casey, http://flylib.com/books/en/2.57.1.74/1/ – „Levels of Certainty“; vgl. auch Casey 2002, S. 70). Angemerkt sei, dass sich die aufgezeigte Problematik verschärft, wenn die digitalen Beweismittel ursprünglich im Rahmen einer unternehmensinternen Ermittlung erhoben wurden. Denn diese folgt als private Ermittlung nur sehr begrenzt strafprozessualen Grundsätzen (ausf. Momsen 2014 § 6 B II 2 a).

5.4 Einhaltung und Dokumentation von IT-Forensik-Standards

Hat bspw. ein Unternehmen zunächst selbst eine Untersuchung durchgeführt, so werden daraus hervorgehende Beweismittel in ihrer Qualität wesentlich davon abhängig sein, ob die Standards der IT-Forensik eingehalten wurden. Gleiches gilt natürlich für externe IT-Services, welche von den Strafverfolgungsbehörden mit der Beweissicherung und -auswertung beauftragt werden. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat in einem Leitfaden die Anforderungen an einen forensischen Ermittlungsprozess im IT-Bereich zusammengefasst, die im Wesentlichen den bereits dargestellten Besonderheiten digitaler Beweismittel Rechnung tragen (diese Vorgaben sind allerdings technisch gesehen zu relativieren, näher Rudolph 2013; Momsen und Hercher 2014, S. 173 ff.) und in methodischer Hinsicht den „Daubert-Standards“ vergleichbar sind. Verlangt wird eine Akzeptanz der angewandten Methoden und Schritte; diese müssen in der Fachwelt beschrieben und allgemein anerkannt sein. Bei der Anwendung neuer Methoden ist deren Korrektheit nachzuweisen. Um eine Glaubwürdigkeit zu gewährleisten muss, die Robustheit und Funktionalität von Methoden nachweisbar gegeben sein. Eine Wiederholbarkeit muss möglich sein. Bedienen sich Dritte der eingesetzten Hilfsmittel und Methoden, so müssen bei dem gleichen Ausgangsmaterial dieselben Ergebnisse erzielt werden. Sichergestellte digitale Beweise dürfen nicht unbemerkt durch die Untersuchung selbst verändert werden. Die Sicherung der Integrität muss belegbar sein. Durch die Auswahl der Methoden muss es möglich sein, logisch nachvollziehbare Verbindungen zwischen Ereignissen und Beweisspuren und auch zu Personen herzustellen; nur so können Ursache und Auswirkung miteinander verknüpft werden. Schließlich muss für jeden einzelnen Schritt des Ermittlungsprozesses eine lückenlose Dokumentation erstellt werden. Zusätzlich bedarf es eines lückenlosen Nachweises über den Verbleib von digitalen Spuren und der Ergebnisse der daran vorgenommenen Untersuchungen, also der Nachverfolgbarkeit der im englisch-

sprachigen Raum bekannten „Chain of Custody“ (Leitfaden IT-Forensik (Fn. 47), S. 24, S. 87 ff.; vgl. auch Casey 2002, 21 f.). Denn der häufigste Ansatzpunkt, die Qualität des digitalen Beweismittels in Zweifel zu ziehen, ist eine lückenhafte oder fehlende Dokumentation.

Literatur

Bock D (2011) Criminal compliance, 1. Aufl. Baden-Baden
Casey E (2002) Error, uncertainty, and loss in digital evidence. Int J Digit Evid 1(2):2 ff
Chaski C (2005) Who’s at the keyboard? – Authorship attribution in digital evidence investigations. Int J Digit Evid 4(1):1 ff
Degen A (2016) § 66. In: Heussen, Hamm (Hrsg) Beck’sches Rechtsanwalts-Handbuch, 11. Aufl. München
Dix A (2014) § 1. In: Simitis (Hrsg) Bundesdatenschutzgesetz, 8. Aufl. München
Eisele J (2013) Computer- und Medienstrafrecht. München
Eisele J, Lenckner T (2014) § 203. In: Schönke-Schröder (Hrsg), StGB, 29. Aufl., München
Endicott-Popovsky B, Frincke D (2007) In: Schmorrow DD, Reeves LM (Hrsg), Augmented cognition, HCII 2007. Berlin, S 364 ff
Eschelbach G (2017) § 100a. In: Satzger, Schluckebier, Widmaier (Hrsg) Strafprozessordnung: StPO mit GVG und EMRK, Kommentar, 3. Aufl. Köln
Fechtner S, Haßdenteufel S (2017) Die Novelle des § 203 StGB und weiterer berufsrechtlicher Normen, CR, 355 ff
Gercke M (2012) Der unterbliebene Schritt vom Computer- zum Internetstrafrecht, AnwBl, 709 ff
Geschonneck A (2004) Computer-Forensik, 1. Aufl. Heidelberg
Graf J-P (2018) § 100b. In: Graf (Hrsg) BeckOK-StPO, 31. Aufl.
Grosskopf L, Momsen C (2018) Outsourcing bei Berufsgeheimnisträgern – strafrechtliche Verpflichtung zur Compliance? CCZ 2018, 98 ff
Haft F (1987) Das Zweite Gesetz zur Bekämpfung der Wirtschaftskriminalität (2. WiKG) – Teil 2: Computerdelikte, NStZ 6 ff
Härting N (2005) IT-Sicherheit in der Anwaltskanzlei – Das Anwaltsgeheimnis im Zeitalter der Informationstechnologie, NJW, 1248 ff
Haß G (1993) Rechtsschutz und Verwertung von Computerprogrammen (Lehmann (Hrsg)), 2. Aufl. Köln
Heger M (2018) § 202a. In: Lackner K, Kühl K (Hrsg) StGB, 29. Aufl. München
Hilgendorf E (2015) Strafrecht Besonderer Teil (Arzt G, Weber U, Heinrich B, Hilgendorf E (Hrsg)), 3. Aufl. Bielefeld
Jahn M, Palm J (2011) Outsourcing in der Kanzlei: Verletzung von Privatgeheimnissen? Die straf- und berufsrechtliche Bewertung eines „Anwaltssekretariats“ außerhalb der Kanzlei, AnwBl, 613 ff
Jessen E (2014) Zugangsberechtigung und besondere Sicherung im Sinne von § 202a StGB. Frankfurt
Koch F A (2014) Rechtliche und ethische Verschlüsselungspflichten? Am Beispiel der Rechtsanwaltschaft. DuD, 691 ff
Lenckner T, Winkelbauer W (1986) Computerkriminalität – Möglichkeiten und Grenzen des 2. WiKG (I), (II), (III), CR, 483 ff., 654 ff., 824 ff
von Lewinski K (2004) Anwaltliche Schweigepflicht und E-Mail. BRAK-Mitteilungen 1:12
Marshall A M (2008) Digital forensics – digital evidence in criminal investigation
Meyer-Goßner L (2018) § 244. In: Meyer-Goßner L, Schmitt B (Hrsg) Strafprozessordnung: StPO. 61. Aufl. München