HRRS-Nummer: HRRS 2015 Nr. 1047
Bearbeiter: Christoph Henckel und Karsten Gaede
Zitiervorschlag: HRRS 2015 Nr. 1047, Rn. X

BGH 1 StR 16/15 - Beschluss vom 21. Juli 2015 (LG Kempten)

Ausspähen von Daten (Überwinden einer Zugangssicherung: Begriff der Zugangssicherung, Anforderungen an die Darstellung im Urteil).

§ 202a Abs. 1 StGB; § 267 Abs. 1 StPO

Leitsätze des Bearbeiters

1. Für die Erfüllung des Straftatbestands des § 202a Abs. 1 StGB ist die Überwindung einer Zugangssicherung erforderlich ist. Denn der Schutzbereich dieser Strafvorschrift erstreckt sich nur auf Daten, die gegen unberechtigten Zugang besonders gesichert sind. Dies sind nur solche, bei denen der Verfügungsberechtigte durch seine Sicherung sein Interesse an der Geheimhaltung der Daten dokumentiert hat (vgl. BGH NStZ 2011, 154).

2. Die Zugangssicherung im Sinne von § 202a Abs. 1 StGB muss darauf angelegt sein, den Zugriff Dritter auf die Daten auszuschließen oder wenigstens nicht unerheblich zu erschweren (vgl. BGH NStZ 2011, 154). Darunter fallen insbesondere Schutzprogramme, welche geeignet sind, unberechtigten Zugriff auf die auf einem Computer abgelegten Daten zu verhindern, und die nicht ohne fachspezifische Kenntnisse überwunden werden können und den Täter zu einer Zugangsart zwingt, die der Verfügungsberechtigte erkennbar verhindern wollte. Schließlich muss der Zugangsschutz auch gerade im Zeitpunkt der Tathandlung bestehen.

Entscheidungstenor

1. Auf die Revision des Angeklagten wird das Urteil des Landgerichts Kempten (Allgäu) vom 29. Oktober 2014 mit den Feststellungen aufgehoben.

2. Die Sache wird zu neuer Verhandlung und Entscheidung, auch über die Kosten des Rechtsmittels, an eine allgemeine Strafkammer des Landgerichts zurückverwiesen.

Gründe

Das Landgericht (Jugendkammer) hat den Angeklagten wegen Ausspähens von Daten in Tateinheit mit Datenveränderung sowie wegen Computerbetruges in 18 Fällen jeweils tateinheitlich mit Fälschung beweiserheblicher Daten zu einer Gesamtfreiheitsstrafe von drei Jahren verurteilt. Es hat zudem den Verfall der sichergestellten 86 Bitcoins und den Verfall von Wertersatz in Höhe von 432.500 Euro sowie die Einziehung von im Einzelnen näher bezeichneter Computerhardware nebst Zubehör angeordnet. 1

Gegen diese Verurteilung wendet sich der Angeklagte mit der nicht näher ausgeführten Sachrüge. Seine Revision hat in vollem Umfang Erfolg (§ 349 Abs. 4 StPO). 2

I.

Das Landgericht hat u.a. folgende Feststellungen und Wertungen getroffen: 3

1. Anfang des Jahres 2012 schloss sich der Angeklagte mit dem (nach Abtrennung des Verfahrens) anderweitig verurteilten Heranwachsenden R. zusammen, um ein sog. Botnetzwerk - d.h. ein der Ressourcengewinnung dienendes Netzwerk jeweils missbräuchlich durch automatisierte Computerprogramme zusammengeschlossener Rechner - aufzubauen und dieses dann ebenfalls missbräuchlich zum Generieren von Bitcoins zu nutzen. Zu diesem Zweck entwickelte er gemeinsam mit dem gesondert Verurteilten R. eine spezielle Schadsoftware, die unerkannt über das Usenet - ein selbständig neben dem Internet bestehendes Netzwerk, welches überwiegend zum Download illegal gefertigter Kopien von Filmen oder Musikdateien genutzt wird - verbreitet werden sollte. Der Angeklagte stellte zu diesem Zweck im Zeitraum vom 1. Januar 2012 bis zum 4. Oktober 2013 diverse Dateien im Usenet zum Download bereit. An diese war die programmierte Schadsoftware für den Anwender nicht wahrnehmbar angekoppelt, die sich nach dem Download einer infizierten Datei automatisch auf dem betroffenen Computer installierte. Die 4

Schadsoftware, ein Trojaner, war für die Betriebssysteme ab Windows XP bis Windows 7 bestimmt, „welche standardmäßig eine ‚Firewall' aktiviert haben, um derartige Angriffe abzuwehren" (UA S. 3). Diese Firewall „wurde durch den Trojaner umgangen" (UA S. 3) und das jeweilige Betriebssystem des Computers verändert. An späterer Stelle in den Urteilsgründen findet sich die Feststellung, dass in vielen Fällen der Trojaner „durch Virenprogramme der Nutzer nicht erkannt wurde" (UA S. 4). Detaillierte Feststellungen zu den auf den betroffenen Computern installierten Schutzprogrammen hat das Landgericht nicht, auch nicht exemplarisch, getroffen. Die Schadsoftware führte dazu, dass jede Eingabe an dem infizierten Rechnersystem, darunter Zugangsdaten zu diversen Accounts nebst Passwörtern, an eine von dem Angeklagten und R. eingerichtete Datenbank übertragen wurde. Sie hatte außerdem die Eigenschaft, bei einer Inaktivität ab 120 Sekunden die Rechenleistung des Computers für die Lösung komplexer Rechenaufgaben zu nutzen, wofür dem Angeklagten und R. Bitcoins gutgeschrieben werden konnten (Ziffer II.1. der Urteilsgründe).

2. Im Zeitraum zwischen dem 19. November 2012 und dem 17. März 2013 mietete der Angeklagte oder von ihm beauftragte „Spreader" in insgesamt 18 Fällen aufgrund jeweils neuen Tatentschlusses für den Betrieb ihres Netzwerks und die Verbreitung der Schadsoftware unter missbräuchlicher Verwendung zuvor ausgespähter Personaldaten Server an. Die Freischaltung der Server erfolgte nach Übermittlung der Zugangsdaten automatisiert. Der Angeklagte wollte eine Zurückverfolgbarkeit von Datenströmen zu ihm ausschließen und sich die durch den jeweiligen Vertragsschluss anfallenden Anschluss- und Nutzungsgebühren ersparen. Dies gelang ihm durch die Verwendung ausgespähter Daten, wodurch den Anbietern jeweils ein entsprechender Schaden, insgesamt in einer Größenordnung von 7.000 Euro, entstand (Ziffer II.2. der Urteilsgründe). 5

II.

Die Rüge der Verletzung materiellen Rechts greift insgesamt durch. 6

1. Die Verurteilung wegen Ausspähens von Daten in Tateinheit mit Datenveränderung (Ziffer II.1. der Urteilsgründe) hält rechtlicher Nachprüfung nicht stand; der Schuldspruch wird von den getroffenen Feststellungen nicht getragen. 7

Die Feststellungen sind teilweise lückenhaft und weisen zudem einen inneren, auch durch den Gesamtzusammenhang der Urteilsgründe nicht auflösbaren Widerspruch auf. Sie belegen nicht hinreichend, dass der Angeklagte jeweils eine Zugangssicherung überwunden hat, die für die Erfüllung des Straftatbestands des § 202a Abs. 1 StGB erforderlich ist. Denn der Schutzbereich dieser Strafvorschrift erstreckt sich nur auf Daten, die gegen unberechtigten Zugang besonders gesichert sind. Dies sind nur solche, bei denen der Verfügungsberechtigte durch seine Sicherung sein Interesse an der Geheimhaltung der Daten dokumentiert hat (vgl. BGH, Beschluss vom 6. Juli 2010 - 4 StR 555/09, NStZ 2011, 154). 8

Die Zugangssicherung im Sinne von § 202a Abs. 1 StGB muss darauf angelegt sein, den Zugriff Dritter auf die Daten auszuschließen oder wenigstens nicht unerheblich zu erschweren (vgl. BGH, Beschluss vom 6. Juli 2010 - 4 StR 555/09, NStZ 2011, 154; LK-StGB/Hilgendorf, StGB, § 202a Rn. 30; MüKo-StGB/Graf, StGB, § 202a Rn. 35; Rübenstahl/Debus, NZWiSt 2012, 129, 131). Darunter fallen insbesondere Schutzprogramme, welche geeignet sind, unberechtigten Zugriff auf die auf einem Computer abgelegten Daten zu verhindern, und die nicht ohne fachspezifische Kenntnisse überwunden werden können und den Täter zu einer Zugangsart zwingt, die der Verfügungsberechtigte erkennbar verhindern wollte (vgl. BT-Drucks. 16/3656 S. 10). Schließlich muss der Zugangsschutz auch gerade im Zeitpunkt der Tathandlung bestehen (vgl. MüKo-StGB/Graf, StGB, § 202a Rn. 20). 9

Ob diese Voraussetzungen in den der Verurteilung zugrunde liegenden Fällen gegeben sind, vermag der Senat anhand der unvollständigen Feststellungen im Urteil nicht abschließend zu beurteilen. Zugleich kann nicht ausgeschlossen werden, dass das Landgericht der vorgenommenen Rechtsanwendung, die nicht näher erläutert wird (UA S. 13), ein fehlerhaftes Verständnis zugrunde gelegt hat. 10

Es fehlt in den Urteilsgründen eine hinreichend genaue Darstellung der Wirkweise der von dem Angeklagten bereitgestellten Schadsoftware, welche die Benennung der im konkreten Einzelfall umgangenen Zugangssicherung erfasst. Der pauschale Verweis auf deren Bestehen reicht dafür ohne nähere Darlegung nicht aus, denn eine revisionsgerichtliche Kontrolle der eingangs genannten Voraussetzungen ist nur auf der Grundlage einer ausreichend deskriptiven Darlegung der konkreten tatsächlichen und technischen Umstände möglich. Die insoweit bestehende Lücke lässt sich durch die Feststellungen auch in ihrer Gesamtheit nicht schließen. 11

Hinzu kommt, dass das Landgericht zwischen den Begrifflichkeiten der Firewall und des Virenschutzprogrammes nicht erkennbar differenziert hat, wodurch unklar bleibt, ob es die technischen Voraussetzungen der Zugangssicherung in tatsächlicher Hinsicht zutreffend bewertet hat. Während es zunächst nämlich darauf abstellt, der Trojaner sei so konzipiert gewesen, die vorinstallierte Firewall bestimmter Betriebssysteme zu umgehen (UA S. 3), findet sich im Widerspruch dazu an späterer Stelle der Urteilsgründe die Feststellung und Wertung, die vom Angeklagten bereitgestellte Schadsoftware sei durch die Virenprogramme der 327.379 Nutzer nicht erkannt worden (UA S. 4). 12

Unter Zugrundelegung der zu der Schadsoftware zuletzt getroffenen Feststellungen käme eine Firewall als tatbestandsmäßige Schutzvorrichtung bereits dem Grunde nach nicht in Betracht.

Die aufgezeigten Mängel haben die Aufhebung auch der tateinheitlich angenommenen Datenveränderung gemäß § 303a Abs. 1 StGB zur Folge (§ 353 Abs. 1 StPO; vgl. BGH, Urteil vom 20. Februar 1997 - 4 StR 642/96, BGHR StPO § 353 Aufhebung 1; Beschluss vom 2. Juli 2015 - 2 StR 134/15). Ob sich der Tatbestand - wofür einiges spricht - auch auf Programmdaten wie hier die Registrierung der von der Schadsoftware befallenen Computer erstreckt, braucht der Senat deshalb nicht zu entscheiden. 13

2. Auch die tatmehrheitlich erfolgte Verurteilung des Angeklagten wegen Computerbetruges in 18 Fällen (§ 263a Abs. 1 Var. 3 StGB) in Tateinheit mit Fälschung beweiserheblicher Daten gemäß § 269 Abs. 1 StGB (Ziffer II.2. der Urteilsgründe) hat keinen Bestand. 14

Schon auf der Grundlage der bisher getroffenen Feststellungen besorgt der Senat, dass das Landgericht das konkurrenzrechtliche Verhältnis des Ausspähens von Daten (in Tateinheit mit Datenveränderung) zu dem Tatbestand der Fälschung beweiserheblicher Daten (§ 269 StGB) nicht zutreffend bewertet hat. Das Landgericht hat nicht erkennbar bedacht, dass sich die betroffenen Tatzeiträume vom 1. Januar 2012 bis zum 17. März 2013 überschneiden. Abhängig von den konkreten Umständen des Handlungs- und Tatablaufs kann dies die Annahme von Tateinheit (§ 52 Abs. 1 StGB) zur Folge haben (vgl. auch Fischer, StGB, 62. Aufl., Rn. 12 zu § 269 und Rn. 18 zu § 303a). Da nach den Feststellungen nahe liegt, dass die 18 unter Ziffer II.2. der Urteilsgründe namentlich benannten Computernutzer bereits zu den 327.379 Geschädigten aus Ziffer II.1. zählen und Feststellungen zum Vorliegen möglicherweise automatisierter technischer Abläufe fehlen, kann der Senat eine (Teil-)Überschneidung von Handlungseinheiten und damit einer einheitlichen Tat im Rechtssinne jedenfalls nicht sicher ausschließen. 15

Die dargelegten Rechtsfehler führen insgesamt zur Aufhebung des Urteils. Aufgrund des aufgezeigten Widerspruches und um dem neuen Tatrichter zu ermöglichen, umfassend stimmige eigene Feststellungen treffen zu können, waren auch die Feststellungen aufzuheben (§ 353 Abs. 2 StPO). 16

III.

Das neue Tatgericht wird Gelegenheit haben, sich mit den Handlungsabläufen in technischer und zeitlicher Hinsicht umfassender als bislang auseinanderzusetzen. Erst die hinreichend genaue Feststellung der technischen Gegebenheiten ermöglicht die strafrechtliche Bewertung der in Frage kommenden - als solche bereits zutreffend erkannten - Straftatbestände. 17

Die Sache war an eine allgemeine Strafkammer und nicht an eine Jugendkammer zurückzuverweisen, weil sich das weitere Verfahren nur noch gegen den Erwachsenen richtet (vgl. u.a. BGH, Urteil vom 28. April 1988 - 4 StR 33/88, BGHSt 35, 267 f.). 18