HERAUSFORDERUNGEN VERANTWORTUNGSLOSER DIGITALISIERUNG

Thomas Hrdinka

Zivilingenieur, ZTH Consulting Engineering, Dissertant, Universität Wien, Arbeitsgruppe Rechtsinformatik
Ocwirkgasse 22, 1210 Wien, AT
thrdinka@zth.at; http://www.zth.at

Schlagworte: ***Spurenbewertung, Beweismittel, IT-Forensik, Fallbeispiele***

Abstract: *Digitale Spuren weisen spezifische Besonderheiten im Gegensatz zu physischen Spuren auf. Da auch die Cyberwelt anderen Gesetzmäßigkeiten als die reale Welt unterliegt, steht die IT-Forensik vor besonderen Herausforderungen, und eine Beweissicherung erfordert hier spezielle Maßnahmen. Eine unverantwortungsvolle Nutzung der digitalen Werkzeuge bis hin zum Missbrauch hat folglich andere rechtliche Auswirkungen als entsprechende konventionelle Straftatbestände. Anhand von reellen, anonymisierten Fallbeispielen soll aufgearbeitet werden, ob die bestehenden Rechtsinstrumente im Zusammenhang mit den Besonderheiten der IT-Forensik ausreichende Möglichkeiten aufweisen.*

1. IT-Forensik

Die Forensik bildet wissenschaftliche Methoden und Techniken zur Untersuchung von Verbrechen ab. In der Kriminaltechnik wird darunter auch die Spurensicherung verstanden. Obwohl bereits früher im 17. Jahrhundert die Besonderheit von Fingerabdrücken bekannt war, wurde erst 1858 von Herschel ein standardisiertes Verfahren, der Daktyloskopie, zur eindeutigen Identifikation von natürlichen Personen eingeführt.

Die Informatik hingegen, als eine relativ junge Wissenschaft brachte erst spät vor ungefähr 20 Jahren erste forensische Methoden hervor, wie die Festplattenforensik. Handelte es sich ursprünglich um die reine Spurenanalyse auf Festplatteninhalten und anderen Medien, so entstanden im Laufe der Jahre weitere Methoden in jenen Bereichen, wo die Informatik Anwendung gefunden hat. 2011 hat erstmals Dewald[1] die «Forensische Informatik» qualifiziert als «*Die Anwendung wissenschaftlicher Methoden der Informatik auf Fragen des Rechtssystems. Insbesondere stellt die forensische Informatik Methoden zur gerichtsfesten Sicherung und Verwertung digitaler Spuren bereit.*»

Zusätzlich zu dieser Definition geht es bei der IT-Forensik um die Aufklärung von Computerkriminalität, dem deliktischen Handeln, bei dem der Computer das Werkzeug oder das Ziel der Tat ist. Wesentlich ist dabei das Erkennen der Methode oder Schwachstelle, die z.B. zu einem Systemeinbruch geführt hat. Es sollen Beweise gesichert, der Schaden ermittelt, und Angreifer identifiziert werden können. Die Anforderungen an die Glaubwürdigkeit, Wiederholbarkeit, Integrität und Dokumentation der Beweissicherung unterliegt hohen Maßstäben, denn die Gefahr, dass durch die forensische Arbeit digitale Spuren verändert oder vernichtet werden ist latent hoch. Die Beantwortung forensischer Hauptfragen verfolgt die Aufklärung der Tat, Feststellung des Tatorts, der Tatzeit, des Tathergangs und die Sicherung von Spuren. Hingegen sind die forensischen Nebenfragen insb. im Strafverfahren relevant, wie jene nach dem Täter und dem Motiv.

Die Identifikation ist daher eine wesentliche Anforderung, um sicheres Internetbanking, Shopping, e-Government, e-Health uvm. zu ermöglichen.

[1] Dewald, Freiling: Forensische Informatik, Books on Demand, 2011.

1.1. Digitale Spuren

Die Eigenschaften von physischen Spuren und der Zusammenhang mit dem Täter, Opfer und dem Tatort sind erstmals 1920 von Locard[2] beschrieben worden. Gemäß dem bekannten «Austauschprinzip» kann es keine Handlungen geben, ohne Spuren zu hinterlassen, und dem zu Folge kann niemand eine Straftat begehen, ohne zahlreiche Zeichen zu hinterlassen. Diese Spuren können eine Theorie über den Tathergang, eine Hypothese, stützen oder widerlegen. Inman[3] verfeinerte das Austauschprinzip, und stellte fest, dass ein Austausch nur dann stattfinden kann, wenn Objekte bzw. Materie sich in kleinere Teile zerteilen lassen. Die Einzelteile behalten gemäß diesem «Zerteilungsprinzip» die charakteristischen Eigenschaften des Objekts. Damit wird die Übertragung von Mustern erst ermöglicht, wie beispielsweise Kratzspuren oder Schuhabdrücke. Kirk[4] konkretisierte diesen Zusammenhang durch das Prinzip der Einzigartigkeit einer Sache, die unter anderem die Relevanz von Spuren für die Identifikation einer Person bestimmt.

Nachdem Computer und die Speichermedien auf physikalischen Gesetzmäßigkeiten aufbauen und selbst aus Materie bestehen, sind digitale Spuren zunächst als physische Spuren zu werten. Gemäß der Definition nach Casey[5] sind «Digitale Spuren» jedoch Daten, die in Computersystemen gespeichert werden. Nachdem diese Speicherung der Daten bei modernen Systemen im mikroskopisch kleinen Nanometerbereich erfolgt, sind solche Spuren für Menschen nicht oder nur sehr schwer zugänglich. Aus diesem Grund muss erst eine Aufbereitung erfolgen, die gemäß mehr oder weniger genau definierten Abstraktionsschichten erfolgt. Diese Ungenauigkeit der Spezifikation oder auch deren Fehlinterpretation ist oft nicht unproblematisch in Bezug auf die Nachvollziehbarkeit und häufig Grund für heftige Auseinandersetzungen vor Gericht.

1.2. Elektronische Beweismittel

Bei elektronischen Beweisen handelt es sich um Urkunden, wobei die Rechtsordnung folgende Varianten kennt:

1. Privaturkunde (§ 294 ZPO[6]): Auf Papier oder elektronisch errichtete Privaturkunden begründen, sofern sie von den Ausstellern unterschrieben oder mit ihrem gerichtlich oder notariell beglaubigten Handzeichen versehen sind, vollen Beweis dafür, dass die in denselben enthaltenen Erklärungen von den Ausstellern herrühren.
2. Öffentliche Urkunde (§ 292 Abs. 1 ZPO): Urkunden, welche im Geltungsbereich dieses Gesetzes von einer öffentlichen Behörde innerhalb der Grenzen ihrer Amtsbefugnisse oder von einer mit öffentlichem Glauben versehenen Person innerhalb des ihr zugewiesenen Geschäftskreises in der vorgeschriebenen Form auf Papier oder elektronisch errichtet sind (öffentliche Urkunden), begründen vollen Beweis dessen, was darin von der Behörde amtlich verfügt oder erklärt, oder von der Behörde oder der Urkundsperson bezeugt wird.

Der Gesetzgeber nennt dabei ausdrücklich elektronisch errichtete Urkunden. Über diese Neuerung gegenüber der Stammfassung geben die parlamentarischen Materialien des BRÄG 2006[7] Auskunft: «*Mit diesen Änderungen wurde auch im gerichtlichen Verfahren eine vollständige Gleichstellung der elektronischen Form mit der Papierform erreicht. Bei Privaturkunden gilt das zu § 292 Abs 1 ZPO Ausgeführte sinngemäß. Auch in der ZPO soll nun zur Klarstellung ausdrücklich normiert werden, dass auf Papier (bzw auf einem anderen beschreibbaren Stoff) oder elektronisch errichtete Privaturkunden gleiche Beweiskraft besitzen.*»

---

2 Locard: L'enquete criminelle et les methodes scientifique. Ernest Flammarion, Paris, 1920.
3 Inman, Rudin: Principles and Practice of Criminalistics: The Profession of Forensic Science. CRC Press, 2000.
4 Kirk: Crime Investigation. John Wiley & Sons, 1974.
5 Casey: Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet. Academic Press, 2011.
6 Zivilprozessordnung, RGBl. 113/1895 idgF.
7 Berufsrechts-Änderungsgesetz für Notare, Rechtsanwälte und Ziviltechniker 2006, BGBl. I 164/2005.

Da der Computer als ein deterministischer Zustandsautomat geschaffen wurde, das bedeutet, dass jede Rechenvorschrift mit selber Eingabe wiederholbar die gleiche Ausgabe produziert, ist der Zufall ausgeschlossen. Obwohl in die reale Welt eingebettet, existieren intern nur zwei abstrakte Zustände: ein Bit, die Information ist wahr oder falsch oder die Zahl 0 oder 1. Nachdem nur diese zwei diskreten Zustände existieren, terminiert die Teilbarkeit der Daten beim Bit, und das ganz im Gegensatz zu den physischen Spuren: eine Art Abdruck oder Kratzspur ist hier nicht möglich, denn Bits sind keine Materie und hinterlassen von sich aus keine Spuren. Aufgrund dieser Terminierung der Teilbarkeit sind perfekte Kopien herstellbar, und folglich existiert im Computerspeicher nie ein Original eines Datensatzes, sondern immer nur Kopien davon. Forensische Untersuchungen arbeiten daher immer mit Kopien und nie mit einem (vermeintlichen) Original. Wir dürfen jedoch sehr wohl von originären[8] Daten bzw. Kopien sprechen.

Nachdem Daten keine Materie sind, gibt es keinerlei Analogie für das Einzigartigkeits-, Zerteilungs- und Austauschprinzip, mit allen Konsequenzen: Eine Konsequenz ist die Bewertung einer Spur. Physisch werden häufig aufbauend auf Messergebnissen konkrete Prozentwerte für eine Wahrscheinlichkeit genannt. Bei Daten wäre solch eine Messung mit einer Wahrscheinlichkeitsbewertung sinnlos, und würde m.E. nach lediglich den Anschein einer Wissenschaftlichkeit vortäuschen. Casey erkannte frühzeitig diese Problematik und schlug eine diskrete Bewertung mit Berücksichtigung von Manipulationsmöglichkeiten vor von Fehlerhaft (C0) – die Spuren widersprechen Fakten oder stimmen nicht überein, bis hin zu Sicher (C6) – die Spuren waren vor Manipulationen geschützt oder haben eine hohe statistische Konfidenz.

Aufgrund der Tatsache, dass sich digitale Spuren leicht manipulieren lassen, ist eine Bewertung aufgrund des festgestellten Manipulationsschutzes, wie bspw., dass elektronische Urkunden (zumindest deren Fingerprint[9]) mittels digitaler Signatur zu signieren sind, was sich auch aus §§ 292 u. 294 ZPO ergibt, eine sehr brauchbare Lösung, um diese Spuren qualitativ zu bewerten. Auch ist die Berücksichtigung der Existenz weiterer Spuren ein sehr guter quantitativer Ansatz, solch eine Bewertung vorzunehmen.

1.3. Fallbeispiele

Die Problematik der technischen Spurensicherung- und Bewertung gegenüber der zu erwartenden rechtlichen Pönalisierung sollen folgende Beispiele aus der beruflichen Praxis des Autors verdeutlichen:

1. Ein wegen Abgabenhinterziehung (§ 33 FinStrG[10]), Abgabenbetrug (§ 39 FinStrG) und des Betrug (§ 146ff StGB[11]) gesuchter Verdächtiger hat jahrelang Identitäten gefälscht, um unter fremden Namen Einkäufe zu tätigen, oder sich Finanzdienstleistungen zu erschleichen. Die Beweise gegen den flüchtigen Tatverdächtigen wurden auf sicher gestellten Festplatten und USB-Sticks vermutet. Nachdem die Untersuchung hinsichtlich verwertbarer Beweise ergebnislos war, wurde versucht verschlüsselte Containerdateien, wo das inkriminierte Beweismaterial vermutet wurde, zu entschlüsseln. Der ausländische Hersteller dieser Verschlüsselungssoftware zeigte sich jedoch nicht kooperativ, er gab lediglich den Hinweis, dass es sich bei den Dateien um TrueCrypt «kompatible» Containerdateien handelt. Obwohl das Brechen sämtlicher vom Tatverdächtigen genutzten Windows- und Internet-Passworte zwar erfolgreich war, konnte letztlich mit Hilfe dieser Informationen, indem alle bekannten Passwortfragmente kombiniert und permutiert wurden, keine Entschlüsselung der Containerdateien erlangt werden. Auch scheiterten sämtliche Angriffe auf bekannte Schwachstellen von TrueCrypt. Nach 6 Monate dauernden Entschlüsselungsversuchen wurde aus Zeitgründen abgebrochen. Hätte man den Softwarehersteller verpflichten können, Informationen zur Verschlüsselung und Dateistruktur zu offenbaren, wäre womöglich eine Entschlüsselung erfolgreich gewesen.

[8] Hrdinka, Auf Spurensuche in der Cyberwelt – Digitale Beweise mit IT-Forensik, 45. Ottensteiner Fortbildungsseminar aus Strafrecht und Kriminologie, NWV Verlag, 2018.

[9] Auch Hashwert: eindeutiger, nicht umkehrbarer kryptographischer Extrakt von Daten.

[10] Finanzstrafgesetz BGBl. 129/1958 idgF.

[11] Strafgesetzbuch BGBl. 60/1974 idgF.

2. Ein weiterer Fall umfasste die Aufgabe, ob ein Angriff auf ein Computersystem (§ 118a StGB) des Verdächtigen nachzuweisen ist, bzw. ob noch weitere Ermittlungen nötig sind. Der Tatverdächtige soll Benutzerkonten einer konkurrierenden Internetplattform geändert und gelöscht haben. Die Untersuchung der Webserver-Protokolle ergab, dass ungewöhnliche Administrationszugänge im inkriminierten Zeitraum statt fanden, als auch sind mehrere, vermutlich erfolgreiche SQL-Injection-Angriffe nachgewiesen worden. Technischerseits konnte ein Zugriff auf den administrativen Bereich des Servers mit der verdächtigen IP-Adresse bewiesen werden. Weiters konnte auch der verwendete User mit dem zwar verschlüsselten, aber gebrochenen Passwort dem Tatverdächtigen mit seinem einzigartigen E-Mail Synonym in Übereinstimmung gebracht werden. Aufgrund des Umstandes, dass zur Zeit der Untersuchung die Frist von 6 Monaten zur damals noch geltenden Vorratsdatenspeicherung aufgrund der Verzögerungen im Rechtshilfeverfahren abgelaufen ist, und der SQL-Injection-Angriff mit einer nicht zuordenbaren IP-Adresse aus dem Ausland erfolgt ist, waren weitere Ermittlungen nicht zielführend.
3. Der letzte Fall betrifft abermals einen widerrechtlichen Zugriff auf ein Computersystem (§ 118a StGB). Der Angeklagten wurde vorgeworfen, die Inhalte eines privaten Social-Media-Accounts entwendet, und in einem Sorgerechtsstreit verwendet zu haben. Obwohl zwar die von der Angeklagten verwendeten Bilder und Screenshots optisch auf einen öffentlichen Account hinwiesen, konnte technisch zweifelsfrei festgestellt werden, dass der Account der Geschädigten tatsächlich von Beginn an privat war. Die Auflösung dieses Falles konnte erst durch das Aufrollen von Protokollen der Vergangenheit erfolgen: demzufolge wurde der private Account regelmäßig, zumeist nächstens, kurzzeitig auf öffentlich umgestellt, und wieder zurück auf privat. Die Zeitstempel der vorgelegten Beweismittel wie Screenshots stimmten mit den Zeitstempeln der Zeiten, wo auf privat geschaltet worden ist, eindeutig überein. Obwohl diese Übereinstimmung zweifelsfrei auf die Angeklagte hingewiesen hat, welche offenbar auch ein Interesse an den kopierten Daten hinsichtlich einem Motiv hatte, konnten keine weiteren technische Spuren – welche auch nicht mehr vorhanden waren – gefunden werden, was folglich in einen Freispruch mündete.

2. Rechtsdogmatische Bewertung

2.1. Cyber-Crime-Convention des Europarats

Die von Österreich ratifizierte Cyber-Crime-Convention[12] – auch Budapest Convention genannt – definiert das «*Computersystem als eine Vorrichtung oder eine Gruppe miteinander verbundener oder zusammenhängender Vorrichtungen, die einzeln oder zu mehreren auf der Grundlage eines Programms automatische Datenverarbeitung durchführen*». In Art. 2 verpflichten sich die unterzeichnenden Vertragsparteien, «*den unbefugten Zugang zu einem Computersystem als Ganzem oder zu einem Teil davon, wenn vorsätzlich begangen, nach ihrem innerstaatlichen Recht als Straftat zu umschreiben. Eine Vertragspartei kann als Voraussetzung vorsehen, dass die Straftat unter Verletzung von Sicherheitsmaßnahmen, in der Absicht, Computerdaten zu erlangen, in anderer unredlicher Absicht oder in Zusammenhang mit einem Computersystem, das mit einem anderen Computersystem verbunden ist, begangen worden sein muss.*»

2.2. Cybercrime Richtlinie der Union

Die Cyber-Crime-Convention bildet den rechtlichen Bezugsrahmen für die Bekämpfung der Cyberkriminalität und damit auch der Angriffe auf Informationssysteme. Die RL Cybercrime[13] der Union baut auf diesem Übereinkommen auf. Art. 3 pönalisiert den rechtswidrigen Zugang zu Informationssystemen: «*Die Mitglied-*

[12] Übereinkommen über Computerkriminalität des Europarats, CETS 185, Budapest, 23.XI.2001.
[13] RL (EU) über Angriffe auf Informationssysteme und zur Ersetzung des Rahmenbeschlusses 2005/222/JI des Rates, ABl. L 218/8 vom 14.08.2013.

staaten treffen die erforderlichen Maßnahmen, um sicherzustellen, dass der vorsätzliche unbefugte Zugang zu einem Informationssystem als Ganzem oder zu einem Teil davon, wenn dieser Zugang durch eine Verletzung von Sicherheitsmaßnahmen erfolgt, zumindest dann unter Strafe gestellt wird, wenn kein leichter Fall vorliegt.»

2.3. Richtlinie zur Netzwerk- und Informationssicherheit der Union

Die NIS-RL[14] normiert unbeschadet der «Wesentlichen Dienste» in Art. 16 die Sicherheitsanforderungen und Meldung von Sicherheitsvorfällen von Anbietern digitaler Dienste: «*Die Mitgliedstaaten stellen sicher, dass die Anbieter digitaler Dienste geeignete und verhältnismäßige technische und organisatorische Maßnahmen ergreifen, um die Risiken für die Sicherheit der Netz- und Informationssysteme, die sie im Rahmen der Bereitstellung der in Anhang III aufgeführten Dienste innerhalb der Union nutzen, zu bewältigen. Diese Maßnahmen müssen unter Berücksichtigung des Stands der Technik ein Sicherheitsniveau der Netz- und Informationssysteme gewährleisten, das dem bestehenden Risiko angemessen ist.*» Die Umsetzung der NIS-RL erfolgte im NISG[15]. Die Definition des Stands der Technik wird gem. dem Verhältnismäßigkeitsgrundsatz normiert, wobei die notwendigen technischen Maßnahmen je nach konkreter Fallgestaltung unterschiedlich sein können, sodass es nicht möglich ist, den Stand der Technik abschließend zu beschreiben. Vgl. dazu Bartels[16]: «*Demzufolge wird dann die zentrale Frage zu stellen sein, unter welchen Voraussetzungen vom objektiv zu bestimmenden Stand der Technik, der das beste und effektivste Schutzniveau meint, welches auf dem Markt erhältlich ist, nach unten aus subjektiven Gründen (technische subjektive Unmöglichkeit und wirtschaftliche Zumutbarkeit) abgewichen werden kann.*»

2.4. Cybersecurity Act der Union

Der jüngst am 27. Juni 2019 in Kraft getretene EU Cybersecurity Act[17] ersetzt den Rechtsakt zur Cybersicherheit aus 2013 und normiert u.a. in Art. 56 eine neu geschaffene Cybersicherheitszertifizierung: «*Für IKT-Produkte, -Dienste, und -Prozesse die auf der Grundlage eines nach Artikel 49 angenommenen europäischen Schemas für die Cybersicherheitszertifizierung zertifiziert wurden, gilt die Vermutung der Einhaltung der Anforderungen dieses Schemas.*» Weiters wird normiert: «*Sofern im Unionsrecht oder im Recht der Mitgliedstaaten nicht anders bestimmt, ist die Cybersicherheitszertifizierung freiwillig.*» Das Ziel ist, das Vertrauen in IKT-Produkte, -Dienste und -Prozesse zu stärken und deren Sicherheit zu erhöhen.

2.5. Österreichisches Strafrecht

Die Umsetzung der Cyber-Crime-Convention erfolgte teilweise im Zuge des StrÄG 2002[18]. Dabei wurde die Pönalisierung des «Hackings» in § 118a Abs. 1 StGB normiert, welche später im StrÄG 2015[19] novelliert wurde, da ein bis dahin strafloser, aber wesentlicher Fall der Einrichtung von «BOT-Netzwerken» sanktioniert werden sollte: «*Wer sich zu einem Computersystem, über das er nicht oder nicht allein verfügen darf, oder zu einem Teil eines solchen durch Überwindung einer spezifischen Sicherheitsvorkehrung im Computersystem*

[14] RL (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016.

[15] NISG: Bundesgesetz zur Gewährleistung eines hohen Sicherheitsniveaus von Netz- und Informationssystemen (Netz- und Informationssystemsicherheitsgesetz – NISG).

[16] Bartels, TeleTrusT – Bundesverband IT-Sicherheit e.V., Berlin, 13.08.2016. Stellungnahme zum «Diskussionspapier zur Absicherung von Telemediendiensten nach Stand der Technik» des BSI.

[17] VO (EU) 2019/881 vom 17. April 2019 über die ENISA (Agentur der Europäischen Union für Cybersicherheit) und über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik und zur Aufhebung der Verordnung (EU) Nr. 526/2013 (Rechtsakt zur Cybersicherheit).

[18] Strafrechtsänderungsgesetz 2002, BGBl. I 134/2002.

[19] Strafrechtsänderungsgesetz 2015, BGBl. I 112/2015.

in der Absicht Zugang verschafft, sich oder einem anderen Unbefugten Kenntnis von personenbezogenen Daten zu verschaffen, deren Kenntnis schutzwürdige Geheimhaltungsinteressen des Betroffenen verletzt, oder einem anderen durch die Verwendung von im System gespeicherten und nicht für ihn bestimmten Daten, deren Kenntnis er sich verschafft, oder durch die Verwendung des Computersystems einen Nachteil zuzufügen.»

Diese Formulierung des Tatbestands lehnt sich dabei sehr eng an Art. 2 der Cyber-Crime-Convention an. Von den gem. Cyber-Crime-Convention zulässigen Tatbestandseinschränkungen wurde nur insofern Gebrauch gemacht, als nicht jeder widerrechtliche Zugriff auf ein Computersystem strafbar ist, sondern nur einer, der unter Überwindung spezifischer Sicherheitsvorkehrungen stattfindet. Nach Reindl-Krauskopf[20] wird diese Absicht neben der Datenverwendungs- und Gewinn- bzw. Schädigungsabsicht verlangt und zusätzlich «*sind solche Sicherheitsmechanismen dadurch gekennzeichnet, dass sie individuell gestaltet sind, es nicht allgemein bekannt ist, wie sie ausgeschaltet werden können, und nur eine beschränkte Anzahl von Personen über dieses besondere Wissen verfügt.*»[21] Darüber hinaus wird ausgeführt «*Mitunter nützten Täter zum Eindringen lediglich Fehler aus, die bei der Programmierung zB des Betriebsprogramms passieren und daher im Programm standardmäßig enthalten sind. Auch in solchen Fällen überwindet der Täter keine spezifische Sicherheitsvorkehrung.*»[22]

Diese Umsetzung im StGB und Auslegung der Cyber-Crime-Convention (wo die Verletzung von Sicherheitsmaßnahmen nur eine Kann-Bestimmung darstellt) entspricht jener der RL Cybercrime, nach welcher der Zugang durch eine Verletzung von Sicherheitsmaßnahmen für eine Pönalisierung zwingend erforderlich ist. Dies erscheint aber durchaus problematisch, da es die besondere Eigenschaft von Angreifern und eben nicht der Allgemeinheit ist, zu wissen, wie die individuellen Sicherheitsmaßnahmen ausschaltbar sind, wie bspw. mittels Backdoors oder Exploits, insb. Zero-Day-Exploits[23]. Zur Erfüllung des § 118a wird jedoch gefordert, dass diese Sicherheitsvorkehrung erst überwunden, beschädigt, das Passwort widerrechtlich erlangt, oder es mit Brute-Force-Scans erraten wird, was üblicherweise die Methoden wenig professioneller Angreifer darstellt. Das Wissen über solche Fehler machen sich Angreifer vermehrt zu Nutze, um in fremde Computersysteme einzudringen. Der technische Nachweis der Ausnutzung von Exploits ist bereits aufwändig und schwierig genug, und wenn trotz dieses Nachweises keine Pönalisierung zu befürchten ist, ist es für Angreifer geradezu eine Einladung, mit Hilfe von Exploits in ein System einzudringen. Weiter ist es evident, dass trotz größter Sorgfalt beim Softwareengineering und der Qualitätssicherung keine fehlerfreie Software entsteht (denn fehlerfrei kann Software nur sein, wenn sie vollkommen funktionslos ist).

Laut einer Studie von Huber[24] sind die «*Gründe für die Nichtaufklärung der Fälle sind vor allem die fehlenden Gründe zur weiteren Verfolgung, fehlende Anhaltspunkte und Beweise, der mangelnde Tatbestand, die fehlende Motivation der Anklage sowie die Nichtzuständigkeit der Staatsanwaltschaft.*» wodurch im OLG Sprengel Wien nur eine verschwindend geringe Anzahl von Angeklagten im Untersuchungszeitraum bestraft wurde.

Die im Gesetz normierte Schwelle für den Eintritt der gerichtlichen Strafbarkeit eines widerrechtlichen Zugriffs auf Computersysteme erscheint daher als zu hoch, und sollte ehest möglich vom Gesetzgeber dem Stand der Technik angepasst werden.

---

20 Reindl-Krauskopf, Cyberstrafrecht im Wandel, ÖJZ 2015/19, 112 ff.

21 Reindl-Krauskopf, Salimi, Stricker: Handbuch IT-Strafrecht, Cyberdelikte und Ermittlungsbefugnisse, Manz, 2018, Rz 2.23.

22 Reindl-Krauskopf, Salimi, Stricker: Handbuch IT-Strafrecht, Cyberdelikte und Ermittlungsbefugnisse, Manz, 2018, Rz 2.28.

23 Exploit, der eingesetzt wird, bevor es einen Patch als Gegenmaßnahme gibt. Von Angreifern werden Zero-Day-Exploits gern geheim gehalten, um sie lange auszunutzen.

24 Huber, Pospisil, Hötzendorfer, Löschl, Quirchmayr, Tschohl, Without a trace – Die ungeklärten Cybercrime-Fälle des Strafandesgerichts Wien, in: Jusletter IT 21. February 2019, Rz 19.

2.6. Bewertung der Fallbeispiele

Die beschriebenen beispielhaften Fälle verdeutlichen, dass obwohl technischerseits ausreichend Mittel zur Beweisführung vorhanden wären, die Rechtslage nicht ausreicht, um Beweise zu erlangen oder, solche Beweise zu erlangen, die für eine Verurteilung ausreichen, da weitere objektive oder subjektive Tatbestandsmerkmale nachweisbar zu erfüllen sind. Ob i.d.Z. zusätzlich zu § 118a StGB auch § 126c erfüllt war, indem der Tatverdächtige ein Computerpasswort, einen Zugangscode oder vergleichbare Daten, die den Zugriff auf ein Computersystem oder einen Teil davon ermöglichen, sich verschafft oder besessen hat, die zur Begehung des § 118a gebraucht werden konnten, ist in diesen beschriebenen Fällen – und darüber hinaus meistens in vielen anderen – jedenfalls anzunehmen. Technisch gesehen erfordert das Übernehmen eines Computersystems i.d.R. auch dessen Veränderung, da Sicherheitsmechanismen zu überwinden sind, und somit das Computersystem zumindest zeitweise manipuliert werden muss, um eindringen zu können. Die Folge solcher Angriffe sind nicht unerhebliche Aufwände der Opfer, welche diese beschädigten Sicherheitsmechanismen wieder in Stand bringen müssen bzw. die Passwörter neu vergeben müssen, und daher das System in der Funktionsweise gestört wird. «*Folglich sind häufig mehrere Tatbestände des StGB §§ 118a und 126a bis c bei einem Hackerangriff gleichzeitig erfüllt.*»[25]

Wieweit die Opfer ein Mitverschulden trifft, hängt davon ab, ob und wieweit der Stand der Technik erfüllt ist, und ob zukünftig eine allfällige Cybersicherheitszertifizierung der eingesetzten IKT-Produkte besteht, welche hins. der Sicherheit zukünftig den Stand der Technik vorgeben wird. Jedoch ist diese Zertifizierung freiwillig, und somit ist es absehbar, dass im Streitfall diese Frage nur ein Sachverständiger beantworten wird können. Auch hinsichtlich digitaler Dienste sind erhöhte Sicherheitsanforderungen und Meldepflichten normiert, jedoch können alle diese Maßnahmen nicht verhindern, sondern nur das Risiko reduzieren, dass Backdoors und Exploits von Angreifern genutzt werden.

Auch hätte im Fall des Social-Media-Accounts die Verdächtige auch die Fälschung eines Beweismittels erfüllt (§ 293 StGB), wenn dieses Beweismittel in einem gerichtlichen Verfahren oder in einem Ermittlungsverfahren nach der StPO[26] gebraucht würde; denn mit der Umschaltung des Accounts auf öffentlich sollte der Eindruck erweckt werden, dass die Screenshots von einem dauerhaft öffentlichen Account stammen, und dies zum Zwecke, dass dieser optische Hinweis auf den Beweismitteln aufscheint.

Im Fall der Verschlüsselungssoftware würde den Softwarehersteller zwar eine Mitwirkungspflicht treffen, eine Offenbarung seiner Geschäftsgeheimnisse kann dem jedoch entgegen stehen. § 154 Abs. 1 StPO normiert die Wahrheitspflicht eines Zeugen, wenn er die zur Aufklärung der Straftat wesentliche oder sonst den Gegenstand des Verfahrens betreffende Tatsachen mittelbar oder unmittelbar wahrgenommen haben könnte und darüber im Verfahren aussagen soll. Obwohl Zeugen verpflichtet sind, richtig und vollständig auszusagen, kann – so ferne nicht Tatbestände gem. §§ 156 bis 157 vorliegen – lt. § 158 Abs. 1 die Beantwortung einzelner Fragen von Zeugen verweigert werden, wenn sie der Gefahr eines unmittelbaren und bedeutenden vermögensrechtlichen Nachteils aussetzen würden. Sie können jedoch trotz Weigerung zur Aussage verpflichtet werden, wenn dies wegen der besonderen Bedeutung ihrer Aussage für den Gegenstand des Verfahrens unerlässlich ist. Von einem unmittelbaren und bedeutenden Vermögensnachteil kann dann ausgegangen werden, wenn eine auf längere Zeit wirksame, nachteilige Beeinträchtigung der wirtschaftlichen Gesamtsituation gegeben ist[27]. Ob dies für einen Softwarehersteller, welcher Verschlüsselungssoftware herstellt, gleichfalls gilt, lässt die Literatur und Rsp. offen. Zumal in diesem Fall auch urheberrechtlich schutzwürdige Interessen betroffen sind, und die Unerlässlichkeit in diesem konkreten Fall offenbar nicht gegeben zu sein scheint (die Informationen würden noch keine Entschlüsselung garantieren), wäre m.E. eine Aussageverweigerung hinsichtlich des Programmcodes oder der Datenstrukturen durchaus gerechtfertigt, und der Hinweis, dass die Containerdateien TrueCrypt kompatibel sind, musste daher ausreichen.

---

[25] Hrdinka: Rechtsfolgen der Evolution von SCADA hin zum IoT, in: Jusletter IT 21. February 2019.

[26] Strafprozessordnung BGBl. 631/1975.

[27] Rz 1 in Foregger/Fabrizy: Die österreichische Strafprozessordnung (Strafprozessordnung 1975) samt den wichtigsten Nebengesetzen. Kurzkommentar (9. Auflage). Wien: Manz, 2004.

3. Bewertung und Ausblick

Technisch sind digitale Beweise anders als physische anzusehen, und rechtlich elektronischen Urkunden gleichzustellen, was eine besondere Vorsicht und Achtsamkeit bei der Spurensuche und deren Sicherung erfordert. Eine digitale Signierung elektronischer Urkundenbeweise durch den Beweisführer, Ermittler oder Sachverständigen ist daher geboten. Die Spurenbewertung folgt ebenfalls gänzlich anderen Gesetzmäßigkeiten als bei den physischen Pendants. Diese Problematik wurde frühzeitig erkannt, und führte letztlich dazu, dass vom Gesetzgeber spezielle Tatbestände geschaffen worden sind, welche das unrechtmäßige Eindringen in ein Computersystem pönalisieren, was davor – so ferne keine Daten beschädigt wurden – straflos war. Die Hürde zum Eindringen, der objektive Tatbestand der Überwindung einer spezifischen Sicherheitsvorkehrung, erscheint aber zu hoch, da er oft nicht erfüllt ist, und nicht erfüllbar sein kann, wenn Angreifer Exploits nützen, um in ein System einzudringen. Technischerseits lassen sich zwar diese Spuren eines Eindringens mittels Exploits oftmals eindeutig nachweisen, der Angreifer braucht eine Bestrafung trotzdem nicht zu fürchten, denn er überwindet nach gängiger Rechtsmeinung keine spezifische Sicherheitseinrichtung (was ja nicht ganz stimmt, denn er überwindet sie dennoch, indem er unbeabsichtigte Hintertüren ausnützt). Dass darüber hinaus verschiedene Aussagenverweigerungsrechte bestehen, macht die Beweisführung auch nicht einfacher.

Wenn die Digitalisierung nun in der gleichen Geschwindigkeit wie bis dato fortschreitet, in alle Lebensbereiche der Gesellschaft eindringt, und unter der Annahme der Tatsache, dass die sich immer rasanter verbreitenden IT-Systeme natürlicherweise Exploits aufweisen in einer Anzahl, die weder kontrollierbar noch handhabbar ist, welche Angreifer risikolos ausnützen können, ist dies eine latente Gefahr für den Schutz der Nutzer, betroffener Dritter und insgesamt der Zivilgesellschaft. Der Gesetzgeber, insb. die Union, ist daher gefordert, ehest möglich zusätzlich zu der jüngst erlassenen NIS-RL und dem Cybersecurity Act, welche eher für präventiven Schutz ausgelegt sind, adäquate Rechtsnormen zu erlassen, welche eine Strafverfolgung von Tatverdächtigen gemäß dem Stand 2020 und darüber hinaus ermöglichen.

4. Literatur

Bartels, TeleTrusT – Bundesverband IT-Sicherheit e.V., Berlin, 13. August 2016. Stellungnahme zum «Diskussionspapier zur Absicherung von Telemediendiensten nach Stand der Technik» des BSI.

Casey: Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet. Academic Press, 2011.

Dewald, Freiling: Forensische Informatik, Books on Demand, 2011.

Foregger/Fabrizy: Die österreichische Strafprozessordnung (Strafprozessordnung 1975) samt den wichtigsten Nebengesetzen. Kurzkommentar (9. Auflage). Wien: Manz, 2004.

Hrdinka: Auf Spurensuche in der Cyberwelt – Digitale Beweise mit IT-Forensik, 45. Ottensteiner Fortbildungsseminar aus Strafrecht und Kriminologie, NWV Verlag, 2018.

Hrdinka: Rechtsfolgen der Evolution von SCADA hin zum IoT, in: Jusletter IT 21. February 2019.

Huber, Pospisil, Hötzendorfer, Löschl, Quirchmayr, Tschohl, Without a trace – Die ungeklärten Cybercrime-Fälle des Straflandesgerichts Wien, in: Jusletter IT 21. February 2019.

Inman, Rudin: Principles and Practice of Criminalistics: The Profession of Forensic Science. CRC Press, 2000.

Kirk: Crime Investigation. John Wiley & Sons, 1974.

Locard: L'enquete criminelle et les methodes scientifique. Ernest Flammarion, Paris, 1920.

Reindl-Krauskopf, Cyberstrafrecht im Wandel, ÖJZ 2015/19, 112 ff.

Reindl-Krauskopf, Salimi, Stricker: Handbuch IT-Strafrecht, Cyberdelikte und Ermittlungsbefugnisse, Manz, 2018.