HRRS-Nummer: HRRS 2021 Nr. 774
Bearbeiter: Christoph Henckel/Karsten Gaede
Zitiervorschlag: HRRS 2021 Nr. 774, Rn. X

BGH 1 StR 78/21 - Beschluss vom 8. April 2021 (LG Stuttgart)

BGHR; Computersabotage (hier: Verbreitung von Ransomware; Begriff des Veränderns von Daten: Hinzufügen von Einträgen in der Windows-Registry-Datei zum automatischen Laden einer Schadsoftware; Begriff der Datenverarbeitung von wesentlicher Bedeutung: Privatpersonen, Ausschluss von Bagatellfällen); Erpressung; Beihilfe (Tateinheit bei Förderung mehrerer Taten durch einheitliche Unterstützungshandlung).

§ 303a Abs. 1 StGB; § 303b Abs. 1 Nr. 2 StGB; § 253 Abs. 1 StGB; § 27 StGB

Leitsätze

1. Zur Strafbarkeit der Verbreitung eines Erpressungstrojaners über das Internet (sog. Ransomware). (BGH)

2. Ein Verändern von Daten i.S.d. §§ 303a, 303b StGB ist auch das Hinzufügen von Einträgen in der Windows-Registry-Datei, wodurch eine Schadsoftware beim Hochfahren des Rechners automatisch geladen wird, ohne dass der Computernutzer hiervon Kenntnis bekam und sofort der ganze Bildschirm und alle weiteren Fenster vom Sperrbildschirm überdeckt werden, so dass dieser weder minimiert noch geschlossen werden kann. Diese System-Dateien sind taugliche Tatobjekte im Sinne der Legaldefinition des § 202a Abs. 2 StGB. Ein Verändern ist auch beim Herbeiführen von Funktionsbeeinträchtigungen der Daten anzunehmen, die eine Änderung ihres Informationsgehalts oder des Aussagewerts zur Folge haben. (Bearbeiter)

3. Das einschränkende Merkmal einer Datenverarbeitung „von wesentlicher Bedeutung“ sollte nach dem Willen des Gesetzgebers als Filter für Bagatellfälle dienen, die vom Tatbestand nicht erfasst werden. Bei Privatpersonen als Geschädigten ist darauf abzustellen, ob die Datenverarbeitung für die Lebensgestaltung der Privatperson eine zentrale Funktion einnimmt Das ist bei einer gegen den Willen der berechtigten Computernutzer installierte Schadsoftware, die jegliche Nutzung der auf den Geräten gespeicherten Daten unmöglich macht und dadurch der Computer nur durch eine mit einem vollständigen Datenverlust verbundene Neuinstallation des Betriebssystems wieder genutzt werden konnten, anzunehmen. (Bearbeiter)

Entscheidungstenor

1. Auf die Revision des Angeklagten wird das Urteil des Landgerichts Stuttgart vom 6. November 2020

a) im Schuldspruch dahingehend abgeändert, dass der Angeklagte der Beihilfe zur Erpressung in Tateinheit mit Beihilfe zur Computersabotage schuldig ist,

b) im Strafausspruch aufgehoben.

2. Die weitergehende Revision des Angeklagten wird als unbegründet verworfen.

3. Im Umfang der Aufhebung wird die Sache zu neuer Verhandlung und Entscheidung, auch über die Kosten des Rechtsmittels, an eine andere Strafkammer des Landgerichts zurückverwiesen.

Gründe

Das Landgericht hat den Angeklagten wegen Beihilfe zur versuchten Erpressung in Tateinheit mit Beihilfe zur versuchten Computersabotage in 396 Fällen sowie wegen Beihilfe zur Erpressung in Tateinheit mit Beihilfe zur Computersabotage in 393 Fällen zu einer Gesamtfreiheitsstrafe von vier Jahren und sechs Monaten verurteilt. Die in Österreich erlittene Auslieferungshaft ist im Maßstab 1:1 angerechnet worden. Weiter ist gegen den Angeklagten die Einziehung des Wertes von Taterträgen in Höhe von 9.800 Euro angeordnet worden. 1

Die Revision des Angeklagten erzielt mit der Sachrüge den aus der Beschlussformel ersichtlichen Erfolg (§ 349 Abs. 4 StPO). Im Übrigen ist das Rechtsmittel unbegründet im Sinne des § 349 Abs. 2 StPO. 2

I.

Das Landgericht hat folgende Feststellungen und Wertungen getroffen: 3

1. Der Angeklagte war Mitglied einer international und arbeitsteilig agierenden Gruppierung aus mehr als drei Personen, die sich spätestens Ende 2013 in K. (Ukraine) um unbekannt gebliebene Haupttäter zur fortgesetzten Begehung von Delikten im Bereich der Cyberkriminalität durch Verbreitung eines „Erpressungstrojaners“ über das Internet (sog. Ransomware) zusammengeschlossen hatte. 4

a) Zur Vorbereitung und Platzierung der Schadsoftware im Internet bediente sich die Gruppierung der Nutzung von Werbeanzeigen auf verschiedenen Webseiten (sog. Adverts), bei deren Anklicken es ohne den Willen der Nutzer zum Nachladen und zur Installation der Schadsoftware auf den Rechnern der Geschädigten kam. Nach dieser Infektion des Zielrechners wurden in verschlüsselter Form vor allem die Geolokationsdaten des geschädigten Rechners an einen Server der Gruppierung übermittelt; denn nur so war es technisch möglich, einen von der Gruppierung vorprogrammierten Sperrbildschirm an die mit der Schadsoftware infizierten Rechnersysteme zu übermitteln, welcher in der jeweiligen Landessprache an das Herkunftsland der geschädigten Computernutzer angepasst war. Die Gruppierung verfügte dazu über Sperrbildschirme in 44 Sprachen. Bei der Gestaltung dieses Sperrbildschirms wurde der Eindruck erweckt, es handele sich um eine von offiziellen Stellen veranlasste Sperrung des Zielsystems, indem hier Logos staatlicher Behörden, beispielsweise des Bundeskriminalamtes oder des Bundesnachrichtendienstes, verwendet wurden. Zudem erhielten die Meldungen am Sperrbildschirm genaue Angaben über den betroffenen Computer, das verwendete Betriebssystem, die IP-Adresse und den Standort des Rechners sowie die unwahre Behauptung, der Nutzer habe illegale Downloads getätigt oder auf seinem Rechner befänden sich Dateien mit verbotenen kinder- oder tierpornografischen Inhalten. Zur Abwendung eines Straf- oder Bußgeldverfahrens sowie zur Freigabe des gesperrten Computersystems wurde eine Geldzahlung gefordert, die über geldwerte PIN-Codes elektronischer Zahlungssysteme - wie zum Beispiel Paysafecards oder Ukash - im Wert von 100 Euro zu leisten war. 5

b) Nach der Infektion des Rechners und der Übermittlung des Sperrbildschirms blieb der Computer mit einer Verschlüsselungssoftware dauerhaft gesperrt. Die Sperrbildschirme wurden auch bei jedem Neustart des infizierten Rechners nachgeladen. Zusätzlich wurden Aufrufe des Task-Managers durch die Schadsoftware beendet, so dass der Sperrbildschirm weder minimiert noch geschlossen werden konnte. Für die Sperrung der Rechner wurden von der Tätergruppierung unterschiedliche Varianten der Schadsoftware eingesetzt, die auch permanent dahingehend überprüft wurden, ob und von welchem Antivirenprogramm diese erkannt werden und laufend entsprechend angepasst. Weder die Schadsoftware selbst enthielt einen Mechanismus, der bei Übermittlung eines geforderten PIN-Codes oder durch Zeitablauf eine Entsperrung des infizierten Systems veranlasste, noch wurde eine solche Entsperrung manuell durch die Gruppierung durchgeführt. Einzig durch Löschen der Festplatte - unter gleichzeitigem unwiderruflichen Verlust aller auf dem Rechner gespeicherten Daten - und anschließender Neuinstallation des Betriebssystems konnten die infizierten Geräte wieder brauchbar gemacht werden. 6

c) Zur Umsetzung dieses Vorhabens verfügte die Gruppierung über eine Vielzahl von Servern. So wurde etwa der Sperrbildschirm über verschiedene Proxy-Server versandt, die jeweils nur über einen Zeitraum von wenigen Tagen bis Wochen verwendet und anschließend durch neue ersetzt wurden. Sie dienten als zwischengeschaltete Server der Anonymisierung und vor allem dazu, die eigentlichen Ziel- bzw. Backend-Server zu verschleiern. Die mit der Schadsoftware infizierten Systeme übermittelten ihre Daten an die Backend-Server, auf denen diese automatisiert gespeichert wurden und von denen aus der länderspezifische Sperrbildschirm mit der Aufforderung zur Zahlung versendet wurde. Auf gleichem Weg vollzog sich auch die Übermittlung der von den Geschädigten erworbenen und in den Sperrbildschirm eingegebenen PIN-Codes im Fall einer Zahlung. Die Backend-Server fungierten zudem als Verwaltungsportal für die erpressten PIN-Codes, die dort in einer Datenbank gesammelt und später verwaltet wurden. Durch die Einschaltung von Finanzagenten wurden die im Verwaltungsportal gespeicherten PIN-Codes über Online-Dienste (z.B. Online-Casinos oder Wettbüros), welche diese als Zahlungsmittel akzeptierten, eingelöst und in einem weiteren Schritt in Form von virtueller Währung auf ein Konto der Gruppierung überwiesen. Weltweit wurden so durch die Tätergruppierung von 2013 bis 2016 über 200 Millionen Rechnersysteme infiziert und von den geschädigten Computernutzern mehr als neun Millionen Euro an geldwerten PIN-Codes übermittelt. 7

d) Der Angeklagte übernahm im Frühjahr/Sommer 2013 im Rahmen der Gruppierung die Tätigkeit eines Systemadministrators und technischen Beraters für einen monatlichen Verdienst von 1.000 US-Dollar und betreute die Server der Gruppierung. Er konnte auf Grund seines technischen Sachverstands sowohl Zweck als auch Funktionsweise der sich auf den Servern befindlichen Sperrbildschirme einordnen. Der Angeklagte hatte spätestens am 29. November 2013 Kenntnis davon, dass die Gruppierung die Server dazu einsetzte, um unter Drohung mit einem behördlichen Verfahren und der dauerhaften Sperrung der Rechner, ein Lösegeld in Höhe von 100 Euro in Form von geldwerten PIN-Codes von Computernutzern zu verlangen. Er setzte gleichwohl seine Tätigkeit für die Gruppierung fort. Der Angeklagte übernahm verschiedene Unterstützungshandlungen innerhalb der von der Gruppierung zur Begehung der Taten aufgebauten Serverinfrastruktur. Im verfahrensgegenständlichen Tatzeitraum vom 29. November 2013 bis 3. Februar 2015 kümmerte sich der Angeklagte auf Anweisung der Führungsmitglieder um die Anmietung neuer Server, die Installation verschiedener Programme auf den Servern, um die Verlinkung 8

einzelner Server untereinander, um die Erhaltung deren Funktionsfähigkeit sowie um die Behebung einzelner technischer Probleme der Serverinfrastruktur. Darüber hinaus stand er den Führungsmitgliedern der Gruppierung als technischer Berater zur Verfügung. In diesem verfahrensgegenständlichen Tatzeitraum wurden in Deutschland mindestens 4.332 Computersysteme an 396 Tagen gegen den Willen der berechtigten Computernutzer (Fälle 1 bis 396 der Urteilsgründe) infiziert, wobei es der Gruppierung in 393 weiteren Fällen (Fälle 397 bis 789 der Urteilsgründe) darüber hinaus auch gelang, den jeweiligen Computernutzer der gesperrten Rechner zum Erwerb und zur Übermittlung von geldwerten PIN-Codes an die Täter im Wert von jeweils 100 Euro zu veranlassen. In allen Infektionsfällen - gleich ob das geforderte Lösegeld in Form von PIN-Codes gezahlt wurde oder nicht - wurden die betroffenen Rechner aber nicht entsperrt.

2. Das Landgericht geht nach wertender Betrachtung der Gesamtumstände davon aus, dass der Angeklagte gewerbs- und auch bandenmäßig gehandelt hat, aber nur als Gehilfe tätig war, da sein eigenes Interesse am Taterfolg begrenzt war und er lediglich ein Festgehalt bezog sowie auch an den Gewinnen aus den Geschäften nicht beteiligt war. Das Landgericht nimmt eine Beihilfehandlung des Angeklagten zu allen 789 ausgeurteilten Einzeltaten an. 9

II.

Der Schuldspruch wegen Beihilfe zur versuchten Erpressung in Tateinheit mit Beihilfe zur versuchten Computersabotage in 396 Fällen sowie wegen Beihilfe zur Erpressung in Tateinheit mit Beihilfe zur Computersabotage in 393 Fällen hält einer revisionsrechtlichen Prüfung nicht stand. Er bedarf in konkurrenzrechtlicher Hinsicht der Korrektur. Dies bedingt auch die Aufhebung des Strafausspruchs. 10

1. Die rechtsfehlerfrei getroffenen Feststellungen des Landgerichts tragen einen Schuldspruch des Angeklagten nur wegen einer einheitlichen Beihilfe (§ 27 Abs. 1 StGB) zur Erpressung nach § 253 Abs. 1 StGB in Tateinheit mit Beihilfe zur Computersabotage nach § 303b Abs. 1 Nr. 1 StGB (§ 52 Abs. 1 StGB). Der Schuldspruch war daher entsprechend abzuändern. 11

a) Durch seine festgestellten Unterstützungshandlungen hat der Angeklagte sowohl eine Beihilfe zur vollendeten Erpressung als auch zur versuchten Erpressung nach § 253 Abs. 1 StGB geleistet. Die jeweils mit der Schadsoftware infizierten Computernutzer wurden durch die Sperrung ihrer Rechner und durch die unwahre Behauptung, illegale Downloads vorgenommen zu haben oder auf den Rechnern Dateien mit verbotenen kinder- oder tierpornografischen Inhalten zu besitzen, zur Abwendung der Sperrung ihrer Rechner zur Zahlung eines Betrages von 100 Euro über geldwerte PIN-Codes elektronischer Zahlungssysteme genötigt; ihrem Vermögen wurde so ein Nachteil in entsprechender Höhe zugefügt. Bei den im Versuchsstadium verbliebenen Taten wurde jedenfalls von den Tätern ein entsprechender Schaden erstrebt. 12

b) Die Infektion der Zielrechner mit der entsprechenden Schadsoftware und der Installation eines Sperrbildschirms erfüllt den Tatbestand der Computersabotage nach § 303b Abs. 1 Nr. 1 StGB. 13

aa) Gemäß § 303b Abs. 1 Nr. 1 StGB macht sich strafbar, wer eine Datenverarbeitung, die für einen anderen von wesentlicher Bedeutung ist, dadurch stört, dass er eine Tat nach § 303a Abs. 1 StGB begeht, also rechtswidrig Daten löscht, unterdrückt, unbrauchbar macht oder verändert. Die Vorschrift schützt in dieser Tatvariante das Interesse des Verfügungsberechtigten an der unversehrten Verwendbarkeit der gespeicherten oder übermittelten Daten und damit das Grundrecht auf Integrität und Vertraulichkeit informationstechnischer Systeme (Bär in Wabnitz/Janovsky/Schmitt, Handbuch Wirtschafts- und Steuerstrafrecht, 5. Aufl., 15. Kapitel Rn. 125; Fischer, StGB, 68. Aufl., § 303b Rn. 2; LK-StGB/Wolff, 12. Aufl., § 303b Rn. 2 mwN; vgl. auch BT-Drucks. 16/3656, S. 13). 14

bb) Die Haupttäter haben durch den Eingriff in die Registry-Dateien der geschädigten Computersysteme Daten im Sinne des § 303a Abs. 1 StGB so verändert, dass der ganze Bildschirm und alle weiteren Fenster vom Sperrbildschirm überdeckt sowie alle Aufrufe des Task-Managers durch die Schadsoftware beendet wurden. Diese System-Dateien sind taugliche Tatobjekte im Sinne der Legaldefinition des § 202a Abs. 2 StGB (BGH, Beschluss vom 27. Juli 2017 - 1 StR 412/16 Rn. 30 f.; Bär aaO Rn. 110 mwN). Ein Verändern ist auch beim Herbeiführen von Funktionsbeeinträchtigungen der Daten anzunehmen, die eine Änderung ihres Informationsgehalts oder des Aussagewerts zur Folge haben (BT-Drucks. 10/5058, S. 35; BGH, Beschluss vom 27. Juli 2017 - 1 StR 412/16 Rn. 33; Bär aaO Rn. 118; Bär in Graf/Jäger/Wittig, Wirtschafts- und Steuerstrafrecht, 2. Aufl., § 303a StGB Rn. 20). Eine solche Veränderung der Daten ist durch das Hinzufügen der Einträge in der Windows-Registry-Datei eingetreten, indem die Schadsoftware beim Hochfahren des Rechners automatisch geladen wurde, ohne dass der Computernutzer hiervon Kenntnis bekam und sofort der ganze Bildschirm und alle weiteren Fenster vom Sperrbildschirm überdeckt wurden, so dass dieser weder minimiert noch geschlossen werden konnte. 15

cc) Das Landgericht geht auch zutreffend davon aus, dass hier die gegenüber der Datenveränderung nach § 303a Abs. 1 StGB qualifizierenden Merkmale der Computersabotage nach § 303b Abs. 1 Nr. 1 StGB vorliegen, nämlich eine Datenverarbeitung von wesentlicher Bedeutung sowie eine Störung der entsprechenden Datenverarbeitung. 16

Das einschränkende Merkmal einer Datenverarbeitung „von wesentlicher Bedeutung“ sollte nach dem Willen des Gesetzgebers als Filter für Bagatellfälle dienen, die vom Tatbestand nicht erfasst werden (BT-Drucks. 16/3656, S. 13). So soll nach der Gesetzesbegründung bei Privatpersonen als Geschädigten darauf abgestellt werden, ob die Datenverarbeitung für die Lebensgestaltung der Privatperson eine zentrale Funktion einnimmt (BT-Drucks. 16/3656, S. 13). Insoweit waren dem Landgericht konkrete Feststellungen zu den einzelnen betroffenen Computersystemen nicht möglich. Im Fall des Anzeigeerstatters lagen diese Voraussetzungen jedenfalls vor. Anhand der übertragenen Daten waren weitere Nachfragen zur Identifizierung der übrigen Nutzer aber ausgeschlossen. Deswegen war das Landgericht hier befugt, auf eine wesentliche Bedeutung der Datenverarbeitung für die betroffenen Computernutzer indiziell zu schließen (vgl. BGH, Beschluss vom 27. Juli 2017 - 1 StR 412/16 Rn. 25). Dies gilt vor allem vor dem Hintergrund, dass bei allen festgestellten Einzeltaten durch die gegen den Willen der berechtigten Computernutzer installierte Schadsoftware jegliche Nutzung der auf den Geräten gespeicherten Daten unmöglich gemacht wurde und die Computer nur durch eine mit einem vollständigen Datenverlust verbundene Neuinstallation des Betriebssystems wieder genutzt werden konnten (UA S. 7), so dass von einer Beeinträchtigung der zentralen Funktionen für die Lebensgestaltung der Betroffenen auszugehen ist. Im Übrigen spricht vor allem der Umstand, dass in vielen Fällen die tateinheitlich verwirklichte Erpressung erfolgreich war, weil die Computernutzer eine Zahlung geleistet haben, für eine wesentliche Bedeutung der Datenverarbeitung und gegen einen Bagatellfall, da sie ansonsten nicht gezahlt hätten. 17

Auch der für die Verwirklichung des Tatbestands von § 303b Abs. 1 Nr. 1 StGB erforderliche Taterfolg, die Störung einer Datenverarbeitung, ist nach den Feststellungen des Landgerichts (UA S. 7) eingetreten. Da die Sperrbildschirme am Rechner einzig durch ein Löschen der Festplatte und anschließender Neuinstallation des Betriebssystems beseitigt werden konnten, war die Infektion des Rechners immer mit einem unwiderruflichen Verlust aller auf dem Rechner gespeicherter Daten verbunden. 18

c) Beide verwirklichten Tatbestände des § 253 Abs. 1 StGB und des § 303b Abs. 1 Nr. 1 StGB stehen in Tateinheit zueinander, da unmittelbar mit der Computersabotage durch die Veränderung der System-Dateien und dem erscheinenden Sperrbildschirm der Computernutzer zur Übermittlung geldwerter PIN-Codes zum Entsperren der Rechner aufgefordert wurde. Entgegen der Auffassung des Landgerichts ist aber konkurrenzrechtlich nicht von einer Beihilfe des Angeklagten zu 789 Einzeltaten, sondern nur von einer einheitlichen Beihilfe zur Erpressung in Tateinheit mit Computersabotage auszugehen. 19

aa) Nach ständiger Rechtsprechung des Bundesgerichtshofs ist die Frage der Handlungseinheit oder -mehrheit nach dem individuellen Tatbeitrag eines jeden Beteiligten zu beurteilen. Fördert der Gehilfe durch ein und dasselbe Tun mehrere rechtlich selbständige Taten des Haupttäters, so ist nur eine Beihilfe im Rechtssinne gegeben (vgl. nur BGH, Beschlüsse vom 13. März 2013 - 2 StR 586/12 Rn. 6 und vom 25. Juli 2019 - 1 StR 230/19 Rn. 5; Urteile vom 23. Oktober 2018 - 1 StR 234/17 Rn. 65 und vom 28. Oktober 2004 - 4 StR 59/04, BGHSt 49, 306, 316). 20

bb) Die bisherigen Feststellungen belegen nicht, dass der Angeklagte bei den im Tatzeitraum vom 29. November 2013 bis 3. Februar 2015 verwirklichten 789 Einzeltaten einen individuellen tatfördernden Beitrag erbracht hat. Das fördernde Verhalten des Angeklagten stellt sich vielmehr nur als eine einheitliche Unterstützungshandlung dar, indem der Angeklagte sich auf Anweisung der Führungsmitglieder um die Anmietung neuer Server, um die Installation verschiedener Programme auf den Servern, um die Verlinkung einzelner Server untereinander und um die Erhaltung der Funktionsfähigkeit sowie um die Behebung einzelner technischer Probleme der Serverinfrastruktur kümmerte. Auch seine vom Landgericht festgestellte weitere Funktion als technischer Berater der Führungsmitglieder der Gruppierung begründet keinen individuellen tatfördernden Beitrag zu konkreten Einzeltaten. 21

2. Der Senat kann die Änderung des Schuldspruchs selbst vornehmen (§ 354 Abs. 1 StPO analog). Auf Grund der bisherigen Feststellungen des Landgerichts kann ausgeschlossen werden, dass noch individuelle tatfördernde Beiträge des Angeklagten zu den jeweiligen vom Landgericht ausgeurteilten 789 Einzeltaten im vorgenannten Tatzeitraum aufgeklärt werden können. Um den Schuldspruch übersichtlich zu halten, sieht der Senat davon ab, die Anzahl der tateinheitlich zusammentreffenden Verstöße (§ 52 Abs. 1 Alternative 2 StGB) anzugeben (§ 260 Abs. 4 Satz 5 StPO). 22

Der Änderung des Schuldspruchs steht § 265 StPO nicht entgegen, da sich der Angeklagte nicht anders als geschehen hätte verteidigen können. 23

3. Die Abänderung des Schuldspruchs führt zur Aufhebung des Strafausspruchs, weil der Senat vorliegend nicht ausschließen kann, dass die Strafzumessung von der Vielzahl der Einzeltaten beeinflusst ist und das Tatgericht bei Annahme einer einheitlichen Beihilfehandlung zu einer niedrigeren Freiheitsstrafe gelangt wäre. Da es sich um einen Wertungsfehler handelt, können die Feststellungen aufrechterhalten bleiben. Ergänzende Feststellungen, insbesondere zum Einfluss des Angeklagten im Hinblick auf das Gesamtgeschehen bleiben möglich. 24

4. Die Entscheidung über die Anrechnung der Auslieferungshaft und die Einziehung des Wertes von Taterträgen bleiben bestehen, da sie vom aufgezeigten Rechtsfehler nicht betroffen sind. 25