Journal für Strafrecht 5, 30-38 (2018)
https://elibrary.verlagoesterreich.at
JSt 2018, 30

Strafrechtliche Implikationen des „WannaCry"-Angriffes – aus Sicht von Tätern und Opfern

In der heutigen, digitalisierten Welt steigt auch die Zahl an „digitalen Verbrechen" stetig an. Dies hat zuletzt der weit verbreitete „WannaCry-Trojaner" gezeigt. Wie derartige Angriffe nach österreichischem Strafrecht zu beurteilen sind und warum sich auch die Opfer sogenannter Ransomware strafbar machen können, soll dieser Beitrag aufzeigen.

Deskriptoren: WannaCry, WannaCry-Trojaner, Ransomware, Erpressungssoftware, Computerkriminalität, Cybercrime, Erpressung, Beteiligung an krimineller Organisation, Zahlung von Lösegeld, Notstand.
Normen: § 126a StGB; § 144 StGB; § 146 StGB; § 278 StGB.

Von Christopher Kahl und Alexander Stücklberger

1. Einleitung[1]

Die neuesten Berichte zur Kriminalitätsentwicklung in Österreich zeigen, dass das Cyberstrafrecht stetig an Bedeutung gewinnt.[2] Neben „Denial-of Service"-Angriffen rückten in letzter Zeit vor allem Angriffe mittels Ransomware in das Zentrum der medialen Aufmerksamkeit. Der bekannteste dieser Ransomware-Angriffe erfolgte unlängst mittels des sogenannten „WannaCry"-Trojaners, der Schätzungen zufolge über 230.000 Computer in 150 Ländern infiziert hat. Betroffen waren neben zahlreichen Privatpersonen auch große Unternehmen wie die Deutsche Bahn, aber auch öffentliche Stellen wie Krankenhäuser in Großbritannien oder das russische Innenministerium.[3]
Der Begriff der Ransomware beschreibt eine Unterart der als Trojaner bekannten Kategorie von Schadsoftware.[4] Einmal im System freigesetzt, verschlüsseln diese Trojaner Benutzerdaten am Computer und fordern den Benutzer automatisch dazu auf, einen bestimmten Betrag in Bitcoins zu bezahlen, um die Daten wieder zu entsperren. Um die strafrechtlichen Implikationen dieser und vergleichbarer Schadsoftware aufzuzeigen, soll im Folgenden davon ausgegangen werden, dass drei Täter gemeinsam den „WannaCry"-Trojaner geschrieben und verbreitet haben. Da auch die Frage, ob die Täter die befallenen Computer nach Zahlung des geforderten Betrages tatsächlich wieder freischalten wollen, eigene strafrechtliche Folgen hat, soll diese Konstellation genauso wie eine mögliche Strafbarkeit des Opfers bei Bezahlung des geforderten Betrages ebenfalls berücksichtigt werden.

2. Strafbarkeit der Hacker – ein Überblick

Durch das Schreiben und Inverkehrbringen des Trojaners kommt eine Reihe von Delikten in Betracht. Um den gegebenen Rahmen nicht zu überschreiten, soll im Folgenden nur auf die wesentlichsten Delikte eingegangen werden.

2.1. § 126a StGB – Datenbeschädigung

Jedenfalls könnten die Täter eine Datenbeschädigung gem § 126a StGB verwirklichen. Nach dieser Bestimmung ist zu bestrafen, wer Daten, über die er nicht alleine verfügen darf, verändert, unterdrückt, löscht oder sonst unbrauchbar macht und sein Opfer dadurch schädigt. Dass die Täter über die Daten auf den betroffenen Computern nicht verfügungsberechtigt sind, liegt auf der Hand. Durch die Verschlüsselung wird mangels inhaltlicher Veränderung des Aussagewertes bzw Informationsgehaltes in aller Regel zwar keine Veränderung der Daten bewirkt[5], doch liegt darin eine Unterdrückung, da der Trojaner den Zugriff auf die verschlüsselten Daten

1 Wir bedanken uns bei Lorenz Benedikt Schilling für seine tatkräftige Unterstützung bei der Erstellung dieses Aufsatzes.
2 So die polizeiliche Kriminalitätsstatistik. Siehe http://www.bmi.gv.at/cms/BK/publikationen/krim_statistik/2016/Web_Sicherheit_2016.pdf (8.10.2017).
3 Siehe zB Der Standard vom 27.10.2017, Britische Regierung: Nordkorea für 'WannaCry'-Attacke verantwortlich, http://derstandard.at/2000066776392/Britische-Regierung-Nordkorea-fuer-WannaCry-Attacke-verantwortlich (8.11.2017).
4 *Salomon*, Cybercrime und Lösegeld – Strafbarkeit der Zahlung von Lösegeld als Reaktion auf Erpressungstrojaner, MMR 2016, 575 (575 ff).
5 *Komenda/Madl* in SbgK § 126a Rz 42; *Leukauf/Steininger/Messner*, StGB[4] (2017) § 126a Rz 8.

zumindest temporär verhindert, sodass der Verfügungsberechtigte sie im betreffenden Zeitraum nicht mehr verwenden kann.[6]

§ 126a StGB verlangt zur Vollendung den Eintritt eines Schadens beim Opfer. Als geschütztes Rechtsgut des § 126a StGB ist jedoch nicht nur das Vermögen des Opfers, sondern auch der Fortbestand und die Verfügbarkeit der Daten als solches anzunehmen[7], weshalb es auf die Beeinträchtigung vermögenswerter Dateien hier nicht ankommt. Der Erfolg der Datenbeschädigung kann somit neben der Verwirklichung eines Vermögensschadens – die Höhe des Vermögensschadens wird hier mit den Kosten der Wiederbeschaffung beziffert – auch in der Beeinträchtigung des reinen Affektionsinteresses bestehen.[8] Aus diesem Grund würde die Verschlüsselung nicht wiederherstellbarer Familienfotos selbst bei fehlender Vermögensschädigung eine Datenbeschädigung konstituieren, da durch die Verschlüsselung in das Interesse an der Verfügbarkeit der Daten eingegriffen wird.

Die Beeinträchtigung des Affektionsinteresses kann im Gegensatz zum objektiv feststellbaren Vermögensschaden nur anhand des subjektiven Interesses des Opfers am Fortbestand der Daten festgestellt werden. So liegt etwa kein Schaden iSd § 126a StGB vor, wenn nur wertlose Datensätze von der Verschlüsselung betroffen sind, die der Verfügungsberechtigte nicht mehr benötigt oder die er ohnedies zur Löschung bestimmt hatte. Mangels Kosten der Wiederherstellung oder Eingriff in das Affektionsinteresse entfällt in diesen Fällen die Strafbarkeit.[9] Gleiches gilt, wenn durch die Verschlüsselung zwar prinzipiell ein Vermögensschaden oder eine Beeinträchtigung des Affektionsinteresses entsteht, eine Art Bagatellschwelle jedoch nicht überschritten wird. Dies liegt dann vor, wenn die Verschlüsselung leicht rückgängig gemacht werden kann oder die Daten ohne erheblichen Aufwand wiederherstellbar bzw wiederbeschaffbar sind.[10] Erst wenn die Wiederherstellung *„für einen vernünftig denkenden Menschen ins Gewicht fällt"*[11], kann nach hA von einem strafrechtlich relevanten Schaden und damit von einer Erfüllung des Tatbestandes des § 126a StGB gesprochen werden.[12]

Trotz der hier genannten Einschränkungen der Strafbarkeit werden die Täter durch das Freisetzen des „WannaCry"-Trojaners meist den Tatbestand des § 126a StGB verwirklichen. Da in der Regel sämtliche Daten auf den betroffenen Computern verschlüsselt werden, ist es höchst unwahrscheinlich, dass nicht zumindest hinsichtlich eines dieser Datensätze in das Affektionsinteresse eingegriffen wird oder wirtschaftlich ins Gewicht fallende Wiederherstellungskosten bestehen. Ausnahmen bestehen nur dann, wenn ein leicht zugängliches und vollständiges Backup existiert, mit dessen Hilfe die betroffenen Daten innerhalb kürzester Zeit und ohne erheblichen Aufwand wiederhergestellt werden können.

2.2. § 144 StGB – Erpressung

Neben der Datenbeschädigung verwirklichen die Täter durch ihr Vorgehen augenscheinlich auch eine Erpressung nach § 144 StGB, ist es doch ihr Ziel, ihren Opfern durch Androhung eines Übels Geldzahlungen abzunötigen. Wesen der Erpressung ist, dass der Täter sein Opfer mit Gewalt oder durch gefährliche Drohung zu einer Vermögensverfügung nötigt, die das Opfer selbst oder einen Dritten am Vermögen schädigt. Dabei muss der Täter neben dem Tatbildvorsatz zusätzlich den erweiterten Vorsatz darauf besitzen, sich selbst oder einen Dritten durch das Verhalten des Opfers unrechtmäßig zu bereichern.

Da der Begriff der Gewalt iSd § 144 StGB als physische Gewalt auszulegen ist[13], bleibt für den gegenständlichen Fall nur die gefährliche Drohung als mögliches Tatmittel. Gefährlich ist eine Drohung iSd § 144 StGB dann, wenn eine Verletzung an einem der in § 74 Abs 1 Z 5 StGB taxativ aufgezählten Rechtsgüter angedroht wird, die angesichts des angedrohten Übels dazu geeignet ist, dem Adressaten begründete Besorgnisse einzuflößen. Da Körper, Ehre und Freiheit (iSd freien Fortbewegung[14]) nicht bedroht sind, kommt bloß eine mögliche Drohung an der Privatsphäre oder am Vermögen in Frage. In der Androhung, die betroffenen Daten nicht freizuschalten, liegt zwar eine Verletzung des persönlichen Lebensbereiches, doch um eine gefährliche Drohung iSd § 74 Abs 1 Z 5 StGB zu konstituieren, müsste diese Verletzung dadurch erfolgen, dass angedroht wird, die Daten anderen zugänglich zu machen oder sonst zu veröffentlichen. Dies geschieht in der zu untersuchenden Fallkonstellation aber gerade nicht, schließlich drohen

6 *Komenda/Madl* in SbgK § 126a Rz 48.
7 *Birklbauer/Hilf/Tipold*, Strafrecht Besonderer Teil I[4] (2017) § 126a Rz 4, 11; *Komenda/Madl* in SbgK § 126a Rz 17 mwN.
8 *Komenda/Madl* in SbgK § 126a Rz 51; im Ergebnis zustimmend, aber ohne Verweis auf den Bestand der Daten als geschütztes Gut auch *Leukauf/Steininger/Messner*, StGB[4] § 126a Rz 1, 14.
9 *Bertel* in WK-StGB[2] § 126a Rz 6; *Komenda/Madl* in SbgK § 126a Rz 51, 55; *Leukauf/Steininger/Messner*, StGB[4] § 126a Rz 14.
10 *Leukauf/Steininger/Messner*, StGB[4] § 126a Rz 14.
11 *Bertel/Schwaighofer/Venier*, Strafrecht Besonderer Teil I[13] (2015) § 126a Rz 2; *Reindl*, E-Commerce und Strafrecht (2003) 104.
12 *Komenda/Madl* in SbgK § 126a Rz 54 mwN.
13 RIS-Justiz RS0093591.
14 *Jerabek/Reindl-Krauskopf/Ropper/Schroll* in WK-StGB[2] § 74 Rz 30.

die Hacker nicht mit der Veröffentlichung der Daten, sondern mit der Aufrechterhaltung der Verschlüsselung. *Reindl-Krauskopf* sieht bei Ransomware-Angriffen eine gefährliche Drohung gegen das Vermögen gegeben, weil die Täter die weitere Verletzung des Eigentumsrechts durch die Sperre des Computers androhen.[15] Dies ist aber im gegenständlichen Fall nicht unbedingt zutreffend, weil der „WannaCry"-Trojaner nicht den gesamten Computer sperrt, sondern nur (viele) Dateien verschlüsselt, ohne jedoch die grundsätzliche Funktionsfähigkeit des Systems zu beeinträchtigen. Für die Drohung am Vermögen kommt es hier vielmehr darauf an, ob tatsächlich „vermögenswerte" Daten betroffen sind. Haben die Daten einen Tauschwert (zB Kundendaten) oder einen Gebrauchswert – letzterer schlägt sich ua erneut auch in den Kosten der Wiederbeschaffung nieder[16] – ist ihre Einordnung als vermögenswert unproblematisch, wären sie doch in ausgedruckter Form auch einer Sachbeschädigung zugänglich.[17] Die Drohung mit der weiteren Beeinträchtigung von Daten, an denen das Opfer zwar Affektionsinteresse besitzt, die aber keinen Vermögenswert darstellen (zB ein mit dem Mobiltelefon angefertigtes, jederzeit wiederholbares Selbstporträt), ist hingegen nicht als Drohung gegen fremdes Vermögen zu qualifizieren. Es wird zumindest irgendein objektiver Vermögenswert zu fordern sein. In der Regel wird dieses Kriterium jedoch keine Probleme bereiten, bestehen doch meist zumindest geringe Kosten der Wiederbeschaffung oder des Ersatzes. Hier wäre beispielsweise an die Wiederbeschaffung kostenpflichtiger Software oder die zur Wiederherstellung benötigte Arbeitszeit zu denken. Sind im Einzelfall keine vermögenswerten Daten von der Verschlüsselung betroffen und fallen auch keine Kosten der Wiederherstellung an, da zB ein leicht zugängliches, vollständiges und nur kurze Zeit in Anspruch nehmendes Backup existiert, kann die Drohung – bei Vorliegen des entsprechenden Vorsatzes – als nur relativ untaugliche Tathandlung jedoch eine Versuchsstrafbarkeit begründen, da die Deliktsverwirklichung aus der ex-ante-Sicht eines begleitenden Beobachters nicht denkunmöglich war.[18]

Ob die Drohung, die persönlichen Daten auf dem Computer weiter verschlüsselt zu halten, geeignet ist, dem Opfer begründete Besorgnis einzuflößen, wird anhand eines objektiv-individuellen Maßstabs beurteilt.[19] Maßgeblich ist hierbei, wie schwer das angedrohte Übel wiegt und wie wahrscheinlich seine Verwirklichung ist.[20] Im Einzelfall wird zur Beurteilung dieses Kriteriums vor allem auf die Art der Daten, deren Wert für den Nutzer und den Aufwand für eine mögliche Wiederherstellung abzustellen sein.

Neben der Gefährlichkeit der Drohung ist zu untersuchen, ob das Opfer in der gegebenen Fallkonstellation durch die Zahlung des Lösegeldes zur Entsperrung der Daten überhaupt am Vermögen geschädigt wird. Die Entscheidung des OGH im „Saliera-Fall"[21] löste eine weitreichende Diskussion in der Literatur zu einer sehr ähnlich gelagerten Frage aus: 2003 wurde die Saliera (Wert: ca 36 Mio Euro) aus dem Kunsthistorischen Museum in Wien gestohlen. In weiterer Folge verlangte der Täter für die Rückgabe ein Lösegeld in Höhe von 10 Mio Euro. In erster Instanz wurde der Täter deshalb wegen Einbruchsdiebstahls und (versuchter) Nötigung verurteilt. Das Erstgericht befand nämlich – wie auch die hL[22] – dass durch den Austausch der Saliera im Wert von 36 Mio Euro gegen das Lösegeld von 10 Mio Euro kein über den Einbruchsdiebstahl hinausgehender Vermögensschaden entstanden sein könne, der für eine Subsumtion als Erpressung notwendig wäre.[23] So würde das Opfer in einer saldierenden Betrachtungsweise zwar den Wert des Lösegeldes verlieren, dafür jedoch den höheren Wert der gestohlenen Sache wieder zurück in sein Vermögen bekommen.

Der OGH sieht in der Zahlung des Lösegeldes hingegen mangels Anrechenbarkeit der Sachrückgabe auf die abgenötigte Leistung des Lösegeldes eine erneute Vermögensschädigung des Opfers und bejaht dementsprechend die Erfüllung des Tatbestandes der Erpressung.[24] Diese Ansicht wird mit dem zivilrechtlichen Eigentumsbegriff begründet, nach dem der Eigentümer sein Eigentumsrecht an der Beute auch durch eine deliktische Wegnahme nicht verliert, sondern vielmehr Herausgabeansprüche besitzt. Hiermit würde in einer saldierenden Betrachtungsweise die Rückgabe der Beute durch den Rückgabeanspruch abgegolten werden, womit der Zahlung des Lösegeldes keine entsprechende Gegenleistung gegenübersteht, weshalb das Opfer insgesamt am Vermögen geschädigt wäre – die Sachrückgabe wäre

15 *Reindl-Krauskopf*, Cyberstrafrecht im Wandel, ÖJZ 2015, 112 (113).

16 Vgl *Jerabek/Reindl-Krauskopf/Ropper/Schroll* in WK-StGB² § 74 Rz 32 zu den vergleichbaren Fällen der Urkundenunterdrückung (Kosten der Wiederbeschaffung als Schaden am Vermögen).

17 Vgl nur *Sagmeister* in SbgK § 125 Rz 56.

18 *Hager/Massauer* in WK-StGB² §§ 15, 16 Rz 82.

19 Ausf *Kienapfel/Schroll*, Strafrecht Besonderer Teil I⁴ (2016) § 105 Rz 44 ff; *Schwaighofer* in WK-StGB² § 105 Rz 61 ff.

20 *Bertel/Schwaighofer/Venier*, BT I¹³ § 105 Rz 10 f; *Schwaighofer* in WK-StGB² § 105 Rz 63 mwN.

21 OGH 6.3.2007, 11 Os 3/07m.

22 *Bertel* in WK-StGB² § 127 Rz 50; *Birklhauer/Hilf/Tipold*, BT I⁴ §§ 144, 145 Rz 7; *Leukauf/Steininger/Flora*, StGB⁴ § 144 Rz 9; *Hintersteininger* in SbgK § 144 Rz 33; *Kienapfel/Schmoller*, Strafrecht Besonderer Teil II² (2017) § 144 Rz 44; *Schmoller*, Lösegelderpressung für die Rückgabe von Diebesgut, JBl 2008, 198 (199 f); *Venier*, „Kunsterpressung" – ein vermögensstrafrechtliches Paradoxon?, JSt 2004, 73 (73 ff).

23 LGSt Wien 7.9.2006, 062 Hv 98/06v-321.

24 OGH 6.3.2007, 11 Os 3/07m; OGH 17.8.2010, 11 Os 54/10s.

aber als nachträgliche Schadensgutmachung strafmildernd.[25] *Schmoller* kritisiert die gegenständliche Rspr des OGH treffend mit dem Argument, dass der Herausgabeanspruch wirtschaftlich bewertet werden müsse. So würde dem Eigentumsrecht mangels faktischer Durchsetzbarkeit allenfalls nur ein kleiner wirtschaftlicher Restwert innewohnen, der den vollen Sachwert bei Weitem nicht erreiche. Dieser volle Sachwert würde erst durch die Rückgabe der Beute wieder in das Vermögen des Opfers übergehen.[26] Solange die Summe aus der Höhe des Lösegeldes und dem wirtschaftlichen Restwert des Herausgabeanspruches den Wert der gestohlenen Sache nicht übersteigt, könne somit nicht von einem Vermögensschaden iSd § 144 StGB gesprochen werden, da das Vermögen des Opfers saldierend betrachtet bei Zahlung des Lösegeldes gegen Rückgabe des Diebesguts wirtschaftlich an Wert gewinnt. Liegt auch kein Vorsatz auf die Zufügung eines (zusätzlichen) Vermögensschadens vor, könnte der Täter hier nur noch eine Nötigung nach § 105 StGB zu verantworten haben.[27]

Zieht man nun die soeben herausgearbeiteten Grundsätze der hL zur Beurteilung der Drohung, die versperrten Daten ohne Zahlung des Lösegeldes nicht wieder freizuschalten, heran, zeigt sich, dass der Schaden schon durch die Verschlüsselung der Daten eingetreten ist. Das Opfer hat zivilrechtlich zwar einen Anspruch auf Freigabe der Daten, doch wird dieser in einer wirtschaftlichen Betrachtungsweise niemals den Wert der Daten selbst erreichen. Diesen vollen Wert erlangt das Opfer erst durch die tatsächliche Entschlüsselung der Daten zurück, womit der Zahlung des Lösegeldes saldierend immer der Wert der entschlüsselten Daten gegenübersteht. Für die Frage der Strafbarkeit nach § 144 StGB kommt es nun stets auf das Verhältnis zwischen der Höhe des Lösegeldes und dem objektiven Wert der Daten an. Da die Täter die Höhe des Lösegeldes nicht individuell auf das konkrete Opfer angepasst, sondern von jedem Opfer pauschal denselben Betrag gefordert haben, wird das begehrte Lösegeld mit Sicherheit in vielen Fällen den tatsächlichen Wert der Daten überstiegen haben. Nach der Literatur würde nur in diesen Fällen ein Vermögensschaden eintreten, der – bei Vorliegen des Schädigungsvorsatzes – zur Vollendung der Erpressung führt.[28] In den gegenteiligen Fällen käme mangels Eintritts eines Vermögensschadens nur eine versuchte Erpressung oder – bei Fehlen des Schädigungsvorsatzes – eine vollendete Nötigung gem § 105 StGB in Frage. Die Rspr hingegen würde die Verursachung des Vermögensschadens und damit gleichgeschaltet die Strafbarkeit nach § 144 StGB stets bejahen.[29]

Die potentielle Subsumtion der Tat unter den Tatbestand der Erpressung ändert sich auch nicht, wenn die Täter gar nicht vorhaben, die Daten nach der Zahlung wieder freizugeben. Grundsätzlich könnte darin zwar ein Betrug liegen, doch stehen die Tatbestände des Betrugs und der Erpressung nach hM hier im Verhältnis der Exklusivität.[30] Während beim Betrug eine Vermögensverfügung des Opfers aufgrund eines Irrtums über die Sachlage gewissermaßen „freiwillig" erfolgen soll, wird das Opfer bei der Erpressung durch Gewalt oder gefährliche Drohung gezwungen, die Vermögensverfügung zu treffen. Dass das Mittel zur Drohung auf einer Täuschung basiert, ist dabei nicht erheblich.[31] Der OGH hat dies in älterer Rspr noch anders gesehen und die Vortäuschung einer Entführung in Bereicherungsabsicht als Betrug und nicht Erpressung beurteilt.[32] Selbst unter Aufrechterhaltung dieser Rspr wäre der hier untersuchte Fall aber als Erpressung zu beurteilen: Gegenüber der faktischen Sperre der Daten und der Drohung, diese gesperrt zu lassen, tritt das täuschende Element klar in den Hintergrund. Das Opfer befindet sich auch nicht in einer Position verdünnter, weil auf einem Irrtum basierender, Willensfreiheit, sondern in einer Zwangslage. Eine Beurteilung als Betrug scheidet deshalb aus. Auf Ebene des Vermögensschadens ergeben sich in dieser Konstellation auch im Hinblick auf den Tatbestand der Erpressung keine Probleme, da der Zahlung des Lösegeldes keine Gegenleistung gegenübersteht.

Verwirklicht der Täter sowohl eine Datenbeschädigung gem § 126a StGB als auch eine Erpressung nach § 144 StGB, stellt sich die Frage, in welchem Verhältnis die beiden Delikte stehen. Richtigerweise ist hier von echter Konkurrenz auszugehen.[33] Eine Konsumtion der Erpressung als straflose Nachtat[34] kommt einerseits aufgrund der Verursachung eines über die Vortat hinaus-

25 OGH 6.3.2007, 11 Os 3/07m; *Eder-Rieder* in WK² StGB § 144 Rz 27.
26 *Schmoller*, JBl 2008, 198 (199 f).
27 *Kienapfel/Schmoller*, BT II² § 144 Rz 44; *Salimi* in SbgK § 127 Rz 221; *Schmoller*, JBl 2008, 198 (198 ff). Ein Teil der Lehre argumentiert in derartigen Fällen gegen das Vorliegen einer gefährlichen Drohung gegen fremdes Vermögen, da der Schaden schon eingetreten ist und somit nicht mehr mit dem (erneuten) Verlust desselben Diebesgutes gedroht werden kann. Vgl *Venier*, JSt 2004, 73 (73 ff). Zur treffenden Gegenargumentation siehe jedoch *Schmoller*, JBl 2008, 198 (199).
28 *Salimi* in SbgK § 127 Rz 221; *Schmoller*, JBl 2008, 198 (199 f).
29 OGH 6.3.2007, 11 Os 3/07m; OGH 17.8.2010, 11 Os 54/10s.
30 *Eder-Rieder* in WK-StGB² § 144 Rz 45; *Kert* in SbgK § 146 Rz 387.
31 *Leukauf/Steininger/Flora*, StGB⁴ § 144 Rz 20.
32 RIS-Justiz RS0092938.
33 Vgl OGH 6.3.2007, 11 Os 3/07m.
34 Diese Konstellation kann nur auftreten, wenn die Täter nach dem Freisetzen des Trojaners weitere Erpressungshandlungen setzen. Fordert der Trojaner die Opfer nach Verschlüsselung der Daten automatisch zur Zahlung auf und setzen die Täter damit keine weiteren Handlungen, stehen §§ 126a und 144 StGB in Idealkonkurrenz und eine Subsumtion als Nach- bzw Vortat kommt schon begrifflich nicht in Frage.

gehenden Schadens, andererseits aufgrund der Divergenzen in den geschützten Rechtsgütern – § 144 StGB schützt im Gegensatz zu § 126a StGB neben dem Vermögen auch die Dispositionsfreiheit[35] – nicht in Betracht. Umgekehrt wird auch die Datenbeschädigung nicht als straflose Vortat von einer nachfolgenden Erpressung konsumiert, da diese abweichend zu § 144 StGB auch den Fortbestand und die Verfügbarkeit der Daten als solches schützt.

2.3. § 278 StGB – Kriminelle Vereinigung

Schlussendlich steht auch eine Strafbarkeit aufgrund eines Organisationsdeliktes – allen voran der kriminellen Vereinigung gem § 278 StGB – im Raum, da sich im Eingangsfall drei Täter zur Durchführung des Trojaner-Angriffes zusammenschließen. Um als kriminelle Vereinigung qualifiziert zu werden, muss dieser Zusammenschluss einerseits auf die Begehung eines oder mehrerer der in § 278 Abs 2 StGB taxativ aufgezählten Vereinigungsdelikte ausgerichtet und andererseits auf *„längere Zeit angelegt"* sein. Ob das Vergehen (§ 17 Abs 2 StGB) der Datenbeschädigung gem § 126a Abs 1-3 StGB unter die in § 278 Abs 2 StGB verwendete Wortfolge *„nicht nur geringfügige Sachbeschädigungen"* subsumiert werden kann und damit unabhängig von der Erfüllung der Qualifikationen des § 126a Abs 4 StGB (Verbrechen gem § 17 Abs 1 StGB) ein Vereinigungsdelikt darstellt, ist zwar strittig[36], aufgrund des im StGB herrschenden, auf körperliche Gegenstände abstellenden, Sachbegriffes[37] jedoch zu verneinen. *Triffterer* argumentiert hingegen, dass der in § 278 StGB verwendete Begriff der „Sachbeschädigung" im Rahmen der Versteinerungstheorie so ausgelegt werden müsse, wie er bei der Schaffung des Deliktes des § 278 StGB im Jahre 1975[38] verstanden wurde und kommt damit zu einer möglichen Erfassung auch der Datenbeschädigung, da der Gesetzgeber bis zur Aufnahme des § 126a StGB im Jahre 1987[39] die dort beschriebenen Handlungen auch von der Sachbeschädigung erfasst gesehen hätte.[40] Diese Ausführungen *Triffterers* beziehen sich jedoch auf das Delikt der Bandenbildung gem § 278 StGB aF und damit auf die Vorgängerregelung zur heutigen kriminellen Vereinigung. Als letztere im Jahr 2002[41] das Delikt der Bandenbildung ersetzte, war der auf körperliche Gegenstände beschränkte Sachbegriff schon fest etabliert, weshalb auch unter Heranziehung der Versteinerungstheorie nicht mehr von einer Erfassung des Vergehens der Datenbeschädigung ausgegangen werden kann.

Jedenfalls kommen als Vereinigungsdelikte hingegen die Verbrechen der Erpressung gem § 144 StGB und der qualifizierten Datenbeschädigung gem § 126a Abs 4 StGB in Frage. Eine kriminelle Vereinigung setzt weder voraus, dass die Mitglieder planen, die einzelnen Straftaten gemeinsam auszuführen[42], noch müssen die in Zukunft geplanten Vereinigungsdelikte schon genau konkretisiert sein. Es reicht vollkommen, wenn sich die Mitglieder die künftige Ausführung einer oder mehrerer bloß nach allgemeinen Kriterien determinierten Katalogstraftaten des Abs 2 durch zumindest ein Vereinigungsmitglied zum Ziel setzen.[43] Dass die Täter die genauen Erpressungsopfer bei der Entstehung des Zusammenschlusses noch nicht kennen, schadet somit nicht.

Das zeitliche Kriterium der Anlage auf längere Zeit ist laut Rspr bei einem geplanten Bestand der Vereinigung von mehreren Wochen oder von unbestimmter Dauer erfüllt.[44] Da die Hacker den Trojaner im Vorfeld des Angriffes zuerst programmieren mussten und auch die Ausbreitung des Virus sowie die Zahlung des Lösegeldes einige Zeit in Anspruch genommen hat, kann durchaus angenommen werden, dass die Täter mit einem Bestand der Vereinigung über längere Zeit gerechnet haben.

Tatbestandsmäßig iSd § 278 StGB handelt nun sowohl derjenige, der die kriminelle Vereinigung gründet, dh die zur Zusammenarbeit erforderliche Willenserklärung abgibt[45], als auch wer sich an ihr gem Abs 3 als Mitglied beteiligt. So der Zusammenschluss als kriminelle Vereinigung zu qualifizieren ist, erfüllen die Gründer durch den Abschluss ihres auf die Begehung von Vereinigungsdelikten abzielenden Übereinkommens jedenfalls den Tatbestand des § 278 Abs 1 Fall 1 StGB. Nicht an der Gründung beteiligte Personen können sich hingegen nur als Mitglied an der kriminellen Vereinigung gem § 278 Abs 1 Fall 2 StGB beteiligen. Diese Tatalternative wird in § 278 Abs 3 StGB definiert und erfasst Personen, die im Rahmen der kriminellen Ausrichtung eine Straftat begehen oder sich in dem Wissen, die Vereinigung zu fördern, durch sonstige Aktivitäten im Rahmen der kriminellen Zielsetzung beteiligen. Während die Alternative des Begehens einer strafbaren Handlung regelmäßig durch die tatsächliche Ausführung des Trojaner-Angriffes und die damit einhergehende Lösegeldforde-

35 *Eder-Rieder* in WK-StGB² § 144 Rz 2.
36 *Plöchl* in WK-StGB² § 278 Rz 22; ausführlich *Triffterer* in SbgK § 278 Rz 42.
37 *Sagmeister* in SbgK § 125 Rz 38 mwN.
38 BGBl 1974/60.
39 BGBl 1987/605.
40 *Triffterer* in SbgK § 278 Rz 42.
41 BGBl I 2002/134.
42 *Hinterhofer/Rosbaud*, BT II⁶ (2016) § 278 Rz 10.
43 *Plöchl* in WK-StGB² § 278 Rz 14.
44 RIS-Justiz RS0119848.
45 *Plöchl* in WK-StGB² § 278 Rz 28 ff.

rung erfolgen wird, bestraft die sonstige Beteiligung die Schaffung der zur Deliktsdurchführung erforderlichen Infrastruktur[46] und erfasst zB Personen, die der Vereinigung die notwendige Hardware oder den verwendeten Virus zur Verfügung stellen.

2.4. Zwischenergebnis

Im Ergebnis werden die Täter in den allermeisten Fällen eine Datenbeschädigung nach § 126a StGB zu verantworten haben. Ob die nachfolgende Forderung des Lösegeldes eine Erpressung nach § 144 StGB oder eine Nötigung gem § 105 StGB konstituiert, hängt nach der hL einerseits vom Verhältnis zwischen der Höhe des geforderten Lösegeldes und dem tatsächlichen Wert der Daten und andererseits vom Vorliegen des Schädigungsvorsatzes ab. Der OGH würde die Verwirklichung einer Erpressung hingegen jedenfalls bejahen. Schlussendlich steht bei mehreren Tätern, die sich zur Begehung des Angriffes zusammenschließen, auch immer eine Strafbarkeit nach dem Organisationsdelikt des § 278 StGB im Raum.

3. Strafbarkeit des Opfers bei Zahlung des Erpressungsbetrages?

3.1. Beteiligung an einer kriminellen Vereinigung gem § 278 StGB

Obwohl Behörden davon abraten, die Forderungen der Hacker zu erfüllen[47], scheint die Zahlung des Lösegeldes doch oftmals zu erfolgen. So sollen bereits 33 % aller deutschen Opfer von Ransomware-Angriffen Lösegeld zur Entsperrung ihrer Daten bezahlt haben.[48] Dies ist aber auch für das Opfer strafrechtlich nicht ungefährlich:

Handeln die Hacker im Rahmen einer kriminellen Vereinigung iSd § 278 StGB[49], könnte sich – entsprechenden Vorsatz vorausgesetzt – auch das Opfer durch die Zahlung des geforderten Geldbetrages nach dieser Bestimmung strafbar machen, weil es die kriminelle Vereinigung durch die (wenn auch abgenötigte) Bereitstellung von Vermögenswerten fördert.[50]

Da § 278 Abs 1 StGB jedoch eine Beteiligung „als Mitglied" verlangt, kommt speziell im Hinblick auf eine eventuelle Strafbarkeit des Opfers der Auslegung dieses Mitgliedschaftserfordernisses entscheidende Bedeutung zu. Seit dem StRÄG 2002[51] statuiert § 278 Abs 3 StGB, dass sich derjenige an einer kriminellen Vereinigung „*als Mitglied beteiligt, [...] wer [...] sich an ihren Aktivitäten durch die Bereitstellung von Informationen oder Vermögenswerten oder auf andere Weise in dem Wissen beteiligt, dass er dadurch die Vereinigung oder deren strafbare Handlungen fördert*". Fraglich ist nun, ob die Setzung einer der in Abs 3 aufgezählten Verhaltensweisen automatisch die in Abs 1 geforderte Mitgliedschaft in einer kriminellen Vereinigung begründet oder ob diese objektiv und losgelöst von den Beteiligungshandlungen vorliegen muss.[52] *Plöchl* führt hierzu aus, dass § 278 Abs 1 StGB zwar eine Beteiligung „als Mitglied" fordert, was bei einer isolierten Betrachtung auf das Vorliegen eines Sonderdeliktes und damit auf die Notwendigkeit einer Mitgliedschaft abseits der Vornahme von Beteiligungshandlungen hindeuten würde. Aufgrund des eindeutigen Wortlautes der Legaldefinition des Abs 3 beteiligt sich jedoch jeder, der eine Beteiligungshandlung iSd Abs 3 mit dem dort geforderten Vorsatz setzt, als Mitglied an einer kriminellen Vereinigung.[53] Im Ergebnis könne sich somit das Erpressungsopfer durch die Zahlung des Lösegeldes wegen Beteiligung an einer kriminellen Vereinigung als Mitglied nach § 278 Abs 1 Fall 2 StGB strafbar machen.[54]

Auch die Rspr scheint diese Auslegung zu präferieren, indem sie einerseits auf eine separate Prüfung der Mitgliedschaft verzichtet[55] und andererseits der OGH unlängst in einem *obiter dictum* ausdrücklich ausgesprochen hat, dass bereits jede wissentliche Förderung einer kriminellen Vereinigung die Mitgliedschaft iSd § 278 Abs 3 StGB begründet.[56]

In der Literatur wird teilweise eine einschränkende Auslegung des § 278 StGB vertreten, die nur Personen erfassen will, die – losgelöst von der Tathandlung – Mitglied

46 *Hinterhofer/Rosbaud*, BT II[6] § 278 Rz 13.

47 Pressemitteilung des BKA vom 16.5.2017, http://www.bmi.gv.at/cms/bk/_news/pressemeldungen.aspx (8.11.2017).

48 *Beiersmann*, Ransomware: Jedes dritte Opfer in Deutschland zahlt Lösegeld, ZDNet vom 4.3.2016, http://bit.ly/1PxwVJ5 (8.11.2017).

49 Gleiches gilt, wenn die Täter im Rahmen einer kriminellen Organisation iSd § 278a StGB handeln.

50 Vgl zur deutschen RL auch *Salomon*, MMR 2016, 575 (575 ff).

51 BGBl I 2002/134.

52 Zum Meinungsstand siehe *Reindl-Krauskopf/Salimi*, Kriminelle Organisation (§ 278a StGB), III-348 BlgNR 24. GP 80 ff.

53 *Plöchl* in WK-StGB[2] § 278 Rz 46; ebenso *Velten*, Die Organisationsdelikte haben Konjunktur: Eine moderne Form der Sippenhaftung? Banken und Tierschützer vor Gericht, JSt 2009, 55 (60 f).

54 *Plöchl* in WK-StGB[2] § 278 Rz 38.

55 So zB OGH 19.2.2009, 12 Os 152/08g; OLG Linz 12.2.2015, 8 Bs 15/15k.

56 OGH 17.12.2015, 12 Os 106/15b; so auch schon vor dem StRÄG 2002 OGH 5.5.1994, 12 Os 36/94.

der kriminellen Vereinigung sind.[57] Der Sache nach wird hier wohl eine teleologische Reduktion des Tatbestandes gefordert.[58] So wird argumentiert, dass die Wortfolge „als Mitglied" ihre eigenständige Bedeutung verlieren würde und insgesamt überflüssig wäre, wenn jede Beteiligungshandlung iSd Abs 3 schon die Mitgliedschaft konstituieren würde.[59] Da nicht davon auszugehen ist, dass der Gesetzgeber überflüssige Tatbestandsmerkmale formuliert[60], müsse die Mitgliedschaft eigenständig und unabhängig vom Setzen von Beteiligungshandlungen vorliegen.[61] Auch die Materialien sprechen für eine enge Auslegung des Mitgliedschaftserfordernisses, da diese als Begründung für die Strafbarkeit nach dem Organisationsdelikt das in der Mitgliedschaft liegende Unrecht anführen.[62]

Zuletzt kann auch die historische Entstehungsgeschichte des § 278a StGB ins Treffen geführt werden, der schon seit der Strafgesetznovelle 1993[63] die Beteiligung als Mitglied an einer kriminellen Organisation bestraft und seit dem StRÄG 2002 zur Auslegung dieser Tathandlung auf § 278 Abs 3 StGB verweist.[64] Aufgrund dieses Verweises sind die Mitgliedschaftserfordernisse der §§ 278 und 278a StGB kongruent auszulegen. Der von *Kienapfel* im Auftrag des Justizausschusses ausgearbeitete Alternativentwurf zur Regierungsvorlage zur Strafgesetznovelle 1993[65] sah neben der Tathandlung des Beteiligens als Mitglied in Übereinstimmung mit der deutschen Regelung des § 129a Abs 1 dStGB noch die „sonstige Unterstützung" vor, wodurch sich auch Nicht-Mitglieder durch Unterstützungshandlungen strafbar machen hätten können. Indem sich der Gesetzgeber jedoch schlussendlich gegen die Aufnahme der „sonstigen Unterstützung" in den Tatbestand des § 278a StGB entschlossen hat[66], kann *e contrario* argumentiert werden, dass nur Mitglieder der kriminellen Organisation von dieser Bestimmung erfasst sein sollten.[67] Hierauf weisen auch die Mat zum StRÄG 1996[68] hin, indem sie punktuelle Beteiligungen an einzelnen Straftaten oder Handlungsweisen, denen das mit dem Begriff der „Mitgliedschaft" verbundene Moment einer gewissen Dauer fehlt, ausdrücklich keiner Strafbarkeit unterwerfen.[69] Da keine Anhaltspunkte dafür existieren, dass der Gesetzgeber im Rahmen des StRÄG 2002 die Strafbarkeit des § 278a StGB – und damit gleichgeschaltet die des § 278 StGB – durch die Aufnahme der Legaldefinition des § 278 Abs 3 StGB auf Nicht-Mitglieder erweitern wollte[70], könnte auf das Vorliegen einer überschießenden Regelung geschlossen werden.

Es existieren somit durchaus Argumente dafür, § 278 StGB einschränkend auszulegen und das Mitgliedschaftserfordernis unabhängig von der Vornahme einer der in Abs 3 aufgezählten Tathandlungen zu prüfen. Aufgrund des eindeutigen Wortlautes der Bestimmung und der Rspr des OGH, die das Erfordernis der Mitgliedschaft automatisch mit der Vornahme der wissentlichen Förderung einer kriminellen Vereinigung erfüllt sieht, ist jedoch generell auch dem Opfer als Nicht-Mitglied selbiger Vereinigung von der Zahlung des Lösegeldes abzuraten.

3.2. Möglichkeit einer Rechtfertigung

Entschließt sich das Opfer dennoch zur Zahlung des erpressten Betrages, muss dies aber nicht zwangsläufig zu seiner Strafbarkeit führen, da die Zahlung zur Wiedererlangung der verschlüsselten Daten gerechtfertigt oder entschuldigt sein könnte. Die meisten Rechtfertigungsgründe erlauben dem Opfer jedoch nur, zur Rettung seiner Daten in die Rechtsgüter des Angreifers und nicht auch in die Rechtsgüter gänzlich unbeteiligter Dritter einzugreifen.[71] Diese Einschränkung führt dazu, dass in der zu untersuchenden Fallkonstellation die Rechtfertigungsgründe der Notwehr gem § 3 StGB, des Anhalterechtes Privater gem § 80 Abs 2 StPO oder des Selbsthilferechtes Privater gem §§ 19, 344 ABGB nicht anwendbar sind, verletzt das Opfer mit der Zahlung des

57 ZB *Hinterhofer/Rosbaud*, BT II[6] § 278 Rz 13a und § 278a Rz 13; *Kienapfel/Schmoller*, Strafrecht Besonderer Teil III[2] (2009) §§ 277-278 Rz 70; *Schmoller*, Mitgliedschaft in einer kriminellen Vereinigung, JBl 2013, 743 (747 ff); *Wessely*, Zu den neuen Terrorismustatbeständen im StGB, ÖJZ 2004, 827 (832).

58 Vgl dazu OGH 27.8.2008, 13 Os 83/08t, der aus formalen Gründen jedoch nicht weiter darauf eingeht; aA *Reindl-Krauskopf/Salimi*, Kriminelle Organisation 81 f, die die engere Auslegung noch vom Wortlaut des § 278 Abs 3 StGB erfasst sehen.

59 *Schmoller*, JBl 2013, 743 (747 f).

60 OGH 29.8.2013, 13 Os 54/13k.

61 *Schmoller*, JBl 2013, 743 (748).

62 ErläutRV 1166 BlgNR 21. GP 35 f; *Lehner*, Die Straftatbestände zur Bekämpfung der Terrorismusfinanzierung (2014) 144.

63 BGBl 1993/527.

64 Zur historischen Entwicklung siehe *Lehner*, Terrorismusfinanzierung 141 ff.

65 Abgedruckt in *Kienapfel*, Bildung einer kriminellen Organisation (§ 278a Abs 1 StGB), JBl 1995, 613 (615).

66 Als einzige Ausnahme wurden Geldwäsche-Handlungen im Auftrag oder im Interesse einer kriminellen Organisation aufgenommen. Siehe *Lehner*, Terrorismusfinanzierung 143.

67 *Kienapfel*, JBl 1995, 613 (620 f); *Lehner*, Terrorismusfinanzierung 142 f; *Reindl-Krauskopf/Salimi*, Kriminelle Organisation 82.

68 BGBl 1996/762.

69 JAB 409 BlgNR 20. GP 12.

70 *Reindl-Krauskopf/Salimi*, Kriminelle Organisation 81.

71 Zu § 3 StGB vgl *Lewisch* in WK-StGB[2] § 3 Rz 99; zu § 80 Abs 2 StPO vgl *Lewisch* in WK-StGB[2] Nachbem zu § 3 Rz 193 ff. Auch das Selbsthilferecht Privater gem §§ 19, 344 ABGB wird wohl keine Eingriffe in die Rechtsgüter Unbeteiligter – hier die Allgemeinheit – rechtfertigen.

Geldbetrages doch nicht die Rechtsgüter des Angreifers, sondern vielmehr das der Allgemeinheit zustehende und durch § 278 StGB geschützte Rechtsgut des öffentlichen Friedens.[72] Anzudenken wäre allerdings die Anwendung des rechtfertigenden Notstandes, der unter engen Voraussetzungen auch Eingriffe in die Rechtsgüter Dritter zulässt[73], wenn dies zur Abwehr eines unmittelbar drohenden, bedeutenden Nachteils für ein Individualrechtsgut des Notstandstäters erforderlich ist.[74] Der Retter darf im Rahmen des rechtfertigenden Notstands aber nur das schonendste Mittel zur Abwehr dieses Nachteils wählen, wobei das gerettete Rechtsgut zusätzlich eindeutig höherwertiger gegenüber dem beeinträchtigten sein und die Rettungshandlung zur Abwehr des Nachteils angemessen erscheinen muss.[75] Eine genauere Betrachtung dieser Kriterien zeigt, dass die Zahlung des Geldbetrages typischerweise nicht gerechtfertigt sein wird. Verkörpern die verschlüsselten Daten zB keinen bzw nur einen sehr geringen wirtschaftlichen Wert, spricht dies gegen die Annahme eines *bedeutenden* Nachteils für ein Individualrechtsgut, weshalb die Drohung, die Daten weiter verschlüsselt zu halten, uU schon gar keine Notstandssituation konstituieren würde. Liegt hingegen ein bedeutender Nachteil vor, stellt sich als nächstes die Frage, ob ein Backup der verschlüsselten Daten existiert. Sollte ein solches bestehen, ist die Zahlung des Erpressungsbetrages nicht mehr das schonendste Mittel zur Wiederherstellung des Systems. Hierfür ist es irrelevant, mit welchen Kosten die Wiederherstellung der Daten verbunden ist[76], da eine legale Vorgehensweise im Vergleich zur Begehung einer strafbaren Handlung immer als schonenderes Mittel anzusehen ist.[77] Wenn kein Backup besteht, muss mittels Güterabwägung untersucht werden, ob die zu rettenden Daten als eindeutig höherwertiger im Vergleich zum Rechtsgut des öffentlichen Friedens anzusehen sind. Dies kann nicht in einer abstrakten Betrachtung beurteilt werden, es kommt vielmehr auf den konkreten Einzelfall an, wobei die Intensität der jeweiligen Rechtsgutbeeinträchtigung (zB der Wert der Daten oder die konkreten Auswirkungen auf den öffentlichen Frieden) sowie die Wahrscheinlichkeit der Rettung des bedrohten Rechtsgutes, dh die Wahrscheinlichkeit der tatsächlichen Freischaltung der Daten durch die Angreifer, in die Interessenabwägung miteinfließt.[78]

Doch selbst wenn die Notstandshandlung das schonendste Mittel zur Rettung eines höherwertigen Rechtsguts ist, kann sich das Opfer nicht erfolgreich auf den rechtfertigenden Notstand berufen, wenn die Tat – bezogen auf die obersten Prinzipien und Wertbegriffe der Rechtsordnung – nicht als angemessen erscheint.[79] Dieses Angemessenheitskorrektiv wird nach der hM in Konstellationen verletzt, in denen jemand eine Straftat gezwungenermaßen begeht, um einen sonst von dritter Seite drohenden Nachteil abzuwenden (sog „Nötigungsnotstand").[80] Begründet wird dies zum einen damit, dass die Beeinträchtigung des fremden Rechtsguts (hier durch die Verwirklichung des § 278 StGB der öffentliche Friede) nicht zur unmittelbaren Bewahrung der eigenen Interessen (der Entsperrung der Daten) führt, sondern bloß die Voraussetzungen dafür schafft, dass der Angreifer die Bedrohung der eigenen Rechtsgüter aufgibt.[81] Zum anderen wäre es aus sozialethischen Gesichtspunkten inakzeptabel, in den Fällen des Nötigungsnotstandes ein Vorgehen des Genötigten aufgrund der Anwendbarkeit des rechtfertigenden Notstands als rechtmäßig anzusehen, zumal sich unbeteiligte Dritte, in deren Rechtsgüter durch den Genötigten eingegriffen wird, zum Schutz ihrer Rechte mangels Rechtswidrigkeit des Angriffs nicht auf das Notwehrrecht berufen könnten.[82]

3.3. Entschuldigender Notstand

Im Ergebnis wird die Zahlung des erpressten Betrages an die Hacker als rechtswidrig anzusehen sein, womit sich die Frage der Strafbarkeit auf Ebene der Schuld entscheidet, weil das Opfer für die Verwirklichung des § 278 StGB prinzipiell gem § 10 StGB entschuldigt sein könnte.[83] Für das Vorliegen der Notstandssituation setzt

72 *Plöchl* in WK² StGB § 278 Rz 2.
73 *Kienapfel*, Der rechtfertigende Notstand, ÖJZ 1975, 421 (427); *Kienapfel/Höpfel/Kert*, Allgemeiner Teil[15] (2016) Z 14 Rz 28.
74 *Kienapfel/Höpfel/Kert*, Allgemeiner Teil[15] Z 14 Rz 14.
75 *Leukauf/Steininger/Tipold*, StGB[4] § 3 Rz 52; siehe auch ausführlich *Kienapfel/Höpfel/Kert*, AT[15] Z 14 Rz 14 ff.
76 Würde die Wiederherstellung der Daten mittels Backups keine bedeutenden Aufwendungen verursachen, könnte freilich argumentiert werden, dass auch hier mangels bedeutenden Nachteils schon keine Notstandssituation vorliegt.
77 Vgl auch *Lewisch* in WK² StGB Nachbem zu § 3 Rz 57, der ausführt, dass der Retter primär die ihm *in concreto* offenstehenden Möglichkeiten einer rechtskonformen Gefahrenabwehr zu wählen hat.
78 *Kienapfel*, ÖJZ 1975, 421 (428 ff); *Lewisch* in WK² StGB Nachbem zu § 3 Rz 67 ff.
79 *Kienapfel*, ÖJZ 1975, 421 (429).
80 *Kienapfel*, ÖJZ 1975, 421 (430); *Lewisch* in WK² StGB Nachbem zu § 3 Rz 101 mwN; *Steininger* in SbgK StGB Nachbem § 3 Rz 61; OGH 18.9.1979, 9 Os 86/79.
81 *Lewisch* in WK-StGB² Nachbem zu § 3 Rz 101.
82 *Kienapfel*, ÖJZ 1975, 421 (430); *Lewisch* in WK-StGB² Nachbem zu § 3 Rz 101 f; *Steininger* in SbgK Nachbem § 3 Rz 61.
83 Für die prinzipielle Anwendbarkeit des § 10 StGB in den Fällen des Nötigungsnotstandes *Fuchs*, Strafrecht Allgemeiner Teil I[9] (2016) 24/20; *Plöchl* in WK-StGB² § 278 Rz 38; *Steininger* in SbgK Nachbem § 3 Rz 61; OGH 18.9.1979, 9 Os 86/79; OGH 15.6.1988, 15 Os 9/88.

der entschuldigende Notstand, kongruent zum rechtfertigenden Notstand, einen unmittelbar drohenden, bedeutenden Nachteil für ein Individualrechtgut voraus. Unterschiede ergeben sich hinsichtlich der Kriterien der Notstandshandlung. So muss die gewählte Handlung weder das schonendste Mittel zur Abwehr des Nachteils darstellen, noch muss das gerettete Rechtsgut höherwertig gegenüber dem geopferten Rechtsgut sein. Der Notstandstäter ist gem § 10 StGB schon dann entschuldigt, wenn der Schaden aus seiner Tat nicht unverhältnismäßig schwerer als der abzuwendende Nachteil wiegt und von einem maßgerechten, mit den rechtlich geschützten Werten verbundenen Menschen kein anderes Verhalten zu erwarten gewesen wäre.[84]

Die Verfügbarkeit eines Backups schließt die Anwendbarkeit des § 10 StGB somit nicht automatisch aus, es kommt vielmehr darauf an, ob sich auch die Maßfigur in der konkreten Fallkonstellation für die Zahlung des Erpressungsbetrages und gegen die Verwendung des Backups entschieden hätte. Dies könnte mitunter dann vorliegen, wenn die selbständige Wiederherstellung mit enormen Zeitaufwand verbunden wäre, der Inhalt der verschlüsselten Daten jedoch sofort benötigt wird – man denke hierbei zB an die Intensivstation eines Krankenhauses. Besteht wiederum kein Backup, wird der Wert der betroffenen Daten sowie der für ihre Neuerstellung verursachte Aufwand in die Abwägung miteinzubeziehen sein. Stets ist jedoch auch die Wahrscheinlichkeit der tatsächlichen Entsperrung der Daten zu berücksichtigen. Wäre bereits bekannt, dass die Angreifer die Daten trotz Zahlung des Lösegeldes nicht wieder entschlüsseln, würde dies die Anwendbarkeit des § 10 StGB ausschließen.

Im Ergebnis ist zwar schon die Frage der Verwirklichung des § 278 StGB durch das Opfer bei Zahlung des Lösegeldes äußerst umstritten, doch muss aufgrund der Rspr des OGH von jeder Zahlung an die Angreifer abgeraten werden. Überweist das Opfer trotzdem den geforderten Betrag zur Entsperrung seiner Daten, wird einer Strafbarkeit in vielen Fällen der Entschuldigungsgrund des entschuldigenden Notstandes im Wege stehen, doch muss hier jedes Mal genau untersucht werden, wie sich die Maßfigur des mit den rechtlichen Werten verbundenen Menschen in der konkreten Fallkonstellation verhalten hätte.

Zusammenfassung

Spätestens seit der Freisetzung des sog „WannaCry"-Trojaners sind Ransomware-Angriffe wieder in das Zentrum medialer Aufmerksamkeit gerückt. Aus strafrechtlicher Sicht sind hierbei aber noch viele Probleme ungeklärt: Klar ist, dass die Täter in den allermeisten Fällen eine Datenbeschädigung begehen. Doch schon die Frage, ob ein Angriff mittels Ransomware – wie der Name impliziert – eine Erpressung nach § 144 StGB konstituiert, kann aufgrund von unterschiedlichen Rechtsansichten zwischen Rspr und Literatur zu ähnlich gelagerten Fallkonstellationen nicht eindeutig beantwortet werden. Sofern nämlich das gezahlte Lösegeld geringer als der Wert der Daten ist, könnte argumentiert werden, dass die Vermögensverfügung unter gleichzeitiger Entsperrung der Daten nicht zu einem Vermögensschaden, sondern sogar zu einem Vermögensgewinn des Opfers führt. Agieren die Täter im Rahmen einer kriminellen Vereinigung, stellt sich darüber hinaus die Frage, ob die Zahlung des Lösegeldes ein (wenngleich faktisch geringes) strafrechtliches Risiko für die Opfer begründet, da dieses Verhalten als Finanzierung der kriminellen Vereinigung verstanden werden könnte. Dabei bleiben bei all diesen Fragestellungen die – aufgrund der Wahrscheinlichkeit, dass die Täter im Ausland gehandelt haben – ebenfalls sehr relevanten aber nicht minder komplizierten Regelungen zum internationalen Strafrecht, insbesondere dem österreichischen Strafanwendungsrecht der §§ 62-67 StGB, aus Gründen des Umfangs noch völlig außer Betracht.

Korrespondenz:
Christopher Kahl, LL.M.,
christopher.kahl@wu.ac.at
Mag. Alexander Stücklberger,
stuecklberger@btp.at

84 *Höpfel* in WK-StGB² § 10 Rz 6 ff; *Kienapfel/Höpfel/Kert*, AT¹⁵ Z 20 Rz 7 ff.

AUTOREN

Mag. Patrick Bugelnig, LL.M. (UoP)

Rechtspraktikant im OLG Sprengel Wien.
patrick.bugelnig@gmx.net

Dr. Oliver Scheiber

ist Richter in Wien und leitet das Bezirksgericht Meidling. Er ist Lehrbeauftragter an der Universität Wien, Vorsitzender des Vorstands des Instituts für Rechts- und Kriminalsoziologie und Vorstandsmitglied ua von SOS Mitmensch und Weissem Ring.
oliver.scheiber@univie.ac.at

Mag. Martin Heissenberger,

ist Richteramtsanwärter im Sprengel des OLG Graz.
martin.heissenberger@justiz.gv.at

Univ.-Ass. MMag. Dr. Kathrin Stiebellehner (vorm. Schmidthuber)

ist seit Februar 2012 Universitätsassistentin am Institut für Strafrechtswissenschaften der JKU Linz (Abteilung für Praxis der Strafrechtswissenschaften und Medizinstrafrecht). Neben anderen Publikationen ist sie Mit-Autorin des Salzburger Kommentars zum StGB.
kathrin.stiebellehner@jku.at

Christopher Kahl, LL.M. (WU)

ist Universitätsassistent am Institut für Österreichisches und Europäisches Wirtschaftsstrafrecht der WU Wien.
christopher.kahl@wu.ac.at

Mag. Alexander Stücklberger

ist Rechtsanwaltsanwärter der Brandl & Talos Rechtsanwälte GmbH.
stuecklberger@btp.at

© privat

Dr. Dieter Neger

ist Rechtsanwalt, allgemein beeideter und zertifizierter Sachverständiger und Gründungspartner der Neger / Ulm Rechtsanwälte GmbH in Graz. Zu seinen Tätigkeitsschwerpunkten zählt das Wirtschaftsstrafrecht. Der Autor hält laufend Fachvorträge und publiziert Fachbeiträge, die sich – auf diesen Tätigkeitsschwerpunkt bezogen – mit Wirtschafts- und Korruptionsstrafrecht beschäftigen.
neger@neger-ulm.at