Amtsgericht Jülich, 17 Cs-230 Js 99/21-55/23

Datum:	17.01.2024
Gericht:	Amtsgericht Jülich
Spruchkörper:	Strafrichter
Entscheidungsart:	Urteil
Aktenzeichen:	17 Cs-230 Js 99/21-55/23
ECLI:	ECLI:DE:AGJUEL:2024:0117.17CS230JS99.21.55.00

Tenor:

Der Angeklagte wird wegen Ausspähens von Daten zu einer Geldstrafe von 50 Tagessätzen zu je 60,- € verurteilt.

Der Angeklagte hat die Kosten des Verfahrens und die eigenen notwendigen Auslagen zu tragen.

- §§ 202a, 205 StGB -

Amtsgericht Jülich

IM NAMEN DES VOLKES

Urteil

In der Strafsache

gegen Z.,

geboren am 00.00.0000 in D.,

wohnhaft P.-straße, N01 G.,

Verteidiger: Rechtsanwalt O.,

B.-straße, N02 F.,

wegen Ausspähens von Daten

hat das Amtsgericht Jülich

aufgrund der Hauptverhandlung vom 17.01.2024,

an der teilgenommen haben:

Richter am Amtsgericht R.

als Richter

Staatsanwalt H.

als Vertreter der Staatsanwaltschaft Köln

Rechtsanwalt O. aus F.

als Verteidiger des Angeklagten Z.

Justizhauptsekretärin J.

als Urkundsbeamtin der Geschäftsstelle

für Recht erkannt:

Der Angeklagte wird wegen Ausspähens von Daten zu einer Geldstrafe von 50 Tagessätzen zu je 60,- € verurteilt.

Der Angeklagte hat die Kosten des Verfahrens und die eigenen notwendigen Auslagen zu tragen.

- §§ 202a, 205 StGB -

Gründe

I.

Der ledige, zum Zeitpunkt der Hauptverhandlung N03-jährige Angeklagte ist von Beruf L.. Derzeit ist er als angestellter L. bei einem in G. ansässigen Unternehmen tätig, zuvor hat er als Selbständiger Dienstleistungen im IT-Bereich sowie Software angeboten. Strafrechtlich ist der Angeklagte bislang nicht in Erscheinung getreten.

II.

Am frühen Morgen des 00.00.0000 nahm der Angeklagte von seiner damaligen Wohnung in der S.-straße N04 in I. aus Zugang zu dem passwortgeschützten Datenbankserver der Geschädigten, der Y. GmbH & Co. KG mit Sitz in W., die als E-Commerce-Dienstleisterin tätig ist und ihren Kunden JTL-Software, ein Warenwirtschaftssystem, anbietet. Die Software verbindet das Warenwirtschaftssystem ihrer Kunden mit dem großer Online-Markplätze, darunter T., V. und U., so dass die Geschädigte auf ihrem Server über persönliche Daten von ca. 600.000 bis 700.000 Endkunden verfügte.

Das Passwort zu der Datenbank mit den Endkundendaten war von der Geschädigten unverschlüsselt im Quellcode ihrer Software abgelegt und vom Angeklagten durch Dekompilierung, also Rückübersetzung von Maschinencode in einen für den Menschen

lesbaren Quellcode, erlangt worden. Der Angeklagte fertigte Screenshots von auf dem Datenbankserver hinterlegten Kundendaten an, wobei ihm bewusst war, dass er hierzu keine Befugnis hatte.

Noch am Morgen desselben Tages wandte sich der Angeklagte anonym per E-Mail mit dem Betreff „Datenleak“ an den ehemals Mitangeschuldigten K., der den Blog „M..de“ betreibt und in diesem Beiträge zu den Themen IT-Sicherheit und Onlinehandel veröffentlicht. Auf dessen Rat hin kontaktierte der Angeklagte, wiederum anonym, die Geschädigte und teilte mit, dass er Zugriff zu mehreren Datenbanken auf ihrem Server habe, die „empfindliche benutzerbezogene Daten“ enthielten. Dabei nahm er auf im Anhang zu der E-Mail versandte Screenshots der Kundendaten Bezug und forderte die Geschädigte auf, ihre Kunden sowie den Landesdatenschutzbeauftragten innerhalb von zwei Tagen zu informieren und das Datenleck innerhalb von sieben Tagen zu schließen. 30

In der Folgezeit berichteten zunächst der ehemals Mitangeschuldigte in seinem Blog, später auch überregionale Medien wie A. Online, E. Online und andere über das „Datenleck“ bei der Geschädigten. Die Geschädigte erstattete am 00.00.0000 Strafanzeige und stellte am 00.00.0000 Strafantrag. 31

III. 32

Dieser Sachverhalt steht aufgrund der Einlassung des Angeklagten und der im Hauptverhandlungstermin verlesenen Schriftstücke fest. 33

Der Angeklagte hat sich dahingehend eingelassen, dass er im Auftrag eines Kunden, der auch Kunde der Geschädigten gewesen sei, einen von deren Software verursachten Fehler untersucht habe. Die Datenbank des Kunden sei überfüllt gewesen, so dass ihre Nutzbarkeit eingeschränkt gewesen sei. Der Angeklagte habe festgestellt, dass eine mySQL-Verbindung zum Datenbankserver der Geschädigten aufgebaut werde und sei zunächst davon ausgegangen, dass sich auf der mit einer generischen Nummer („N05“) bezeichneten Datenbank nur die Daten des Kunden befunden hätten. Das Passwort für die Datenbank sei in unmittelbarer Nähe zum Hostnamen aufgeführt und mit einem einfachen Texteditor auffindbar gewesen. Als er festgestellt habe, dass in der Datenbank wesentlich mehr Kundendaten hinterlegt waren, als für den Kunden sichtbar sein sollten, habe er die Verbindung sofort getrennt. Gesichert habe er die Daten nicht. Der Zugriff sei über das Tool „N.“ erfolgt; an eine Dekompilierung der Software der Geschädigten könne sich der Angeklagte nicht erinnern. Eingeräumt hat der Angeklagte, über die E-Mail-Adresse „E-Mail01“ mit dem ehemals Mitangeschuldigten K. kommuniziert und die Geschädigte kontaktiert zu haben. An die Versendung von Kundendaten mit diesen E-Mails konnte sich der Angeklagte den eigenen Angaben zufolge hingegen nicht erinnern. 34

Aus der Einlassung des Angeklagten folgt, dass er unter Verwendung eines Passworts, das der Software der Geschädigten entnommen worden ist, Zugriff auf deren Datenbankserver genommen hat. Insoweit ist die Einlassung auch glaubhaft, da sich entsprechendes aus dem Inhalt der unmittelbar nach der Tat verfassten Mitteilungen des Angeklagten an den ehemaligen Mitangeschuldigten und die Geschädigte ergibt. 35

Aufgrund der Beweisaufnahme steht zur Überzeugung des Gerichts fest, dass der Angeklagte das Passwort für die Datenbank dem Dekompilat der Software entnommen hat. Die Dekompilierung der Software der Geschädigten ist durch objektive Beweismittel belegt. Auf dem im Rahmen der Wohnungsdurchsuchung beim Angeklagten sichergestellten PC mit der Asservaten-Nr. N06 waren ausweislich des polizeilichen Auswertungsberichts mehrere 36

Programme installiert, mit denen eine Dekompilierung vorgenommen werden konnte, darunter zwei des Herstellers HR. („SA.“ und „VC.“). Auf dem PC sind außerdem die Software der Geschädigten mit der ausführbaren „MS_Connect.exe“ sowie Dateien gefunden worden, die aus dem Kompilat jener Datei erzeugt worden sind und das im Bericht genannte Datenbank-Passwort enthielten. Der Vorgang der Dekompilierung ist von dem Programm in den ersten Zeilen des Quellcodes eingefügten Kommentar („Decompiled wirth HR. decompiler“) sowie dem Ziel der Dekompilierung, der in einem Ordner auf dem Desktop abgelegten Datei „MS_Connect.exe“, belegt. Der Zeitpunkt der letzten Ausführung beider Programme von HR. liegt nach den technischen Feststellungen der Ermittlungsbeamten nach dem Tattag, so dass sich insoweit keine Widersprüche ergeben. Ferner enthält das auf dem Rechner des Angeklagten aufgefundene Dekompilat der MS_Connect.exe selbst angefertigte Kommentare mit abfälligen Äußerungen über die Qualität der Programmierung: *„//TODO WTF? Hier hört selbst die Inkompetenz auf“* sowie *„//TODO Junge, junge. So parsed man doch kein Datum in C#! Habt ihr DateTime.ParseExact nicht zum Laufen bekommen?“*

Der Angeklagte hat auch gewusst, dass er sich unerlaubt Zugang zu den passwortgesicherten Kundendaten verschafft hat. Seine Einlassung, dass er bei Zugriff auf die Datenbank davon ausgegangen sei, dass es sich nur um die Daten seines Auftraggebers gehandelt habe und die Verbindung nach der Feststellung, dass hier wesentlich mehr Daten vorhanden gewesen seien, sofort getrennt habe, ist unglaubhaft. Die Behauptung eines einmaligen, „versehentlichen“ Zugriffs auf die Datenbank ist mit dem feststehenden Versand der E-Mails mit Screenshots der Kundendaten an den ehemals Mitangeschuldigten und die Geschädigte unvereinbar. Die Anfertigung und der unter Hinweis auf eine Sicherheitslücke erfolgte Versand der Screenshots dokumentiert, dass dem Angeklagten bei dem – erneuten oder fortdauernden – Zugriff auf die Endkundendaten bewusst gewesen ist, dass diese nicht für ihn bzw. seinen Kunden bestimmt waren. 37

IV. 38

Der Angeklagte hat sich damit wegen Ausspähens von Daten gem. § 202a Abs. 1 StGB strafbar gemacht. 39

Der Angeklagte hat sich Zugang zu Daten verschafft, die gegen unberechtigten Zugriff besonders gesichert waren, indem er mit dem zuvor aus der Software ausgelesenen Passwort Zugriff auf den Server der Geschädigten nahm. Darüber hinaus hat er sich die Daten selbst verschafft, indem er Screenshots vom Inhalt der Kundendatenbank anfertigte. Die erlangten Daten (§ 202a Abs. 2 StGB) sind die auf dem Server der Geschädigten gespeicherten persönlichen Informationen der Endkunden. 40

Diese Daten waren nicht für den Angeklagten bestimmt und gegen unberechtigten Zugang besonders gesichert. 41

Die Sicherung des Zugangs zu einer Datenbank durch ein Passwort reicht als Zugangssicherung im Sinne des Straftatbestandes aus (BGH Beschl. v. 13.05.2020 – N06 StR 614/19 –, juris = NStZ-RR 2020, 278). 42

Nach der im Beschwerdeverfahren über die Ablehnung des Erlasses eines Strafbefehls durch das erkennende Gericht ergangenen Entscheidung des Landgerichts Aachen (LG Aachen, Beschl. vom 27.07.2023 – 60 Qs 16/23 –, juris = BeckRS 2023, 21018 = MMR 2023, 866 m. Anm. Kipker) stellt das Auslesen des Passwortes nach Dekompilierung des Objektcodes in den Quellcode auch eine Überwindung einer besonderen Zugangssicherung dar. Danach ist ein weites Verständnis des Überwindens einer Zugangssicherung zugrunde zu legen, bei 43

dem eine Orientierung am technischen Laien erfolgt (ebenso: Kargl, in: NK-StGB, 6. Aufl. 2023, § 202a StGB Rn. 42; vgl. auch Fischer, StGB, 71. Aufl. 2024, § 202a Rn. 11b). Dieser Auffassung schließt sich das erkennende Gericht nunmehr an. Sie entspricht dem Willen des Gesetzgebers, der neben Bagatelltaten lediglich solche Fälle ausschließen wollte, in denen die Durchbrechung des Schutzes für jedermann ohne weiteres möglich ist, nicht aber solche, in denen die Zugangssicherung aufgrund spezieller Kenntnisse oder Möglichkeiten im Einzelfall leicht überwunden wird (BGH a.a.O. Rn. 24 unter Verweis auf BT-Drucks. 16/3656, S. 10). Eine solche abstrakt-generelle Betrachtungsweise ist unter Berücksichtigung des von § 202a StGB geschützten Rechtsguts – dem formellen Geheimhaltungsinteresse des Verfügungsberechtigten – geboten (BGH a.a.O.). Es genügt, dass der Täter durch die Schutzvorkehrung zu einer Zugangsart gezwungen wird, die der Verfügungsberechtigte erkennbar verhindern wollte (BGH, Beschl. v. 06.07.2010 – 4 StR 555/09 –, Rn. 6, juris = BeckRS 2010, 18206).

Ein solcher Fall liegt hier vor. Die Geschädigte hat erkennbar nicht gewollt, dass das Passwort für die Datenbank mit Endkundendaten dem Quellcode ihrer Software entnommen wird. 44

Der Tatbestandsmäßigkeit steht nicht entgegen, dass die Geschädigte den Zugriff des Angeklagten auf die Kundendaten durch Nichteinhaltung der gebotenen Sicherheitsanforderungen der Software, insbesondere die fest einprogrammierte Ablage des unverschlüsselten Passwortes (vgl. Deusch/Eggendorfer, K&R 2023, 649, 652), ermöglicht hat. Soweit dem Erfordernis der „besonderen Sicherung“ ein viktimodogmatisches Element entnommen wird, wonach solche Verhaltensweisen auszunehmen sind, denen gegenüber das Opfer nicht schutzwürdig und -bedürftig ist (Valerius, in: Graf/Jäger/Wittig/Valerius, Wirtschafts- und Steuerstrafrecht, 2. Aufl. 2017, StGB § 202a Rn. 19, Eisele, in: Schönke/Schröder, StGB, 30. Aufl. 2019, § 202 Rn. 1a; vor § 13 Rn. 70b, vgl. zum vorliegenden Fall auch Kipker, MMR 2023, 866, 868), führt dies hier zu keiner anderen Beurteilung. Das für die Beurteilung der Strafbarkeit entscheidende Geheimhaltungsinteresse des Berechtigten wird bereits durch die Verwendung des Passworts als solche dokumentiert. Demzufolge stellen Passwörter nach richtiger Auffassung etwa auch dann eine besondere Sicherung gegen unberechtigten Zugang dar, wenn „Allerweltsnamen“, einfache Buchstaben- und Zahlenfolgen oder leicht zu erratende Bezeichnungen verwendet werden (Eisele, a.,a.O. § 202a Rn. 14 m.w.N. auch zu abw. Auffassungen). Auch die „zufällige“ Kenntnisnahme eines Passworts, etwa bei heimlicher Beobachtung der Eingabe, hebt die dadurch gewünschte Sicherung und ihren strafrechtlichen Schutz nicht auf (Graf, in: MüKoStGB, 4. Aufl. 2021, § 202a Rn. 46). Anderes gilt etwa bei Verwendung werkseitiger, standardisierte Passwörter (Eisele, a.a.O.) oder wenn ein Passwort in Rechnernähe für Benutzer ersichtlich notiert wird (Graf, a.a.O.). Bei dem hier zu beurteilenden Fall hat die Geschädigte zwar durch die unverschlüsselte Ablage des Passworts im Code der Software nachlässig gehandelt und die Effektivität des Passwortschutzes eingeschränkt. Die Zugangssicherung war aber dadurch – anders als in den zuletzt genannten Gegenbeispielen – nicht aufgehoben; vielmehr hat sich der Angeklagte auf einem dafür nicht vorgesehenen Weg, nämlich der Dekompilierung, Kenntnis vom Passwort verschafft. 45

Der Angeklagte hätte sich nach diesen Grundsätzen im Übrigen auch dann strafbar gemacht, wenn er – seiner Behauptung entsprechend – das Passwort nicht erst durch die Dekompilierung, sondern bereits durch das Auslesen des Programms mit einem „Texteditor“ in Erfahrung gebracht haben sollte. Der Angeklagte hat in diesem Zusammenhang das Tool „N.“ genannt, bei dem es sich nicht (nur) um Software für Textbearbeitung handelt, wie sie auf jedem Computer installiert ist, sondern um ein Programm zur Verwaltung von MySQL- 46

Datenbanken. Auf die Verwendung einer solchen Software deutet auch die E-Mail des Angeklagten an den ehemals Mitangeschuldigten vom 00.00.0000 hin, in der er mitteilt, dass man sich die Daten aller Kunden des Anbieters [...] „mit etwas SQL-Kenntnis“ anschauen und kopieren könne. Damit war das Auffinden des Passwortes und die Überwindung des damit verbundenen Schutzes aber nicht „für jedermann ohne weiteres möglich“, sondern erforderte eine spezielle Software und zumindest Grundkenntnisse über die Bedeutung und Funktion von Datenbanksprachen, über die ein technischer Laie nicht verfügt.

Strafverfolgungshindernisse stehen der Verurteilung nicht entgegen. Dabei kann offenbleiben, ob die Geschädigte gem. § 205 StGB strafantragsberechtigt war, was im Hinblick auf die erforderliche formelle Verfügungsberechtigung an den insoweit maßgeblichen Endkundendaten fraglich ist (vgl. Deusch/Eggendorfer, a.a.O. 653; Hillert, jurisPR-ITR 23/2023 Anm. 3, a.a.O.) Denn das Antragserfordernis ist durch die Bejahung des besonderen öffentlichen Interesses durch die Staatsanwaltschaft entfallen. Ausdrücklich hat die Staatsanwaltschaft Köln zwar nicht erklärt, dass das besondere öffentliche Interesse bejaht werde. Sie hat aber mit Stellung des Strafbefehlsantrags – und erneut mit der Erhebung der sofortigen Beschwerde gegen die Ablehnung – konkludent das öffentliche Interesse bejaht, was ausreichend ist und in jeder Lage des Verfahrens erfolgen kann (vgl. nur Graf, in: MüKoStGB, StGB § 205 Rn. 18; Fischer, StGB, § 230 Rn. 4). 47

V. 48

Das Ausspähen von Daten wird gem. 202a Abs. 1 StGB mit Geldstrafe oder Freiheitsstrafe bis zu drei Jahren bestraft. 49

Zu Lasten des Angeklagten ist zu berücksichtigen, dass die Geschädigte, deren formellen Geheimhaltungsinteresse der Straftatbestand dient, durch das vom Angeklagten veranlasste Bekanntwerden der Sicherheitslücke einen erheblichen Imageschaden erlitten hat. 50

Strafmildernd wirkt, dass er Angeklagte nicht vorbestraft ist. Zu seinen Gunsten ist außerdem zu berücksichtigen, dass die Geschädigte die Tat durch nachlässige Sicherungsmaßnahmen erheblich begünstigt hat, was sowohl den Erfolgs- als auch den Handlungsunwert verringert. Außerdem strafmildernd zu berücksichtigen ist, dass sich das Ermittlungsverfahren über einen erheblichen Zeitraum erstreckte. Weitere Belastungen infolge der gegen ihn gerichteten Ermittlungen hat der Angeklagte dadurch erfahren, dass die infolge der Wohnungsdurchsuchung sichergestellten und vom Angeklagten auch beruflich genutzten Gegenstände, darunter mehrere Notebooks, Computer und Festplatten, erst nach fast anderthalb Jahren wieder an ihn herausgegeben worden sind. 51

Das Verhalten des Angeklagten nach der Tat führt hingegen nicht zu einer weiteren Strafminderung. Insbesondere kann dem Angeklagten nicht zugutegehalten werden, dass er den ungeschriebenen Regeln des verantwortungsvollen Umgangs mit Sicherheitslücken („responsible disclosure“) entsprechend der Geschädigten vor Veröffentlichung ausreichend Gelegenheit zur Behebung der Sicherheitslücke gegeben hätte. Der Angeklagte hatte die Geschädigte zwar informiert und zur Behebung aufgefordert, jedoch bereits zuvor den ehemals mitangeschuldigten Blogger über Art und Ausmaß des Vorfalls informiert und damit zurechenbar veranlasst, dass die Sicherheitslücke unmittelbar – noch am Tag ihrer Entdeckung – öffentlich wurde und für die Geschädigte kein angemessener Zeitraum für eine Reaktion zur Verfügung stand. 52

Unter Abwägung der strafzumessungserheblichen Umstände ist eine 53

54

tat- und schuldangemessen. 55

Die Einkommensverhältnisse des Angeklagten sind nicht bekannt geworden; Angaben hierzu hat der Angeklagte nicht gemacht. Vor diesem Hintergrund schätzt das Gericht die Tagessatzhöhe des Angeklagten gem. § 40 Abs. 3 StGB in Übereinstimmung mit der Staatsanwaltschaft auf 60,- €. 56

VI. 57

Die Kostenentscheidung folgt aus § 465 Abs. 1 StPO. 58

R. 59
