AJP / PJA

AKTUELLE JURISTISCHE PRAXIS / PRATIQUE JURIDIQUE ACTUELLE

1 / 2020
29. Jahrgang
29e année

Sonderdruck

DIKE

AJP/PJA 1/2020

Hacking und Hacker im Schweizer Recht

Sandro Germann*

David Wicki-Birchler**

Die Entwicklung der Technik im Bereich Informationstechnologie und Hacking schreitet rasant voran, weshalb der Gesetzgeber immer höhere rechtliche Anforderungen an die erforderlichen Schutzvorkehrungen für Daten stellt. Infolgedessen besteht das Bedürfnis, sich vor Angriffen («Hacking») bestmöglich zu schützen. Dies kann auch dadurch erreicht werden, dass Hacker zu Testzwecken dazu aufgerufen werden, die vorliegenden oder geplanten Systeme anzugreifen. Wie muss man mit diesen erwünschten Hackern rechtlich umgehen? Der nachfolgende Beitrag zeigt zunächst auf, zwischen welchen Arten von Hacking und Hackern unterschieden wird. Anschliessend werden die rechtlichen Rahmenbedingungen – mit Fokus auf erwünschte Hacker – illustriert und diskutiert. Dabei zeigt sich, dass der erwünschte Hacker infolge entsprechender Vertragsgestaltung strafrechtlicher sowie haftungsrechtlicher Konsequenzen entgehen kann. Im Weiteren wird am Beispiel der Schweizerischen Post aufgezeigt, welche Besonderheiten beim öffentlichen Aufruf zum Hacking zu beachten sind.

Les technologies informatiques et le piratage évoluent à vitesse grand V, menant ainsi le législateur à imposer des exigences de plus en plus strictes concernant les mesures de protection de données. Il est nécessaire de se protéger du mieux possible contre les attaques (piratage, hacking). Une manière d'y parvenir est d'inviter des pirates, ou hackers, à attaquer les systèmes existants ou envisagés afin de les tester. Comment traiter ces hackers bienveillants (« white hats ») menant ainsi plan juridique ? La contribution présente tout d'abord les diverses variétés de hacking et de hackers. Elle illustre et discute ensuite le cadre juridique, en se concentrant sur les « white hats ». À l'examen, il s'avère que ceux-ci peuvent échapper à toute conséquence pénale et aquilienne, pourvu qu'ils soient au bénéfice d'un contrat correctement rédigé. Enfin, à l'exemple de la Poste suisse, les auteurs soulignent les particularités à observer lors d'un appel public aux hackers.

Inhaltsübersicht

I. Einführung

In der Schweizer Rechtswissenschaft assoziiert man den Begriff *Hacking* gemeinhin mit den Bestimmungen aus dem Strafgesetzbuch betreffend unbefugte Datenbeschaffung nach Art. 143 StGB sowie das Verbot des unbefugten Eindringens in ein Datenverarbeitungssystem nach Art. 143bis StGB.[1] Allenfalls wird noch die Bestimmung

* Sandro Germann, Dr. iur., LL.M., Rechtsanwalt (Schweiz/New York, US), Head of US CB Monitoring and Advisory, Credit Suisse AG.

** David Wicki-Birchler, Dr. iur., LL.M., Attorney-at-law (Wisconsin, US), General Counsel LEANmade AG.

1 Andreas Donatsch, Strafrecht III, Delikte gegen den Einzelnen, 11. A., Zürich 2018, 204.

Art. 179novies StGB in Betracht gezogen, welche das unbefugte Beschaffen von Personendaten unter Strafe stellt.

Vergleichbar mit den verschlungenen und mannigfaltigen Wegen, auf denen sich die Hacker Zugang zu ihren Zielobjekten zu verschaffen versuchen, hat sich die Thematik rund um den unbefugten Zugriff und Zugang zu elektronischen Datenverarbeitungssystemen in verschiedensten Disziplinen der Rechtswissenschaft eingenistet. Wie so häufig ist auch hier das Recht ein Spiegelbild der Vorgänge in der Gesellschaft.

Die Entwicklung des *Hackings* geht täglich weiter und wird wahrscheinlich mit dem baldigen Durchbruch der Quantencomputer vor einem gewaltigen Sprung stehen.[2] Cyberattacken sind mittlerweile in der Allgemeinheit ein weitbekanntes Phänomen resp. eine erkannte Gefahr, deren sich die meisten Benutzer von Datenverarbeitungsgeräten zumindest vordergründig bewusst sind. Sicherheitsfirmen, welche *White Hacking*[3] auf Wunsch und mit expliziter Einwilligung der Kunden anbieten, sind nicht verwundert darüber, dass es ihnen praktisch immer gelingt, in das Zielobjekt des Hackings einzudringen, sondern darüber, wie erschreckend leicht sie das erreichen. Die Liste der meistverwendeten Passwörter wird seit Jahren mit «1234», «123456», «QWERTZ», «Passwort» und ähnlichen Schlüsseln angeführt.

II. Definition von Hacking und Hackern

A. Hacking

Als *Hacking* versteht der Schweizer Gesetzgeber gemeinhin das unbefugte Eindringen in eine Datenverarbeitungsanlage.[4] Historisch taucht der Begriff *Hacking* erstmals im Zusammenhang mit Studenten des MIT (Massachusetts Institute of Technology)[5] in den fünfziger Jahren auf,[6] wo sich eine Gruppe junger Studenten zunächst um die technischen Details einer Modelleisenbahn kümmerte und sich dann begeistert den Computern des MIT widmete.[7] Eine clevere Verbindung zwischen zwei Relais nannten die Studenten einen *Hack*.[8] Damit ging die Bezeichnung für Studenten, welche damals die effektive technische Fähigkeit hatten, bestehende Programme elegant abzuändern, als *Hacker* einher.[9] Der Black's Law Dictionary[10] beschreibt den Hacker als «… someone who surreptitiously uses or changes the information in another's computer system».

B. Hacking im engeren Sinne (unbefugtes Abändern von Soft-/Hardware)

Nach der hier vertretenen Auffassung ist Hacking im engeren Sinne das unbefugte Abändern einer Hard- oder Software in ihrer ursprünglich angedachten Funktionsweise. Dies erfordert zunächst den Zugang zur Hard- oder Software.

Für den Zugang auf ein gesichertes Portal im Internet oder Intranet wird in den meisten Fällen nach einem Benutzernamen und einem Passwort gefragt. Normalerweise erlauben die Systeme nur eine begrenzte Anzahl von Anmeldeversuchen, gefolgt von einer temporären Sperre des Benutzers auf dem Portal, welche nur durch einen autorisierten Prozess wieder aufgehoben werden kann. Das blosse Erraten von Benutzernamen und Passwort gilt sicherlich nicht als Hacking, genauso wenig, wenn die entsprechenden Daten auf einem Kärtchen notiert nach einer Trennung von Ehepartnern gefunden und verwendet werden.[11] Der Grund dafür ist, dass die ursprüngliche Funktionsweise, nämlich die Zugangsbeschränkung, nicht verändert wurde. Anders wäre der Fall, wenn eine Person die Beschränkung der Anzahl Anmeldeversuche aufhebt und in der Folge durch die Methode *Brute Forcing* oder auch *Social Engineering* versucht, sich Zugang zu den geschützten Daten auf dem Portal zu verschaffen. Dabei ist nur die Aufhebung der Systembeschränkung der Anzahl Anmeldeversuche als Hacking im engeren Sinne zu qualifizieren, nicht aber das *Brute Forcing* oder auch *Social Engineering*.

---

2 Vor allem, was die Möglichkeiten von Hacking mittels *Brute Forcing* angeht.

3 Zum Begriff *White Hacker* siehe unten II.D.1.

4 Botschaft und Gesetzesentwürfe vom 24. April 1991 über die Änderung des Schweizerischen Strafgesetzbuches und des Militärstrafgesetzes (Strafbare Handlungen gegen das Vermögen und Urkundenfälschung) sowie betreffend die Änderung des Bundesgesetzes über die wirtschaftliche Landesversorgung (Strafbestimmungen), BBl 1991 969 ff., 1011.

5 Paul A. Taylor, From hackers to hacktivists: speed bumps on the global superhighway?, New Media Society 2005, 625 ff., 628; Debora Halbert, Discourses of Danger and the Computer Hacker, The Information Society 1997, 361 ff., 362.

6 Steven Levy, Hackers – Heroes of the Computer Revolution, Beijing 2010, 8.

7 Christian Imhorst, Die Anarchie der Hacker – Richard Stallman und die Freie-Software-Bewegung, Marburg 2004, 20.

8 Imhorst (FN 7), 20.

9 Imhorst (FN 7), 21.

10 Bryan A. Garner, Black's Law Dictionary, 11. A., St. Paul 2019, 856.

11 BGE 145 IV 185.

C. Hacking im weiteren Sinne (Zugang verschaffen)

Im allgemeinen Sprachgebrauch wird der Begriff *Hacking* sehr breit verwendet. Man spricht davon, dass ein Social-Media-Account, ein Smartphone oder ein Laptop «gehackt» wurde. In all diesen Fällen wurde jedoch weder die Hard- noch die Software in ihrer ursprünglichen Funktionsweise abgeändert. Der Social-Media-Account enthält immer noch die eingegebenen Informationen, das Smartphone kann immer noch zum Telefonieren und/oder zum Gebrauch der installierten Applikationen benutzt werden, genauso wie der Laptop noch die Software und die Daten enthält. Der Zugang zu den genannten Geräten kann durch Hacking im weiteren Sinne gelingen. Dafür gibt es eine Vielzahl[12] von Methoden, welche sich ständig verändern. Diese Abhandlung beschränkt sich auf eine Auswahl von gängigen relevanten Hacking-Methoden.

1. Brute Forcing

Das *Brute Forcing* versucht, sich durch eine sehr hohe Anzahl an möglichen Buchstaben- und Zahlkombinationen Zugang zum System resp. zu einer Passwort geschützten Umgebung zu verschaffen.[13] Dabei werden zunächst die gängigen Möglichkeiten wie Geburtstage, Namen von Familienmitgliedern, Wohnorte usw. in allen denkbaren Kombinationen eingegeben.

2. Social Engineering

Im Gegensatz zur brachialen Methode *Brute Forcing,* wo vor allem die Rechner-Kapazität der Hackers entscheidend ist, versucht *Social Engineering,* den Eingang in ein Datenverarbeitungssystem möglichst elegant zu finden. Dazu werden die öffentlich zugänglich gemachten oder erhältlichen Informationen systematisch gesammelt und verarbeitet, um danach mögliche Passwort-Kombinationen für den Portal-Zugang zu eruieren.[14] Dadurch stellt *Social Engineering*[15] eine spezifische, zielgerichtete Bedrohung dar, welche die vorhandenen Informationen über die Benutzer bspw. in sozialen Medien nutzt, um Zugang zu Informationen zu erhalten oder das System zu kompromittieren.[16] Es kann dabei auch vorkommen,[17] dass der Eindringling vorgibt, eine Person mit Autorisierung für den Zugriff auf die Hardware, Software oder Netzwerkkomponenten zu sein, oder durch den Vorwand, ein IT-Supporter zu sein, den Fernzugriff beantragt, um ein gemeldetes Computerproblem zu beheben.

3. Phishing

Mit *Phishing*[18] versucht der Hacker, Informationen wie Benutzernamen, Passwörter oder Finanzdaten zu erhalten, indem er sich als legitimes Unternehmen resp. autorisierte Person ausgibt. In der Regel stellt der Täter eine E-Mail oder einen Link zur Verfügung, womit das Opfer aufgefordert wird, personenbezogene Daten auf einer gefälschten Website einzugeben. Die Fälschung ist praktisch nicht als solche erkennbar, da sie eine etablierte, legitime Website täuschend echt nachahmt, die das Opfer entweder zuvor genutzt hat oder als sicheren Ort für die Eingabe von Informationen wahrnimmt.[19]

4. Spear-Phishing

Das *Spear-Phishing* ist eine Abwandlung von *Phishing,* welches sich dadurch auszeichnet, dass nicht eine unbestimmte Vielzahl von Personen generisch angeschrieben wird, sondern lediglich einzelne spezifische Personen ins Visier geraten.[20] Häufig werden Personen in der Geschäftsleitung oder deren enge Mitarbeitende mit einem

---

12 Auf einem einschlägigen Portal sind über hundert verschiedene Methoden je nach Systematik und Funktionsweise aufgeführt. Vgl. Internet: https://mitre-attack.github.io/attack-navigator/enterprise/ (Abruf 5.12.2019).

13 Ähnlich: *United States of America v. Phillips,* 477 F.3d 215 (5th Cir. 2007), 218: «Term of art in computer science used to describe a program designed to decode encrypted data by generating a large number of passwords.» Vgl. dazu auch *Earthcam, Inc. v. Oxblue Corp.,* 49 F. Supp. 3d 1210 (N.D. Ga. 2014).

14 Ausführlich zum Begriff *Social Engineering:* Christopher Hadnagy, Social Engineering – The science of Human Hacking, 2. A., Indianapolis 2018, 6 ff., sowie Pascal C. Kocher, Social Engineering – Risikofaktor Mensch, Anwaltsrevue 2017, 431 ff., 431.

15 Vgl. dazu *Parsons Infrastructure & Env't Grp., Inc. v. State,* Docket No. A-1893-16T4, N.J. Super. Feb. 26, 2018, 6.

16 Ein Beispiel von *Social Engineering* aus der US-Politik: 2008 wurde das Mail-Account der US-amerikanischen Vizepräsidentschaftskandidatin Sarah Palin durch *Social Engineering* der sogenannten Sicherheitsfrage «Wo haben Sie Ihren Ehepartner kennengelernt?» eruiert. Die Antwort wurde auf einer weltweit zugänglichen Suchplattform gefunden und ist auch heute noch dort zu finden: die High School «Wasilla High». Internet: https://www.theguardian.com/technology/askjack/2008/sep/19/security.email (Abruf 5.12.2019).

17 Vgl. dazu *Parsons Infrastructure & Env't Grp., Inc. v. State,* Docket No. A-1893-16T4, N.J. Super. Feb. 26, 2018.

18 Vgl. dazu *Choice Escrow & Land Title, LLC v. Bancorpsouth Bank,* 754 F.3d 611 (8th Cir. 2014), 615.

19 Matthias Ammann, Sind Phishing-Mails strafbar?, AJP 2006, 195 ff., 195.

20 Dan Swinhoe, What is spear phishing? Why targeted email attacks are so difficult to stop, Internet: https://www.csoonline.com/article/3334617/what-is-spear-phishing-why-targeted-email-attacks-are-so-difficult-to-stop.html (Abruf 5.12.2019).

Mail angegangen, welches durchaus glaubwürdigen Inhalt hat und teilweise nur sehr schwer als Angriff eines Hackers zu identifizieren ist. Besonders tückisch und deshalb schwierig zu erkennen ist ein *Spear-Phishing*-Angriff, wenn die vom Hacker benutzte Mailadresse mit einer firmeninternen Mailadresse identisch ist.

5. Malware

Malware im Wortsinn ist die Kurzform von «malicious software». Die *Malware* ist also nichts anderes als eine Software, welche «malicious», also bösartig ist und damit versucht, Schaden zu verursachen. Dabei sind verschiedene Arten denkbar: Die Malware kann ein unerwünschtes Foto oder Emblem am Bildschirm einblenden oder lässt systematisch Daten zum Hacker oder ins Internet transferieren.[21] In seiner schlimmsten Ausprägung zerstört die Malware alle Daten unwiderruflich. Damit die *Malware* unerkannt in ein Datenverarbeitungssystem eindringen kann, wird häufig die Technik des Trojaners[22] benutzt. Einmal erfolgreich unerkannt wie das Trojanische Pferd im System eingeschleust, arbeitet die *Malware* häufig im Hintergrund und wird durch den Anwender der Datenverarbeitungsanlage spät oder gar nie bemerkt.

6. Ransomware

Ransomware ist eine Weiterentwicklung der Malware:[23] Sie hat zum Ziel, Dateien des Opfers zu verschlüsseln und damit unbrauchbar zu machen, verbunden mit der Forderung an das Opfer, ein Lösegeld (engl. ransom) zu bezahlen, um die Dateien wieder brauchbar zu machen.[24] *Policy Ransomware*[25] meint eine besondere Ausprägung von *Ransomware,* wo eine scheinbar behördliche Mitteilung erscheint, welche das Opfer auffordert, eine Busse zu bezahlen, damit dieses den Computer resp. die Daten wieder nutzen kann. Hier setzt der Hacker darauf, dass das Opfer sich beim Besuchen von illegalen Seiten im Internet ertappt fühlt, und um zu verhindern, dass die vermeintlichen Behörden rechtlich weitere Schritte einleiten (verbunden mit einer allfälligen Publizität in der Familie oder gar am Arbeitsplatz), eine vermeintliche Busse zur Erledigung der Angelegenheit begleicht.

D. Hacker

1. White Hat Hacker

Der *White Hat Hacker*[26] oder *White Hacker* versucht, seine Hacking-Fähigkeiten zum Nutze der Gesellschaft anzuwenden. Häufig wird er auch von Unternehmen oder Behörden damit beauftragt, mögliche Schwachstellen im IT-Sicherheitskonzept aufzudecken.[27] Im rechtlichen Sinne kann die Intention des Hackers durchaus von Relevanz sein, etwa bei der strafrechtlichen Beurteilung einer allfälligen Bereicherungsabsicht.[28] Aus Sicht des White Hackers wird es sinnvoll sein, diese Gesinnung und den nach Art. 394 OR erteilten Auftrag rechtsgenügend und vor allem vor dem Beginn seiner Tätigkeiten angemessen zu Beweiszwecken zu dokumentieren.

2. Black Hat Hacker

Der *Black Hat Hacker* setzt seine Programmierkenntnisse für kriminelle Zwecke ein.[29] Sein Handeln erfüllt damit alle Voraussetzungen der Strafbarkeit, d.h., unter Beurteilung nach Schweizer Strafrecht handelt er tatbestandsmässig, widerrechtlich und schuldhaft bei seinem Verstoss gegen die Rechtsordnung. Im Vordergrund steht vor allem der Verstoss gegen Art. 143 StGB sowie Art. 143bis StGB.

3. Grey Hat Hacker

Wie schon die Namensgebung vermuten lässt, ordnet sich der *Grey Hat Hacker* zwischen dem White Hat und dem

---

21 Illustrativ *Zango v. Kaspersky Lab,* 568 F.3d 1169 (9th Cir. 2009).

22 Christa Pfister, Hacking in der Schweiz im Spiegel des europäischen, des deutschen und des österreichischen Computerstrafrechts, Berlin/Wien/Zürich 2008, 36.

23 Azad Ali, Ransomware: A Research and Personal Case Study of Dealing with this Nasty Malware, Issues in Informing Service + Information Technology 2017, 88 ff., 88 f.

24 Giovanni Molo/Jana Drzalic, Können Kryptowährungen compliant sein?, AJP 2019, 40 ff., 45; Deneesha Kansagra/Malaram Kumhar/Dhaval Jha, Ransomware: A Threat to Cyber Security, IJCSCS 2015/2016, 224 ff., 226.

25 Bernhard Isenring/Roy D. Maybud/Laura Quiblier, Phänomen Cybercrime – Herausforderungen und Grenzen des Straf- und Strafprozessrechts im Überblick, SJZ 2019, 439 ff., 441.

26 *United States v. Hutchins,* 361 F. Supp. 3d 779 (E.D. Wis. 2019), 784.

27 Courtney Falk, Grey Hat Hacking: Morally Black and White, Cyber Security Group (CSG) Training Conference Paper, 2004, 1 ff., 1; Jill Thomas, The moral ambiguity of social control in cyberspace: a retroassessment of the «golden age» of hacking, New Media and Society 2005, 599 ff., 617; Dieter Kochheim, Cybercrime und Strafrecht in der Informations- und Kommunikationstechnik, 2. A., München 2018, 569.

28 Der subjektive Tatbestand von Art. 143 StGB verlangt eine Bereicherungsabsicht, seit der Revision des Strafrechts vom 1. Januar 2012 wird dies hingegen beim Art. 143bis StGB nicht mehr gefordert.

29 Illustrativ *Smith v. Mastercard Int'l,* No. 4:16CV1866 CDP (E.D. Mo. Dec. 15, 2016); Falk (FN 27), 1.

Black Hat Hacker ein.[30] Er verhält sich grundsätzlich ähnlich wie der White Hacker, indem er Schwachstellen von Computersystemen und Netzwerken aufzeigen will. Diese Befunde der Schwachstellen stellt er regelmässig der Öffentlichkeit zur Verfügung und nimmt dabei in Kauf, dass auch sogenannte Black Hat Hacker diese Informationen zu ihren Zwecken missbrauchen, womit gegebenenfalls eine Strafbarkeit nach Art. 144bis Ziff. 2 StGB in Frage kommt.[31]

III. Hacking und Hacker aus strafrechtlicher Sicht

A. Art. 143 StGB: Unbefugte Datenbeschaffung

Gemäss Art. 143 StGB macht sich strafbar, wer in der Absicht, sich oder einen andern unrechtmässig zu bereichern, sich oder einem andern elektronisch oder in vergleichbarer Weise gespeicherte oder übermittelte Daten beschafft, die nicht für ihn bestimmt und gegen seinen unbefugten Zugriff besonders gesichert sind.[32]

Die Strafbarkeit ist dann gegeben, wenn sich der Täter Daten beschafft, die nicht für ihn bestimmt und gegen seinen unbefugten Zugriff besonders gesichert sind.[33] Nach der früheren Lehrmeinung hatten Phishing-Mails keine Schutzmechanismen zu überwinden, welche die Daten des Opfers schützen sollten.[34] Diese Ansicht ist angesichts der heute standardmässigen Firewalls und sonstiger technischer Schutzmassnahmen, welche zum Ziel haben, möglichst viele illegitime Mails von der Mailbox fernzuhalten, überholt.[35]

Das Hacking durch Brute Forcing erfüllt dieses Kriterium der Überwindung einer besonderen Sicherung, da es ja gerade durch seine grosse Anzahl von Passwort-Kombinationen versucht, den Kennwortschutz zu durchbrechen.

Bei der Malware kommt es für die Beurteilung einer möglichen Strafbarkeit darauf an, zu welchem Zweck das Schadprogramm angewendet wurde: Falls es ausschliesslich zur Zerstörung von Soft- oder Hardware angewendet wird, würde die Strafbarkeit nach Art. 143 StGB entfallen, da gar keine Daten beschafft würden. Anders ist die Situation rechtlich zu beurteilen, wenn die Malware die Daten für den Hacker sichtet und/oder überträgt. In diesem Fall ist das Kriterium der Datenbeschaffung erfüllt.

Ähnlich verhält es sich bei der Ransomware: Falls der Zweck des Einsatzes sich auf die Lösegelderpressung beschränkt, fällt die Anwendbarkeit von Art. 143 StGB ausser Betracht. Würde aber die Ransomware die Daten sichten und/oder übertragen, käme eine Bestrafung wegen unbefugter Datenbeschaffung in Frage. Der Tatbestand der Erpressung nach Art. 156 StGB ist in beiden Fällen natürlich zu prüfen.

Beim Social Engineering kommt es auf die konkrete Ausgestaltung des Hackings an. Wenn die durch ein erfolgreiches Social Engineering eruierten Daten zum Überwinden einer technischen Schranke verwendet werden, wäre dieses Tatbestandsmerkmal von Art. 143 StGB erfüllt. Dies gilt insbesondere beim Versuch, Passwörter durch Social Engineering zu ermitteln.

B. Art. 143bis StGB: Unbefugtes Eindringen in ein Datenverarbeitungssystem

Nach Art. 143bis Abs. 1 StGB wird bestraft, wer auf dem Wege von Datenübertragungseinrichtungen unbefugterweise in ein fremdes, gegen seinen Zugriff besonders gesichertes Datenverarbeitungssystem[36] eindringt.

Nach Abs. 2 von Art. 143bis StGB macht sich strafbar, wer Passwörter, Programme (Hacking-Tools) oder andere Daten verbreitet, von denen er weiss, dass sie für eine strafbare Handlung nach Abs. 1 verwendet werden. Damit stellt sich insbesondere die Frage nach einer allfälligen Strafbarkeit des White Hackers. Sein ausdrücklicher Auftrag ist es, dem Auftraggeber Schwachstellen in seiner Datenverarbeitungskonfiguration aufzuzeigen und zu dokumentieren, damit diese behoben werden können. Der White Hacker handelt betreffend den Aspekt der Weitergabe der Informationen ohne Zweifel vorsätzlich. Er muss sich in sinnvoller Weise vergewissern, dass das

---

30 Cassandra Kirsch, The Grey Hat Hacker: Reconciling Cyberspace Reality and the Law, Northern Kentucky Law Review 2014, 383 ff., 388.

31 Kirsch (FN 30), 388.

32 Günter Stratenwerth/Guido Jenny/Felix Bommer, Schweizerisches Strafrecht, Besonderer Teil I: Straftaten gegen Individualinteressen, 7. A., Bern 2010, 358.

33 CR CP II-Monnier, Art. 143 N 9, in: Alain Macaluso/Laurent Moreillon/Nicolas Queloz (Hrsg.), Code pénal II, Commentaire romand, Basel 2017 (zit. CR CP II-Verfasser); BSK StGB-Weissenberger, Art. 143 N 23, in: Marcel Alexander Niggli/Hans Wiprächtiger (Hrsg.), Strafrecht II, Basler Kommentar, 4. A., Basel 2018 (zit. BSK StGB II-Verfasser).

34 Ammann (FN 19), AJP 2006, 197.

35 Das gilt analog für das *Spear-Phishing*.

36 Michel Dupuis/Laurent Moreillon/Christophe Piguet/Séverine Berger/Miriam Mazou/Virginie Rodigari (Hrsg.), Code pénal, Petit commentaire, 2. A., Basel 2017, Art. 143bis CP N 11.

Wissen um die Schwachstellen nicht für strafbare Zwecke verwendet wird. Die Schwelle ist tief anzusetzen; es muss genügen, dass zwei Personen, die laut Handelsregister für das auftraggebende Unternehmen zeichnungsberechtigt sind, dem White Hacker den Auftrag geben. Diese niedrige Hürde ist für die Arbeit des White Hackers essentiell. Die Sorgfaltspflicht nach Auftragsrecht fordert, dass er erst dann seine Tätigkeit aufnimmt, wenn er die Auftraggeber rechtlich genügend identifiziert hat und damit vermeidet, dass er selbst quasi als Werkzeug von Social Engineering missbraucht wird.

Eine beliebte Methode, um Malware oder Ransomware zu installieren, ist das scheinbar zufällige Liegenlassen von Datenträgern (bspw. USB-Sticks), vorzugsweise mit einer Beschriftung «vertraulich» oder «persönlich». Das blosse Liegenlassen eines USB-Sticks erfüllt den objektiven Tatbestand von Art. 143bis StGB noch nicht. Erst wenn der Datenträger bei einer Hardware eingesteckt wird und damit *Malware* oder auch *Ransomware installiert* werden kann, kommt allenfalls eine unbefugte Datenbeschaffung nach Art. 143 StGB in Frage.[37] Dies wird aber nur dann der Fall sein, wenn die *Malware* oder *Ransomware* auch effektiv Daten beschafft, d.h. auf irgendeine Weise dem Hacker zugänglich macht.

Beschränkt sich die Funktionsweise der Malware oder Ransomware lediglich auf die Zerstörung von Hard- und/oder Software, kommt gegebenenfalls eine Bestrafung nach Art. 144bis Ziff. 1 StGB wegen Datenbeschädigung in Frage.[38]

Das Social Engineering erfüllt dann die objektiven Tatbestandsvoraussetzungen von Art. 143bis StGB, wenn durch diese Art von Hacking effektiv in eine Datenverarbeitungseinrichtung eingedrungen werden konnte und diese mit einem besonderen Zugriffsschutz versehen war.

C. Art. 144bis Ziff. 1 StGB: Datenbeschädigung

Für dieses Delikt kommt das Hacking mittels Malware und Ransomware in Frage, wenn jeweils effektiv eine Beschädigung der Hard- und/oder Software vorliegt. Interessanterweise ist auch eine Begehung dieses Deliktes durch Unterlassung denkbar.[39] Das bedeutet konkret, dass, wenn ein IT-Verantwortlicher in einer Firma gemäss internen Richtlinien jeden Abend ein Backup der gesamten Firmendaten zu erstellen hat, dies unterlässt und auf diese Weise die Daten zerstört werden, eine Strafbarkeit nach Art. 144bis Ziff. 1 StGB in Betracht kommt.[40]

Hier wird in Zukunft nach der Revision des schweizerischen Datenschutzgesetzes das Prinzip «Privacy by Design and Default»[41] auch im Strafrecht eine Rolle spielen. Wird dieses datenschutzrechtliche Prinzip u.a. betreffend die adäquate Sicherung von Daten im Unternehmen verletzt, stellt sich unseres Erachtens auch die Frage der Strafbarkeit nach Art. 144bis Ziff. 1 StGB.

D. Art. 144bis Ziff. 2 StGB: Herstellen von datenschädigenden Programmen

Damit die Sicherheit von elektronischen Datenverarbeitungssystemen stetig verbessert werden kann, ist die Arbeit von White Hackern sehr wichtig. Diese können wichtige Hinweise auf mögliche Schwachstellen im System geben. Bei dieser auch gesellschaftlich erwünschten Tätigkeit wird darauf zu achten sein, nicht tatbestandsmässig im Sinne von Art. 144bis Ziff. 2 StGB zu handeln.

Denn für gewisse White-Hacking-Aufträge werden notwendigerweise entsprechende Hacking-Programme in Verkehr gebracht. Der White Hacker muss aber für die Erfüllung des ordnungsgemässen Auftrages ein Programm benutzen, welches keine Daten schädigt.

E. Art. 147 StGB: Computerbetrug

Nach Art. 147 StGB macht sich strafbar, wer in der Absicht, sich oder einen andern unrechtmässig zu bereichern, durch unrichtige, unvollständige oder unbefugte Verwendung von Daten oder in vergleichbarer Weise auf einen elektronischen oder vergleichbaren Datenverarbeitungs- oder Datenübermittlungsvorgang einwirkt und dadurch eine Vermögensverschiebung zum Schaden eines andern herbeiführt oder eine Vermögensverschiebung unmittelbar darnach verdeckt.[42]

---

37 Sofern ein Arbeitnehmer gegen jede übliche Vorsicht einen gefundenen Datenträger beim PC des Unternehmens einsteckt, stellt sich die Frage, ob eine arbeitsrechtliche Sorgfaltspflichtverletzung (vgl. Art. 321a OR) vorliegt.

38 Ist mit der Installation der Ransomware eine Lösegeldforderung verbunden, kommt eine Bestrafung nach Art. 156 StGB (Erpressung), allfällig in Realkonkurrenz mit Art. 146 StGB (Betrug), in Frage.

39 Donatsch (FN 1), 218.

40 Donatsch (FN 1), 218.

41 Vgl. dazu Philipp Räther, Die Anwendung der neuen EU-Datenschutz-Grundverordnung im Unternehmen, ZHR 2019, 94 ff. 95.

42 Stefan Trechsel/Dean Crameri, in: Stefan Trechsel/Mark Pieth (Hrsg.), Schweizerisches Strafgesetzbuch, Praxiskommentar, 3. A., Zürich 2017, Art. 147 StGB N 1.

Nach der bundesgerichtlichen Rechtsprechung[43] ist der Missbrauch eines Mobiltelefons, wo die Kosten beim Opfer anfallen, der Täter aber die Leistung (Führen des Ferngespräches) für sich bezieht, nach Art. 147 StGB strafbar.[44] In der heutigen Zeit muss analog Gleiches für den unbefugten Benutzer von Computern, der mit dem Zweck handelt, Rechnerleistung bspw. für die Schürfung von Kryptowährungen abzuzweigen, gelten.

F. Art. 179^{novies} StGB: Unbefugtes Beschaffen von Personendaten

Der Täter beschafft aus einer Datensammlung unbefugt besonders schützenswerte Personendaten oder Persönlichkeitsprofile, die nicht frei zugänglich sind.[45] Mit diesem Artikel werden richtigerweise besonders schützenswerte Personendaten[46] strafrechtlich zusätzlich geschützt. Damit werden die datenschutzrechtlich besonders behandelten schützenswerten Personendaten (Art. 3 lit. c DSG) konsequenterweise auch im Strafrecht gesondert behandelt. Hier kommen als Hacking-Methoden *Phishing, Spear-Phishing, Malware* und *Ransomware* in Frage, da diese Methoden die technische Fähigkeit haben, dem Hacker Daten zugänglich zu machen. Das *Social Engineering* sowie das *Brute Forcing* fokussieren auf die Überwindung der Zugangsschranken zum jeweiligen Portal.

G. Würdigung

Die rechtliche Qualifikation der Aktivitäten des *Black Hat Hackers* als strafbare Tätigkeit dürfte in der Regel keine Schwierigkeiten bereiten. Der *White Hat Hacker* wird sich auf die Einwilligung des Verletzten nach dem Grundsatz *volenti non fit iniuria* berufen.[47] Dies ist aber rechtlich heikel, denn bei Unternehmen wird regelmässig die juristische Person entsprechend der Verfügungsbefugnis des Rechtsgutträgers[48] einwilligen, nicht aber jeder einzelne betroffene Mitarbeiter, dessen schützenswerte Daten möglicherweise durch den White Hacker kompromittiert werden. Dieses Problem stellt sich auch dem *Grey Hat Hacker,* welcher sich auf die bloss mutmassliche und nicht ausdrückliche Einwilligung des Verletzten berufen wird. Zudem wird sein Handeln zumindest teilweise durch Art. 144bis Ziff. 2 StGB erfasst.

IV. Hacking und Hacker aus privatrechtlicher Sicht

A. Allgemein

Die privatrechtliche Einordnung des (White) Hackings richtet sich grundsätzlich nach der vertraglichen oder quasivertraglichen Realität des Einzelfalls. Da eine generelle Einordnung den Rahmen dieses Beitrags sprengen würde, drängt sich der Untersuch des Hackings anhand eines schweizweit bekannten Beispiels auf: Vom 25. Februar bis 24. März 2019 stellte die Schweizerische Post ihr (umstrittenes[49]) E-Voting-System einem öffentlichen Intrusionstest zur Verfügung.[50] Hacker aus aller Welt wurden dabei aufgerufen, die von Scytl entwickelte Technologie auf Herz und Nieren zu prüfen.[51] Dabei wurden die (White) Hacker gebeten, sich auf einer Website zu registrieren und einen Verhaltenskodex zu unterschreiben.[52] Im Falle des Erfolgs wurden diesen Prämien je nach Art des Hackings in Aussicht gestellt.[53]

Im Anschluss an die Offenlegung des Quellcodes im Februar 2019 haben Forschende erhebliche Sicherheitslücken am neuen, vollständig verifizierbaren System der

---

43 BGE 129 IV 315.

44 Andreas Donatsch/Carolin Hürlimann, Entwicklungen im Strafrecht, SJZ 2004, 541 ff., 543.

45 Stratenwerth/Jenny/Bommer (FN 32), 283.

46 CR CP II-Monnier (FN 33), Art. 179^{novies} N 6.

47 Caroline Guhl, Trotz rechtswidrig beschaffter Beweise zu einem gerechten Urteil, Zürich 2018, 108.

48 Andreas Donatsch/Brigitte Tag, Strafrecht I, Verbrechenslehre, 9. A., Zürich 2013, 256.

49 Zur Einführung des E-Votings gab es immer wieder kritische Stimmen, insbesondere bezüglich der Sicherheit. Bereits in seinem ersten Bericht im Jahr 2002 hebt der Bundesrat die Risiken dieser neuen Abstimmungsmethode hervor. Vgl. dazu Bericht vom 9. Januar 2002 über den Vote électronique, Chancen, Risiken und Machbarkeit elektronischer Ausübung politischer Rechte, BBl 2001-2575, 645 ff., 647 und 656 ff. Diese Befürchtung wird insofern untermauert, als Ende 2018 das E-Voting-System des Kantons Genf von Hackern des Chaos Computer Club Schweiz angegriffen und ausgehebelt wurde.

50 Statt vieler Erich Aschwanden, Sicherheitstest fürs E-Voting: Wer erfolgreich hackt, erhält bis zu 50 000 Franken, NZZ vom 7.2.2019, Internet: https://www.nzz.ch/schweiz/wer-e-voting-hackt-erhaelt-bis-zu-50-000-franken-ld.1458123 (Abruf 5.12.2019).

51 Gemäss den Angaben von swissinfo.ch hatten sich bis 13. Februar 2019 knapp 1800 Hacker angemeldet: 28% stammen aus der Schweiz, 15% aus Frankreich, 6% aus den USA und 5% aus Deutschland. Vgl. dazu Susan Misicka, E-Voting – Schweizerische Post lässt Hacker-Armada auf eigenes E-Voting-System los, Onlinebeitrag vom 14.2.2019, Internet: https://www.swissinfo.ch/ger/politik/e-voting_schweizerische-post-laesst-hacker-armada-auf-eigenes-e-voting-system-los/44755812 (Abruf 5.12.2019).

52 Vgl. dazu Internet: www.onlinevote-pit.ch (Abruf 5.12.2019).

53 Die höchste Vergütung wurde mit CHF 30'000–50'000 für eine unentdeckte Manipulation in Aussicht gestellt, vgl. Internet: www.onlinevote-pit.ch (Abruf 5.12.2019).

Schweizerischen Post offengelegt.[54] Je nach Sicht kann somit von einer (un-)erfreulichen Übung gesprochen werden. Doch wie lässt sich eine solche Aufforderung zum Hacking rechtlich einordnen?

B. Auslobung nach Art. 8 OR

1. Allgemein

Während sich private vertragliche Vereinbarungen zwischen zwei oder mehreren Parteien generell nach Auftragsrecht (Art. 394 OR ff.) richten dürften,[55] handelt es sich beim Hacking-Aufruf an die Öffentlichkeit wie beim oben dargestellten Beispiel der Schweizerischen Post um eine Auslobung gemäss Art. 8 OR. Hier verpflichtet sich der Erklärende bzw. Auslobende durch ein einseitig bedingtes Rechtsgeschäft öffentlich, an einen unbestimmten Kreis von Personen eine Belohnung zu entrichten, sofern mindestens ein Adressat eine vorausgesetzte Leistung erbringt.[56] Der Auslobende hat dabei ein Interesse an der Leistung, wobei nicht restlos geklärt scheint, ob der Auslobungszweck dem eigenen Interesse dienen muss.[57]

Bei der Auslobung handelt es sich insofern um einen «Fremdkörper», als sich ihr Geltungsgrund weniger nach klassischer Konsenslehre, sondern eher nach dem Grundsatz von Treu und Glauben richtet: Geschützt wird nicht das Vertrauen der konkret (ausführenden) Einzelperson, sondern vielmehr das kollektive Vertrauen der Öffentlichkeit in die Erklärung, dass der Auslobende die eingeforderte Leistung nicht unentgeltlich beziehen werden wird. So wäre es stossend, trotz erhöhter Erfolgsaussichten infolge Aussicht einer Vielzahl möglicher Leistungserbringer auf die auf die Leistung auszurichtende Belohnung nur deshalb zu verzichten, weil es an einer (ausdrücklichen) Annahme fehlte.[58]

Die Auslobung nach Art. 8 OR ist im vorliegenden Kontext abzugrenzen von der Auskündigung bzw. der Einladung zur Offertstellung nach Art. 7 Abs. 2 OR, welche kein verbindliches Angebot darstellt. Hier gilt es jedoch zu beachten, dass bei einer unverbindlichen Anfrage zum Hacking mit in Aussicht gestellten Erfolgsprämien bei einer sehr selektiven Auswahl an Hackern bald einmal von einer antizipierten Annahmeerklärung ausgegangen werden könnte.[59] Des Weiteren ist die Auslobung zum Hacking von der Submission abzugrenzen, daher der öffentlichen Ausschreibung für die Vergabe von Hacking-Aufträgen, denn hier fehlt das bedingte Leistungsversprechen.[60]

2. Auslobungserklärung

Die Auslobung erfolgt in Form einer Willenserklärung, gemäss welcher der Erklärende seinen entsprechend der Auslobung bedingten Verpflichtungswillen manifestiert. Entscheidend ist zunächst der wirkliche Wille. Fehlt ein solcher oder kann er nicht eruiert werden, liegt ein normativer Wille vor, sofern die Adressaten nach Treu und Glauben und unter Berücksichtigung der Umstände die Willenserklärung des Erklärenden entsprechend verstehen durften und mussten.[61] Die Erklärung ist an keine besondere Form gebunden.[62] Da sich eine Auslobung an nicht von vornherein individuell bestimmte Teilnehmer richtet, reicht es bei einer Auslobung zum Hacking aus, wenn die abgegebene Erklärung generell-abstrakt geeignet ist, beim durchschnittlichen Hacker den Eindruck des bedingten Verpflichtungswillens des Erklärenden hervorzurufen. Die Auslobungserklärung beim Beispiel der Schweizerischen Post erfolgte durch die Medienmitteilung der Bundeskanzlei.[63]

---

54 Vgl. dazu die Medienmitteilung der Bundeskanzlei vom 12.3.2019, Offenlegung des Quellcodes führt zur Entdeckung eines Mangels im neuen E-Voting-System der Post, Internet: https://www.bk.admin.ch/bk/de/home/dokumentation/medienmitteilungen.msg-id-74307.html (Abruf 5.12.2019).

55 Beim Grey Hat Hacker, der keinen Schaden verursacht und dem Geschäftsherrn mitteilt, wie er (akute oder eklatante) Sicherheitslücken beseitigen kann, erscheint die Anwendung der Geschäftsführung ohne Auftrag nach Art. 419 ff. OR zumindest vorstellbar.

56 KGer SG, BO.2011.22/23, 8.3.2012, E. 4d. Für die Lehre statt vieler Wilhelm Schönenberger/Peter Jäggi, Zürcher Kommentar, Obligationenrecht, Kommentar zur 1. und 2. Abteilung (Art. 1–529 OR), Teilband V1a, Zürich 1973 (zit. ZK-Verfasser), Art. 8 OR N 6 ff.

57 BSK OR I-Zellweger-Gutknecht, Art. 6 N 1 m.w.H., in: Corinne Widmer Lüchinger/David Oser (Hrsg.), Obligationenrecht I, Basler Kommentar, 7. A., Basel 2019 (zit. BSK OR I-Verfasser); KUKO OR-Wiegand/Hurni, Art. 8 N 2, in: Heinrich Honsell (Hrsg.), Kurzkommentar OR, Basel 2014 (zit. KUKO OR-Verfasser). Nicht von einem einseitig bedingten Rechtsgeschäft, sondern von einem Antrag (Auslobung) und der daraufhin erbrachten Leistung als Realakzept scheint in neuerer Zeit noch Hans Merz, Vertrag und Vertragsschluss, Freiburg 1992, N 267, auszugehen.

58 Vgl. BGE 39 II 591 E. 6, wonach der Tatbestand der Auslobung angenommen wurde, obwohl der Leistende von der Auslobung keine Kenntnis hatte: «Die Auslobung ist perfekt, sobald ihr Urheber alles getan hat, was nach Umständen von seiner Seite getan werden musste, um ein Versprechen zur Kenntnis der dafür in Betracht kommenden Personen gelangen zu lassen.»

59 Vgl. dazu BSK OR I-Zellweger-Gutknecht (FN 57), Art. 7 N 7.

60 BGE 46 II 369 E. 2.

61 BSK OR I-Zellweger-Gutknecht (FN 57), Art. 7 N 16.

62 BGE 39 II 591 E. 6.

63 Medienmitteilung der Bundeskanzlei vom 7.2.2019, Öffentlicher Intrusionstest für E-Voting findet im Februar und März 2019 statt, Internet: https://www.admin.ch/gov/de/start/dokumentation/medienmitteilungen.msg-id-73898.html (Abruf 5.12.2019).

3. Öffentlichkeit

Die Erklärung zur Auslobung muss *öffentlich* sein.[64] Sie muss sich grundsätzlich an mindestens eine unbestimmte Person richten. In Übereinstimmung mit der heutigen Lehre ist es auch ausreichend, wenn der Personenkreis beschränkt wird, solange die Teilnehmer nicht individuell bestimmt sind.[65]

Durch die Medienmitteilung der Bundeskanzlei wurde die Auslobung öffentlich an einen unbestimmten Personenkreis, nämlich sämtliche (fähigen) Hacker, gerichtet. Nach dem Gesagten wäre es auch möglich, den Adressatenkreis auf eine oder mehrere bestimmte Hacker-Gruppen zu beschränken, jedenfalls solange keine Personen individuell bestimmt sind. Dies setzt voraus, dass die Gruppe über eine bestimmte Anzahl an Mitgliedern verfügt, da sich bei einer Gruppe mit wenigen Teilnehmern irgendwann eben doch die individuelle Bestimmtheit offenbart. Keine Rolle spielt hingegen, ob in Tat und Wahrheit nur wenige Hacker im Stande sind, die Bedingung überhaupt zu erfüllen.

4. Leistung

Die Adressaten müssen die in der Auslobung umschriebene Leistung erbringen.[66] Diese kann *beliebig* geartet sein und deshalb sowohl ein Tun als auch ein Unterlassen beinhalten.[67] Die Leistung kann auch bloss ideeller Natur sein. Des Weiteren – und hier von Interesse – kann auch eine Schädigung oder ein Eindringen eine Leistung sein, wobei hier nicht der Schadenseintritt, sondern vielmehr das Erschaffen oder Testen von Sicherheit beim Betroffenen im Zentrum steht.[68]

Im Weiteren darf die Leistung gemäss allgemeinen Grundsätzen des Obligationenrechts weder unmöglich noch rechts- oder sittenwidrig sein, andernfalls deren Nichtigkeit droht.[69] Die Rechtswidrigkeit – insbesondere bezüglich der einschlägigen strafrechtlichen Normen[70] – entfällt im vorliegenden Beispiel, weil durch den Aufruf zum Eindringen der Auslobende bzw. die Schweizerische Post in die entsprechende Handlung einwilligt («volenti non fit iniura»).[71] Die Auslobung verstösst auch nicht gegen die herrschende Moral bzw. das allgemeine Anstandsgefühl oder gegen die der Gesamtrechtsordnung immanenten ethischen Prinzipien und Wertmassstäbe, weil das Testen von Datenverarbeitungsanlagen oder technischen Einrichtungen zum Alltag gehört; hier wird lediglich der Kreis der zum Eindringen Aufgerufenen gesondert gewählt. Auch Sittenwidrigkeit infolge Leistungsinäquivalenz ist zu verneinen,[72] beispielsweise nach wochenlangen Versuchen des Eindringens infolge Ausbezahlung geringer, jedoch im Voraus festgelegter Erfolgsprämien, weil dieser Übung immanent ist, dass der Aufwand ungewiss ist. Insofern ist die Erfolgsprämie des sekundenschnellen Eindringens auch nicht herabzusetzen. Schliesslich wird die Auslobung zu Intrusionstests insofern nicht anfänglich objektiv unmöglich sein, als objektiv in praktisch jedes technische System eingedrungen werden kann.

Zeitlich muss die geforderte Leistung *nach* der Auslobung erfolgen und die Leistung kann an eine Frist gebunden werden.[73] Ohne Fristansetzung endet die Erbringbarkeit, sobald der Auslobende für den Dritten erkennbar kein Interesse mehr an der Leistung hat.[74] Die Post hat für den Intrusionstest eine Frist vom 25. Februar bis 24. März 2019 vorgesehen, was ohne weiteres zulässig ist. Allerdings tauchte der entsprechende Source-Code bereits vor dem vorgesehenen Zeitfenster auf. Hier stellt sich die Frage, ob entsprechende Hacking-Erfolge vor dem Zeitfens-

---

64 Statt vieler CHK-Kut, Art. 8 OR N 5, in: Marc Amstutz et al. (Hrsg.), Handkommentar zum Schweizer Privatrecht, 3. A., Zürich 2016 (zit. CHK-Verfasser). Dies wurde durch das Bundesgericht in BGE 39 II 591 insofern relativiert, als es eine Niederschrift in einem Polizeirapport für ausreichend hielt. Vgl. ferner ZK-Schönenberger/Jäggi (FN 56), Art. 8 OR N 8 m.w.H., welche als Empfänger eine bestimmte Person akzeptieren, sofern die Erklärung in der Meinung an sie gerichtet wird, dass jede Drittperson, welche die im Versprechen umschriebene Bedingung erfüllt, daraus berechtigen kann.

65 BSK OR I-Zellweger-Gutknecht (FN 57), Art. 7 N 16; CHK-Kut (FN 64), Art. 8 OR N 5; OFK-Kostkiewicz, in: Jolanta Kren Kostkiewicz/Stephan Wolf/Marc Amstutz/Roland Fankhauser (Hrsg.), Kommentar Schweizerisches Obligationenrecht, 3. A., Zürich 2016 (zit. OFK-Verfasser), Art. 8 OR N 3. Vgl. auch KGer ZG, in: SJZ 1992, 255.

66 Statt vieler CHK-Kut (FN 64), Art. 8 OR N 6.

67 Ausführlich dazu ZK-Schönenberger/Jäggi (FN 56), Art. 8 OR N 15 ff.

68 BSK OR I-Zellweger-Gutknecht (FN 57), Art. 8 N 22.

69 OFK-Kostkiewicz (FN 65), Art. 8 OR N 6; KUKO OR-Wiegand/Hurni (FN 57), Art. 8 N 4; ZK-Schönenberger/Jäggi (FN 56), Art. 8 OR N 39.

70 Siehe dazu oben III.

71 BSK StGB II-Weissenberger (FN 33), Art. 143bis N 22 m.w.H. Die Legitimation dieses Grundsatzes beruht auf dem Gedanken der Selbstbestimmung. Ausführlich dazu – wenn auch für das deutsche Recht – Ansgar Ohly, «Volenti non fit iniuria», Die Einwilligung im Privatrecht, München 2001.

72 Vgl. dazu BGE 115 II 323 E. 4c; BGer, 4A_542/2012, 24.1.2013; BGer, 4A_18/2011, 5.4.2011, sowie CHK-Kut (FN 64), Art. 19–20 OR N 27 m.w.H., wonach Art. 21 OR als abschliessende Regelung bezüglich Leistungsinäquivalenz angeschaut wird. Hingegen hat das Bundesgericht die Sittenwidrigkeit überhöhter Darlehenszinse bejaht (vgl. BGer, 4A_69/2014, 28.4.2014).

73 BSK OR I-Zellweger-Gutknecht (FN 57), Art. 8 N 24 f.

74 BSK OR I-Zellweger-Gutknecht (FN 57), Art. 8 N 25; CHK-Kut (FN 64), Art. 8 OR N 7.

ter als Leistungserfüllung hätten eingestuft werden müssen. Dies ist nach vorliegender Meinung zu verneinen, da es am Erklärenden bzw. an der Schweizerischen Post lag, die zeitlichen Spielregeln für die Leistungserbringung festzulegen.[75]

Mangels ausdrücklich anderslautender Anordnung ist durch Auslegung zu ermitteln, ob die Belohnung nur an den ersten, der die umschriebene Bedingung erfüllt, oder auch an jeden nachfolgenden Leistungserbringer zu entrichten ist. Dabei ist davon auszugehen, dass sie im Zweifel nur einmal geschuldet ist, und zwar demjenigen, der seine Leistung dem Auslobenden zuerst angezeigt hat.[76] Haben nach einer Auslobung mehrere Hacker gemeinsam die Bedingung erfüllt, hat mangels anderer Anordnung jeder Mitwirkende nach billigem Ermessen Anspruch auf seinen Anteil an der Erfolgsprämie.[77] Die Post hat angezeigt, dass insgesamt CHF 150'000 für die Ausrichtung von Erfolgsprämien zur Verfügung stehen, und damit zum Ausdruck gebracht, dass sie lediglich bis zu diesem Betrag die bedingte Leistung verspricht.[78]

5. Bedingtheit

Als einseitige Verpflichtung ist die Leistungsvornahme suspensiv bedingt, weshalb diese erst durch Erbringen der gemäss Auslobung umschriebenen Leistung, dann jedoch *ipso iure* fällig wird.[79] Beim Beispiel der Schweizerischen Post wird die Leistung vom ungewissen Ereignis der Intrusion ins Datensystem abhängig gemacht und dabei genau umschrieben, welches Eintreten des ungewissen Ereignisses wie vergütet wird.[80] Fordert ein Hacker die Erfolgsprämie ein, liegt es – nach nicht unumstrittener – Auffassung am Auslobenden, den Nichteintritt der Bedingung zu beweisen.[81] Fraglich erscheint, ob auch bei einer Teilerfüllung der Bedingung entsprechend ein Teil der Erfolgsprämie zu entrichten ist. Dies ist zu verneinen,[82] da es am Auslobenden liegt, den Inhalt der Bedingung, deren Erfüllung die eigene Leistungspflicht auslöst, entsprechend eigener Vorstellung zu umschreiben.

Der zum Hacking Auslobende hat zu beachten, dass er – beispielsweise nach ersten Eindringenserfolgen – durch Code- oder System(zugriffs)anpassungen nach erfolgter Auslobung allenfalls Gefahr läuft, dass das einseitige Leistungsversprechen infolge treuwidriger Verhinderung des Bedingungseintritts wirksam wird.[83] Demgegenüber steht es dem «Angegriffenen» und Auslobenden jederzeit zu, – in gleicher Form – von der Auslobung zurückzutreten,[84] wodurch jedoch ein Anspruch auf Ersatz derjenigen Aufwendungen anfallen kann, die bis zum Widerruf in guten Treuen erbracht wurden.[85]

C. Arbeitsrechtliche Fürsorgepflicht nach Art. 328 OR

Die allgemeine Treuepflicht des Arbeitnehmers hat ihr Gegenstück bekanntlich in der Fürsorgepflicht des Arbeitgebers.[86] Der Arbeitnehmer hat im Rahmen seiner arbeitsrechtlichen Sorgfaltspflicht nach Art. 321a OR Schaden für den Arbeitgeber abzuwenden, indem er u.a. dafür sorgt, dass durch seinen normalen geschäftlichen Gebrauch keine *Malware* oder *Ransomware* auf die Datenverarbeitungsanlage des Arbeitgebers heruntergeladen wird. Wenn der Arbeitnehmer angemessen sicherstellen muss, dass den berechtigten Interessen des Arbeitgebers durch sachgemässen Gebrauch von Datenverarbeitungsgeräten Rechnung getragen wird, muss dies *e contrario* auch für den Persönlichkeitsschutz der Arbeitnehmer nach Art. 328 OR und damit bezüglich des Schutzes privater bzw. besonders schützenswerter Daten des Mitarbeiters gelten. Eine Möglichkeit, diesen Schutz gegenüber (unerwünschten) Hackangriffen zu gewährleisten und zu verbessern, ist der regelmässige Einsatz von (erwünschten) White Hackern zur Feststellung von möglichen Schwachstellen.

---

75 Für die Möglichkeit der Leistungserfüllung spricht sich Hermann Becker, Berner Kommentar zum schweizerischen Privatrecht, Allgemeine Bestimmungen, Art. 1–183 OR, Bern 1945, Art. 8 OR N 34, aus. Wie hier dagegen BSK OR I-Zellweger-Gutknecht (FN 57), Art. 8 N 24.

76 CHK-Kut (FN 64), Art. 8 OR N 7; ZK-Schönenberger/Jäggi (FN 56), Art. 8 OR N 52.

77 ZK-Schönenberger/Jäggi (FN 56), Art. 8 OR N 51.

78 Vgl. Internet: www.onlinevote-pit.ch (Abruf 5.12.2019).

79 Eine Annahmeerklärung braucht es nicht. Vgl. KUKO OR-Wiegand/Hurni (FN 57), Art. 8 N 4; ZK-Schönenberger/Jäggi (FN 56), Art. 8 OR N 34, die diesbez. von einer Abschwächung des Vertragsprinzips sprechen.

80 Vgl. Internet: www.onlinevote-pit.ch (Abruf 5.12.2019).

81 BGer, 4C.264/2004, 20.10.2004, E. 3.4; BGer, 4C.212/2004, 25.10.2004, E. 3.1; OGer ZH, TR120028, 25.4.2012, E. 4.2 (sog. «Einwendungstheorie»). A.M. KUKO OR-Honsell (FN 57), Art. 151 N 10 m.w.H.; Andreas von Tuhr/Arnold Escher, Allgemeiner Teil des Schweizerischen Obligationenrechts, Band II, Zürich 1974, 263 (sog. «Leugnungstheorie»).

82 Ebenso CHK-Kut (FN 64), Art. 8 OR N 8.

83 Vgl. dazu Art. 156 OR.

84 Explizit steht dies im deutschen Recht (Art. 658 BGB). Vgl. zum Ganzen BSK OR I-Zellweger-Gutknecht (FN 57), Art. 8 N 38 f.

85 ZK-Schönenberger/Jäggi (FN 56), Art. 8 OR N 70 ff.

86 Statt vieler CHK-Emmel (FN 64), Art. 321a OR N 1 ff.

V. Hacking und Hacker aus datenschutzrechtlicher Sicht

A. Schutz personenbezogener Daten

Gemäss Art. 13 Abs. 2 BV sind persönliche Daten bzw. Personendaten geschützt (sog. «Recht auf informationelle Selbstbestimmung»).[87] Solche Daten liegen vor, wenn sich diese auf eine bestimmte oder bestimmbare Personen beziehen.[88] Personendaten dürfen bekanntlich nach Schweizer Rechtsordnung nur rechtmässig bearbeitet werden.[89] Einschränkungen von diesem Grundsatz unterliegen den allgemeinen Voraussetzungen von Art. 36 BV.[90] Zu den Schutzrechten der Datenschutzsubjekte gehören das Recht auf Berichtigung (Art. 5 Abs. 2 DSG), das Recht auf Auskunft (Art. 8 DSG) sowie spezifische Rechte gegenüber Privaten sowie gegenüber Bundesorganen.[91] Im Geflecht zur Aufstellung adäquater Datenschutzmechanismen spielen überdies die Erfordernisse des sog. «Privacy by Design» (Einbezug des Datenschutzes in der Projektphase) sowie des «Privacy by Default» (datenschutzfreundliche Voreinstellungen) voraussichtlich eine zentrale Rolle.[92]

B. Konkludente Einwilligung?

Art. 7 DSG hält fest, dass Personendaten durch technische und organisatorische Massnahmen gegen unbefugtes Bearbeiten geschützt werden müssen.[93] Durch die Formulierung des Gesetzgebers wird klar, dass er bei der Betrachtung von Datenbearbeitungen das Datenschutzgesetz auch als das Technikfolgerecht verstanden hatte, wobei Organisation und Technik dazu beitragen sollen, die datenschutzrechtlichen Zielsetzungen zu erreichen.[94] Dieser datenschutzrechtliche Auftrag liefert einen starken Nachweis des Interesses, bestehende Systeme bzw. Datenverarbeitungsanlagen – beispielsweise durch (White) Hacker mittels Auslobung zur Intrusion – überprüfen zu lassen. Denn das Interesse an der Datensicherheit besteht nicht nur auf Seiten des Datenverarbeiters, sondern auch auf Seiten der geschützten Personen.[95] Dessen ungeachtet vermag dieses Interesse – auch bei vorgängiger und angemessener Information der Betroffenen[96] – eine Einwilligung der geschützten Subjekte nicht zu rechtfertigen.[97] Noch deutlicher wird dieser Befund aus strafrechtlicher Sicht, jedenfalls in Bezug auf besonders schützenswerte Personendaten oder Persönlichkeitsprofile.[98] So wird klar, dass bei einer Auslobung zum Hacking die Spielregeln und (System-)Voraussetzungen so zu wählen sind, dass potenziell Personendaten weder erlangt noch verarbeitet werden können. Andernfalls riskiert der Auslobende die Gefahr, gegen datenschutzrechtliche oder strafrechtliche Normen zu verstossen. Entsprechend erstaunt es nicht, dass die Schweizerische Post bei der Auslobung zum Intrusionstest genaue Spielregeln aufgestellt hat.[99]

---

87 Grundlegend dazu ist das sog. «Volkszählungsurteil» des deutschen Bundesverfassungsgerichts. Vgl. BVerfG 65, 1, 15.12.1983, 41 ff. Relevant bezüglich Schutzgehalt sind freilich zusätzliche Normen, beispielsweise Art. 8 EMRK, Art. 28 ZGB oder Art. 179 StGB, wodurch ein Schutzgeflecht entsteht. Die vorliegende Abhandlung beschränkt sich weitgehend auf Schweizer Recht. Bekanntlich kann insbesondere die DSGVO, welche spätestens seit dem 25. Mai 2018 für alle EU-Mitgliedstaaten verbindlich ist, Anwendung auf Schweizer Unternehmen finden. Ebenso bleibt das E-DSG ausser Betracht (vgl. zur Revision des DSG Botschaft vom 15. September 2017 zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz, BBl 2017 6941 ff. [zit. Botschaft Datenschutz]).

88 Art. 3 lit. a DSG.

89 Art. 4 Abs. 1 DSG. Bearbeiten ist in einem weiten Sinne zu verstehen und umfasst auch das Beschaffen, Aufbewahren, Verwenden, Umarbeiten, Vernichten etc. von Daten. Vgl. DSG-Schweizer/Rechsteiner, in: Nicolas Passadelis/David Rosenthal/Hanspeter Thür (Hrsg.), Datenschutzrecht, Basel 2015 (zit. DSG-Verfasser), 47 ff.

90 DSG-Gerschwiler (FN 89), 83.

91 Zum Ganzen DSG-Widmer (FN 89), 149 ff.

92 Diese Grundsätze sollen auch ins Schweizer Recht überführt werden. Vgl. dazu Botschaft Datenschutz (FN 87), 6941 ff. Diese Grundsätze finden heute bereits mit Art. 25 der EU-Datenschutz-Grundverordnung (DSGVO) – und damit je nachdem auch auf Schweizer Unternehmen, sofern diese in deren Geltungsbereich fallen – Anwendung.

93 Es gilt der sog. «risikobasierte Ansatz». Vgl. auch die einschlägige Konkretisierung in Art. 8–12 sowie 20–23 VDSG. So besteht beispielsweise die Pflicht zur Implementierung von Zugangs-, Personendatenträger-, Transport-, Bekanntgabe-, Speicher-, Benutzer-, Zugriffs- oder Eingabekontrollen (Art. 9 VDSG).

94 SHK DSG-Baeriswyl, in: Bruno Baeriswyl/Kurt Pärli (Hrsg.), Datenschutzgesetz (DSG), Bern 2015 (zit. SHK DSG-Verfasser), Art. 7 N 3.

95 Siehe dazu auch oben die Überlegung bezüglich arbeitsrechtlicher Fürsorgepflicht, IV.C.

96 Vgl. SHK DSG-Baeriswyl (FN 94), Art. 4 N 58, wonach eine Datenverarbeitung im klaren Interesse der betroffenen Person auch durch nachträgliche Information und Einwilligung gerechtfertigt werden kann.

97 Zur Einwilligung SHK DSG-Baeriswyl (FN 94), Art. 4 N 54 ff.

98 Vgl. Art. 179novies StGB. Siehe dazu oben III.F.

99 Vgl. dazu Terms, Conditions and Code of Conduct der Schweizerischen Post, 5.3, Internet: www.onlinevote-pit.ch (Abruf 5.12.2019).

VI. Schlussbemerkungen (de lege ferenda?)

Hacking hat einen schlechten Ruf, denn oftmals werden damit Schäden für Einzelpersonen, Websites oder Informationssysteme in Verbindung gebracht. Der gesetzeskonforme Einsatz von *White Hackern* bietet sich jedoch vermehrt an, um allfällige Sicherheitslücken im System unter geregelten Bedingungen aufzudecken und zu schliessen. Werden *White Hacker* beauftragt, gilt es, die strafrechtlichen, zivilrechtlichen sowie datenschutzrechtlichen Konsequenzen bzw. Gebote und Verbote zu beachten – und zwar je nachdem, in welcher Rechtsform die Zusammenarbeit gewählt wird. Es wäre wünschenswert, wenn der Gesetzgeber das *White Hacking* gesetzlich regelt oder sich zumindest zu dieser Figur äussert, um Rechtssicherheit und Akzeptanz zu schaffen. Der wirksame Einsatz von White Hackern zur Verbesserung des effektiven Schutzes der Datenverarbeitungsanlagen und der schützenswerten Personendaten würde damit erleichtert. Vorstellbar wäre beispielsweise ein Leitfaden für Unternehmen oder ein Positionspapier des Bundes, des eidgenössischen Datenschutzbeauftragten (EDÖB) oder – bei einer allfälligen Revision – die Anpassung einschlägiger Gesetze.