Landgericht Aachen, 74 NBs 34/24

Datum:	04.11.2024
Gericht:	Landgericht Aachen
Spruchkörper:	4. kleine Strafkammer
Entscheidungsart:	Urteil
Aktenzeichen:	74 NBs 34/24
ECLI:	ECLI:DE:LGAC:2024:1104.74NBS34.24.00

Tenor:

Die Berufung des Angeklagten gegen das Urteil des Amtsgerichts Jülich vom 17.01.2024 wird als unbegründet verworfen.

Der Angeklagte trägt die Kosten des Berufungsverfahrens und seine notwendigen Auslagen.

Gründe: 1

I. 2

Das Amtsgericht Jülich hat den Angeklagten mit Urteil vom 17.01.2024 wegen Ausspähens von Daten zu einer Geldstrafe von 50 Tagessätzen zu je 60,00 € verurteilt. Gegen dieses Urteil hat der Angeklagte mit Schriftsatz seines Verteidigers vom 18.01.2024, am selben Tag eingegangen bei Gericht, Berufung eingelegt. Die Berufung hat in der Sache keinen Erfolg. 3

II. 4

Hinsichtlich der persönlichen und wirtschaftlichen Verhältnisse des Angeklagten konnte die Kammer die folgenden Feststellungen treffen: 5

Zum Zeitpunkt der Hauptverhandlung 27 Jahre alte Angeklagte wurde in G. geboren und ist derzeit in Z. wohnhaft. Er ist ledig und von Beruf Programmierer. Derzeit ist er als angestellter Programmierer bei einem in Z. ansässigen Unternehmen tätig, zuvor war er als selbstständiger Dienstleister im Bereich der IT-Branche tätig und betrieb das Unternehmen C. V., einen Dienstleisterbetrieb für Onlinehändler. 6

Ausweislich des Bundeszentralregisterauszugs vom 04.10.2024 ist der Angeklagte in der Bundesrepublik Deutschland bislang nicht strafrechtlich in Erscheinung getreten. 7

8

III.

Im Rahmen der Hauptverhandlung konnten die folgenden tatsächlichen Feststellungen getroffen werden: 9

Zu einem im Rahmen der Hauptverhandlung nicht näher aufklärbaren Zeitpunkt innerhalb von zwei Wochen vor dem 23.06.2021 nahm der Angeklagte von seinem Rechner in seiner damaligen Wohnung in der W.-straße 00 in D. aus Zugang zu einer Datenbank der R. F. GmbH & Co KG (im Folgenden: R. F.) mit Sitz in M.. Diese hostete eine eCommerce-Lösung der Y. Software GmbH und stellte sie zahlreichen Firmenkunden mit großen Online-Marktplätzen, u.a. dem J., X., II. und WF., über eine hauseigene Schnittstelle entgeltlich zur Verfügung, so dass sie auf ihrem Server über persönliche Daten von ca. 600.000 bis 700.000 Endkunden verfügte. 10

Der Angeklagte war von einem Kunden, der die Software der R. F. verwendete, damit beauftragt worden, einen Fehler auf dessen Homepage zu untersuchen. Im Rahmen der Analyse stieß der Angeklagte im Quellcode der Software der R. F. auf ein dort hinterlegtes Passwort. Tatsächlich war das Passwort „N01“ zu der Datenbank mit den Endkundendaten von der R. F. unverschlüsselt im Quellcode der Software abgelegt worden, so dass dieses nach Anwendung von frei verfügbaren Programmen – etwa durch ein Öffnen der ausführbaren Datei durch einen Texteditor, möglicherweise auch durch Dekompilierung, also durch Rückübersetzen von Maschinencode in einen für den Menschen lesbaren Quellcode, zur Kenntnis genommen werden konnte. Der Angeklagte gab nach entsprechender Kenntnisnahme das Passwort ein und erkannte spätestens hiernach, dass er nunmehr Zugriff auch auf sämtliche Endkundendaten und damit auch solche Daten hatte, auf die der ihn beauftragende Kunde keinen Zugriff haben sollte. Dennoch fertigte der Angeklagte Screenshots von den in der Datenbank der R. F. hinterlegten Kundendaten an, obwohl ihm bewusst war, dass er hierzu keine Befugnis hatte. 11

Am Morgen des 23.06.2021 wandte sich der Angeklagte unter der von ihm eingerichteten Email-Adresse E-Mail01 mit dem Betreff „NR.“ anonym an die R. F. und teilte dieser das Folgende mit: 12

„(…) Bei der Einrichtung Ihrer Software ist uns aufgefallen, dass diese versuchte, eine Datenbankverbindung in das Internet aufzubauen. Unsere Firewall hat direkt Alarm geschlagen und die Verbindungsanfrage samt Zugangsdaten geloggt. 13

Da wir grundsätzlich gewisse Kommunikationswege auf unseren Servern blockieren, wie etwa der Zugriff auf eine unbekannte, entfernte Datenbank, habe ich geprüft, worum es sich bei der Datenbank handelt. 14

Mit erschrecken musste ich feststellen, dass die übermittelten Zugangsdaten zu mehreren Datenbanken auf ihren Servern führen. Die genaue Aufstellung der Datenbanken entnehmen sie der Datei OB.. 15

Unter den Datenbanken befindet sich eine mit dem Namen VD.', in welcher eine Y.-Shop Installation vom 12.09. 2017. In diese Datenbank befinden sich empfindliche benutzerbezogene Daten wie in der Tabelle SU. zu sehen. Exemplarisch dafür die ersten zehn Einträge aus dieser Tabelle in MN.. Weitere Kundendaten lassen sich aus anderen Tabellen auslesen. Auch die Verschlüsselung ist kein Problem, denn aus der Datenbank heraus ist es möglich, Code im Shop-System auszugeben, welcher den privaten Schlüssel ausgibt. 16

Unter der Datenbank ER. befinden sich noch mehr benutzerbezogene Daten. Hier wird z.B. in der Tabelle VO. die Kundenkorrespondenz festgehalten. Siehe GF.. 17

Weitere Datenbanken, mit vermutlich vorhergehenden Helpdesks und Ticket-Systemen, wie etwa OG. und die YK., enthalten teilweise ebenfalls empfindliche Daten. Dazu habe ich Ihnen als Beispiel die DX. angehangen. 18

Ich bitte Sie, innerhalb der nächsten zwei Werktage Ihre Kunden und den Landesdatenschutzbeauftragten (nachweislich) über das NR. zu informieren. 19

Zudem bitte ich Sie, dass NR. innerhalb von 7 Werktagen zu schließen. 20

Ich erbitte zusätzlich zu den Forderungen ebenfalls einen Nachweise, welchen Sie mir über diese E-Mail-Adresse zusenden können. 21

Ich bitte um eine Lesebestätigung. 22

Mit freundlichen Grüßen 23

Anonym“ 24

Die R. F. erstatte am 25.06.2021 Strafanzeige. 25

IV. 26

Die Feststellungen zu den persönlichen und wirtschaftlichen Verhältnissen beruhen auf den im Rahmen der Hauptverhandlung verlesenen erstinstanzlichen, glaubhaften Angaben des Angeklagten sowie der seitens des Angeklagten als richtig bestätigten Auskunft aus dem Bundeszentralregister. Die tatsächlichen Feststellungen beruhen auf der ebenfalls gemäß § 256 StPO verlesenen, teilgeständigen Einlassung des Angeklagten, soweit dieser gefolgt werden konnte, sowie den sonstigen ausweislich des Hauptverhandlungsprotokolls erhobenen Beweisen, insbesondere den gemäß §§ 249 ff. StPO verlesenen Urkunden. 27

Der Angeklagte hat sich im Rahmen der erstinstanzlichen Hauptverhandlung dahingehend eingelassen, dass er zwei Wochen vor dem Vorfall von einem Kunden auf einen Fehler auf seine Homepage aufmerksam gemacht worden sei. Der Kunde habe gewollt, dass er sich den Fehler anschaue. Die Datenbank sei so groß geworden, dass ein Limit erreicht worden sei, sodass der Kunde die Homepage nur noch eingeschränkt habe nutzen können. Er habe sich die Software angesehen um auszuschließen, dass der Fehler erneut auftauchen würde. Dabei habe er festgestellt, dass die Software eine Verbindung aufbaue, die untypisch sei. Er habe innerhalb von fünf Minuten eine Verbindung gefunden und eine generische Nummer. Diese habe N02 gelautet. Er habe sich zu dieser Datenbank verbunden, weil er gedacht habe, das sei die Nummer seines Kunden. Dabei habe er festgestellt, dass dort deutlich mehr Daten lagerten als nur diejenigen von seinem Kunden. Dann habe er die Datenbank getrennt. 28

Das Programm bei seinem Kunden habe er im Texteditor geöffnet. Er habe sich dann mit einem Klienttool verbunden und festgestellt, dass es deutlich mehr Daten gewesen seien, als er vermutet habe. Er erinnere sich nicht daran, ob er eine Dekompilierung vorgenommen habe. Es sei schwer zu beurteilen, ob er mit seiner Firma eine Konkurrenz zu der R. F. dargestellt habe, sie seien beide Dienstleister und hätten verschiedene Schnittstellen zu Firmen hergestellt. Er habe die R. F. aus dem Y.-Umfeld gekannt. Es sei richtig, dass er die E-Mail-Adresse „E-Mail01“ eingerichtet habe. Die Intention sei gewesen, dass er seine Identität habe verschleiern wollen. Er habe der R. F. nicht schaden wollen. Er habe lediglich 29

mit ihr kommunizieren wollen, damit sie in Zukunft eine sichere Software anbieten könnten. Er habe den Netzverkehr in der virtuellen Umgebung mitgelesen. Mithilfe dieser Informationen habe er in seinen Texteditor z.B. nach dem Hostnamen suchen können und in unmittelbarer Nähe habe das Kennwort gestanden. Das Kennwort sei im Klartext hinterlegt gewesen. Er habe sich zu der Datenbank verbunden und sehr schnell festgestellt, dass dort mehr Daten seien, als für den Kunden sichtbar sein sollten. In dem Moment habe er aufgehört. Er habe Exit eingegeben und sich abgemeldet. Die Daten habe er nicht gesichert. Er habe keine Screenshots erstellt. Er habe gedacht, dass es sich um die Datenbank des Kunden N02 handele. Die „exe“-Datei sei auf dem dem Kunden zur Verfügung gestellten Server installiert gewesen.

Der Angeklagte hat somit eingeräumt, das Passwort, welches zu der die Endkundendaten enthaltenden Datenbank führte, dem Quellcode der seinem Kunden zur Verfügung gestellten Software der R. F. entnommen zu haben, welches dort im Klartext hinterlegt gewesen sei, und auf die Datenbank Zugriff genommen zu haben. Insoweit bestehen nach dem Ergebnis der Beweisaufnahme zwar mehrere Hinweise darauf, dass zuvor – entgegen der Einlassung des Angeklagten – eine Dekompilierung des Quellcodes erforderlich war; hierauf deuten etwa die Angaben der Vertreter der R. F. im Rahmen der verlesenen Strafanzeige hin, in welcher festgehalten ist, die Dekompilierung sei nach „interner Prüfung“ aus dortiger Sicht das wahrscheinlichste Szenario. Auch wurde in dem polizeilichen Ermittlungsbericht vom 26.01.2022, welcher ebenfalls im Rahmen der Hauptverhandlung verlesen worden ist, festgehalten, dass auf dem in Rahmen der Durchsuchung bei dem Angeklagten sichergestellten Rechner nicht nur die Software der Geschädigten, die ausführbare, kompilierte Datei „QW.“, sondern auch ein Dekompilat festgestellt wurde, welches das veröffentlichte Passwort „N01“ enthielt. Auf dem PC des Angeklagten waren zudem ausweislich des polizeilichen Auswertungsberichts vom 13.10.2021, welcher ebenfalls im Rahmen der Hauptverhandlung verlesen worden ist, Programme installiert, mit denen eine sogenannte Dekompilation durchgeführt werden konnte, unter anderem die Programme „PQ.“ und „TZ.“ des Herstellers XR.. Aus dem Bericht ergibt sich, dass sich konkrete Spuren der Anwendung einer die Dekompilierungssoftware finden; so finden sich in verschiedenen Verzeichnissen scheinbar dekompilierte Dateien, welche in den ersten Zeilen des Quellcodes den Kommentar „YC.“ sowie einen Kommentar des Ziels der die Komprimierung (DB.) angeben. Der dekompilierte Code enthält an verschiedenen Stellen vom Benutzer erstellte Kommentare, in denen sich augenscheinlich über die Qualität des Quellcodes lustig gemacht wurde; diese lauten: *UV. sowie UE.* Letztlich kann die Frage einer Dekompilierung jedoch nach Ansicht der Kammer dahinstehen (vgl. hierzu unter V.). 30

Die Kammer geht zudem davon aus, dass dem Angeklagten bereits beim ersten Zugriff bewusst war, dass er sich unerlaubt Zugang zu einer passwortgesicherten Kunden Datenbank verschafft hat und es sich bei seiner entgegenstehenden Behauptung, der Zugriff sei gewissermaßen „versehentlich“ erfolgt, um eine in Anbetracht der besonderen IT Kenntnisse des Angeklagten unglaubhafte Schutzbehauptung handelt. Letztlich kann dies jedoch dahinstehen, da dem Angeklagten jedenfalls in dem Zeitpunkt, als Screenshots von den Kundendaten gefertigt wurden, bekannt war, dass es sich um Daten handelt, die weder für ihn, noch für seinen Kunden bestimmt waren und hinsichtlich welcher kein Verfügungsrecht seines Kunden bestand. Dass entgegen der Einlassung des Angeklagten entsprechende Screenshots gefertigt wurden, ergibt sich nach Ansicht der Kammer aus dem Inhalt der im Rahmen der Hauptverhandlung verlesenen E-Mail vom 23.06.2021, in welcher auf zahlreiche derartige Screenshots Bezug genommen wird. Der Inhalt der entsprechenden E-Mail kann nach Ansicht der Kammer nur dahingehend verstanden werden, dass entsprechende Screenshots auch tatsächlich gefertigt wurden; dass der Angeklagte das 31

Vorhandensein entsprechender JPEG-Dateien behauptet haben sollte, ohne entsprechende Screenshots tatsächlich gefertigt zu haben, ist fernliegend und wird von dem Angeklagten, der auf entsprechende Nachfrage des Amtsgerichts auch lediglich erklärt hat, sich „nicht daran zu erinnern, Kundendaten mitgeschickt“ zu haben, auch nicht behauptet. Der Angeklagte hat schließlich eingeräumt, die E-Mail-Adresse, von welcher am 23.06.2021 die in den Feststellungen dargestellte E-Mail versendet wurde, eingerichtet zu haben; dies ergibt sich im Übrigen auch aus dem im Rahmen der Hauptverhandlung verlesenen Ermittlungsbericht, wonach bei einem eingeschalteten System in den Räumlichkeiten des Angeklagten bereits unmittelbar vor Ort eine regelmäßige Zugriff auf das verwendete E-Mail Postfach E-Mail01 festgestellt wurde. In dem E-Mail-Postfach befanden sich mehrere E-Mails mit dem Wort „NR.“ im Betreff; unter anderem informierte der Absender hierüber am 02.07.2021 die Firma CR. über das zugrundeliegende NR. und bot seine Unterstützung für etwaige Rückfragen an. Außerdem konnte die E-Mail vom 23.06.2021 an die R. F. ebenfalls in dem Postfach aufgefunden werden.

V. 32

Nach den getroffenen Feststellungen hat sich der Angeklagte wegen Ausspähens von Daten schuldig gemacht, strafbar gemäß § 202a Abs. 1 StGB. 33

Der Angeklagte hat sich unter Überwindung der Zugangssicherung unbefugt Zugang zu der Datenbank der R. F. verschafft, obwohl die enthaltenen Daten nicht für ihn bestimmt und gegen unberechtigten Zugang besonders gesichert waren. 34

Unter den allgemeinen Datenbegriff fallen grundsätzlich solche Informationen, die für eine Datenverarbeitungsanlage codiert sind, wobei eine Verarbeitung nicht zwingend bezweckt sein muss (vgl. Mansdörfer, in: BeckOK IT-Recht, 16. Ed. 1.10.2024, StGB § 202a Rn. 4, beck-online). 35

Die in der Datenbank enthaltenen Informationen waren nicht für den Angeklagten bestimmt. Maßgebend ist diesbezüglich der Willen des Dispositionsbefugten (vgl. Mansdörfer, in: BeckOK IT-Recht, 16. Ed. 1.10.2024, StGB § 202a Rn. 9, beck-online m.w.Software; Grözinger, in: Müller/Schlothauer/Knauer, Münchener Anwaltshandbuch Strafverteidigung, 3.A., § 50 Cybercrime und Datenkriminalität, Rn. 33), vorliegend mithin der R. F.. Nach ihrem Willen indes sollten weder der Angeklagte, noch sein Auftraggeber Zugang zu der vollständigen Datenbank erhalten. Denn in dieser waren in erheblichem Umfang gerade auch Daten solcher Personen enthalten, bei denen es sich nicht um Endkunden des Auftraggebers des Angeklagten handelte. Unabhängig davon, dass der Auftraggeber des Angeklagten – wie von diesem im Rahmen eines Beweisantrags behauptet – ordentlicher Kunde der R. F. gewesen sein und als solcher auch über eine Nutzungsberechtigung der hier betroffenen Software verfügt haben mag, umfasste seine Dispositionsbefugnis jedenfalls nicht solche Endkundendaten, die nicht durch ihn, sondern lediglich durch andere Online-Händler erzeugt, abgespeichert oder empfangen worden waren (vgl. hierzu Mansdörfer, in: BeckOK IT-Recht, 16. Ed. 1.10.2024, StGB, § 202a Rn. 9, beck-online). Soweit der Angeklagte durch seinen Verteidiger im Rahmen eines von ihm gestellten Beweisantrags behauptet hat, Gegenstand der Nutzungslizenz seines Auftraggebers sei auch ein Zugriffsrecht auf die hier betroffene Kundendatenbank gewesen, so hält die Kammer dies zwar – insbesondere in Anbetracht der auch gegenüber dem Auftraggeber des Angeklagten bestehenden Passwortsicherung (vgl. hierzu noch unten) für äußerst fernliegend, letztlich kann dies jedoch dahinstehen. Denn jedenfalls hätte ein solches Zugriffsrecht lediglich begrenzt bestanden (vgl. hierzu BGH, NStZ-RR 2020, 278, 279), und lediglich soweit gereicht, wie eine Nutzung der Datenbank für den Zweck des Geschäftsbetriebs des Auftraggebers des Angeklagten erforderlich gewesen 36

wäre. Ein solches Zugriffsrecht mag auch Zwecke der Fehlersuche oder Fehlerbehebung der von dem Kunden genutzten Software umfasst haben; jedenfalls das Anfertigen von Screenshots von solchen Daten, die erkennbar keine eigenen Kundendaten waren, war von einem dem Auftraggeber des Angeklagten zugewiesenen Nutzungsrecht indes erkennbar nicht umfasst. Jedenfalls insoweit war ein Einverständnis zur Nutzung der Daten durch die Berechtigte und eine Bestimmung der Daten für den Angeklagten daher nicht gegeben (vgl. hierzu Graf, in: Münchener Kommentar zum StGB, 4. Aufl. 2021, StGB § 202a Rn. 23, beck-online).

Der Angeklagte hat sich die Daten auch verschafft. Verschaffen von Daten bedeutet das Erlangen der tatsächlichen Herrschaft über die Daten, wobei dies entweder durch Besitzverschaffung am Ursprungs-Datenträger, durch Kopieren auf ein eigenes Speichermedium, durch Kenntnisnahme oder durch eine sonstige Aufzeichnung der Daten erfolgen kann (Graf, in: Münchener Kommentar zum StGB, 4. Aufl. 2021, StGB § 202a Rn. 56, beck-online). Im vorliegenden Fall hat sich der Angeklagte die Daten dementsprechend in zweifacher Hinsicht verschafft: Er hat sie zum einen zur Kenntnis genommen, zum anderen jedoch auch Screenshots gefertigt. Wer auf einem Monitor sichtbare Daten abschreibt, ablichtet bzw. eine Videoaufzeichnung fertigt oder einen Bildschirmausdruck (Hardcopy) herbeiführt, „verschafft“ sich diese (Graf, in: Münchener Kommentar zum StGB, 4. Aufl. 2021, StGB § 202a Rn. 58, beck-online). 37

Soweit der Angeklagte sich darauf berufen hat, er habe die Daten zunächst gewissermaßen „versehentlich“ zur Kenntnis genommen, da er davon ausgegangen sei, dass die Eingabe des von ihm aufgefundenen Passworts lediglich zu Kundendaten seines Auftraggebers führe, so mag dies geeignet sein, bezüglich der erstmaligen Kenntnisnahme einen Vorsatz des Angeklagten hinsichtlich des „Verschaffens“ von Daten auszuschließen; jedenfalls aber anlässlich der willentlichen Fertigung der Screenshots war dem Angeklagte bewusst, dass er sich Daten verschaffte, die nicht für ihn oder seinen Kunden bestimmt waren, so dass jedenfalls diese zweite Tathandlung auch vorsätzlich erfolgte. 38

Die Daten waren zudem gegen unberechtigten Zugang besonders gesichert, wobei der Angeklagte die entsprechende Zugangssicherung überwunden hat. 39

Die besondere Sicherung muss den Zweck haben, den Zugang Unbefugter zu den geschützten Daten zu verhindern oder zumindest erheblich zu erschweren (Graf, in: Münchener Kommentar zum StGB, 4. Aufl. 2021, StGB § 202a Rn. 39, beck-online). Zur Art der Sicherung hat der Gesetzgeber keine Vorgaben gemacht, jedoch zur Auslegung des Begriffs auf die Regelungen der § 202 Abs. 2 StGB und § 243 Abs. 1 Nr. 2 StGB verwiesen. Allerdings kann dies nicht abschließend sein, da dort allein körperliche Gegenstände geschützt werden, während Daten vielfach auch in unkörperlicher Form (zB bei Be- und Verarbeitung oder während der Übermittlung) vorliegen. Daher kommen sowohl physische Schutzmaßnahmen für die Datenverarbeitungs- bzw. Übertragungsanlage (bauliche Maßnahmen und/oder technische Schutzvorrichtungen) als auch – der Datentechnik entsprechend – systemimmanente Sicherungen auf Hardware- oder Software-Ebene in Betracht (Graf, in: Münchener Kommentar zum StGB, 4. Aufl. 2021, StGB § 202a Rn 40, beck-online). Daten sind jedenfalls dann besonders gesichert, wenn Vorkehrungen getroffen sind, den Zugriff auf Daten auszuschließen oder wenigstens nicht unerheblich zu erschweren. Durch die Sicherung muss der Berechtigte sein spezielles Interesse an der Geheimhaltung dokumentieren (vgl. BT-Dr. 16/3656, S. 10; BGH, Beschluss vom 27. Juli 2017 – 1 StR 412/16 –, Rn. 38, juris m.w.Software). 40

41

Eine Sicherung durch Passwörter reicht als Zugangssicherung grundsätzlich aus (BGH, NStZ-RR 2020, 278, beck-online m.w.Software). Diese Sicherung hat der Angeklagte vorliegend überwunden, indem er das Passwort zur Datenbank der R. F. aus den Quellcode ihrer Software ausgelesen und durch die anschließende Eingabe des Passworts Zugriff auf die Endkundendaten erlangt hat. Ob es zuvor einer sog. Dekompilierung des Quellcodes bedurfte, ist nach Ansicht der Kammer nicht entscheidend.

Eine besondere Sicherung des Quellcodes stellt eine Kompilierung nicht dar. Wenn die Rückübersetzung mittels gängiger Hilfsprogramme möglich ist – wovon hier auszugehen ist –, fehlt es an der entsprechenden Tatbestandsvoraussetzung (vgl. hierzu Graf, in: Münchener Kommentar zur StGB, 4. Aufl. 2021, § 202a, Rn. 34). 42

Ein Computerprogramm, welches ursprünglich in Form eines „Quellcodes“ in einer verständlichen Programmiersprache abgefasst ist, wird mittels eines als „Compiler“ bezeichneten speziellen Programms in eine für den Computer ausführbare Form, d.h. den „Objektcode“, umgewandelt. Der Vorgang der Umwandlung des Quellcodes in den Objektcode wird „Kompilierung“ genannt (EuGH, in: MMR 2021, 951 Rn. 35-37, beck-online). Die Kompilierung dient damit gerade nicht dem Schutz des Quellcodes, sondern erreicht einen solchen – wenn auch in schwacher Form – allenfalls als Nebeneffekt. Vorliegend steht jedoch auch nicht das Ausspähen des Quellcodes in Rede, bei welchem es sich unzweifelhaft ebenfalls um Daten handelt. Ein solches kann daher letztlich dahinstehen. Ansatzpunkt des strafbaren Verhaltens des Angeklagten ist vielmehr der Zugriff auf die Endkundendaten in der passwortgesicherten Datenbank der R. F.. Diese waren jedoch – wie ausgeführt – passwortgesichert. Lediglich dann, wenn die entsprechende Passwortsicherung völlig unzureichend gewesen wäre, könnte das Tatbestandsmerkmal der „besonderen Sicherung“ vorliegend verneint werden. 43

Soweit sich der Angeklagte darauf beruft, die Daten seien nachlässig gesichert gewesen, da das Passwort im Klartext dergestalt im Objektcode der Datei QW. zum Tatzeitpunkt enthalten gewesen sei, dass bereits ein schlichtes Öffnen der ausführbaren Datei mit einem Texteditor genügt hätte, um diese zur Kenntnis zu nehmen, führt dies nach Ansicht der Kammer nicht zu einem Ausschluss des objektiven Tatbestands. Für das Vorliegen einer Zugangssicherung ist auf die allgemeine Sicherung der Daten gegenüber dem Zugriff Unbefugter abzustellen, nicht darauf, ob Eingeweihte oder Experten leicht auf die Daten zugreifen können. Es ist auch nicht erforderlich, dass die Sicherung gerade gegenüber dem Täter wirkt (vgl. BGH, NStZ-RR 2020, 278, beck-online m.w.Software). 44

Wenn es in den Gesetzesmaterialien heißt, die Überwindung der Zugangssicherung müsse einen nicht unerheblichen zeitlichen oder technischen Aufwand erfordern, weshalb vom Tatbestand solche Fälle nicht erfasst würden, in denen die Durchbrechung des Schutzes ohne weiteres möglich sei (BT-Dr. 16/3656, S. 10), wird dies seitens des Bundesgerichtshofs (vgl. BGH a.a.O.) dahingehend ausgelegt, dass die Überwindung der Zugangssicherung typischerweise – also unabhängig von spezifischen Möglichkeiten oder Kenntnissen des konkreten Täters – einen nicht unerheblichen Aufwand erfordern muss. Unter Überwinden ist diejenige Handlung zu verstehen, die geeignet ist, die jeweilige Sicherung auszuschalten oder zu umgehen. Auch wenn eine Zugangssicherung auf Grund besonderer Kenntnisse, Fähigkeiten oder Möglichkeiten schnell und ohne besonderen Aufwand überwunden wird, ist der Tatbestand erfüllt. Für das geschützte Rechtsgut – das formelle Geheimhaltungsinteresse des Verfügungsberechtigten (vgl. BGH a.a.O. m.w.Software; BGH, NStZ N02, 401, beck-online) – ist es unerheblich, ob die Sicherung von Daten vor unberechtigtem Zugang schnell oder langsam, mit viel oder wenig Aufwand überwunden wird. Der Gesetzgeber wollte aus 45

dem Tatbestand neben Bagatelltaten lediglich solche Fälle ausschließen, in denen die Durchbrechung des Schutzes für jedermann ohne weiteres möglich ist, nicht aber solche, in denen die Zugangssicherung auf Grund spezieller Kenntnisse oder Möglichkeiten im Einzelfall leicht überwunden wird. Nur eine solche abstrakt-generelle Betrachtungsweise lässt sich mit dem Schutzzweck der Norm vereinbaren (BGH, NStZ-RR 2020, 278, beck-online).

Hiernach waren die Daten im Sinne der Norm besonders gesichert, und der Angeklagte hat die entsprechende Zugangssicherung überwunden. Zwar kann von einer Sicherung dann nicht ausgegangen werden, wenn eine Passwortabfrage umgangen werden kann oder beispielsweise das Passwort in Rechnernähe für Benutzer ersichtlich notiert ist (Graf, in: Münchener Kommentar zum StGB, 4. Aufl. 2021, § 202a Rn. 46, beck-online). Ein solcher Fall – in dem von einer deutlichen, dem Täter gesetzten Schranke oder bzw. einem seitens des Berechtigten dokumentierte, ernsthaften Geheimhaltungsinteresse auch nicht ausgegangen werden kann – liegt hier indes nicht vor. Die Anforderungen an den notwendigen „nicht unerheblichen zeitlichen oder technischen Aufwand“ zur Überwindung der Sicherung dürfen zum Schutz technischer Laien freilich nicht zu hoch angesetzt werden. Daher wird man bei Passwörtern auch „Allerweltsnamen“, einfache Buchstaben- und Zahlenfolgen sowie leicht zu erratende Bezeichnungen genügen lassen müssen, da auch diese das Interesse an der Geheimhaltung dokumentieren (Schönke/Schröder/Eisele, 30. Aufl. 2019, StGB § 202a Rn. 14, beck-online). 46

Zwar mag die Sicherung der Endkundendaten durch ein im Quellcode hinterlegtes Passwort im konkreten Fall durchaus nachlässig gewesen sein; dennoch liegt eine Zugangssicherung vor, die eine deutliche Schranke setzte und deren Überwindung kriminelle Energie manifestierte (vgl. BGH a.a.O.; Gottwald/Ohrloff: Strafrechtliche Risiken bei der Entschlüsselung passwortgeschützter Dateien im Rahmen einer internen Untersuchung, CCZ 2022, 253 m.w.Software). Denn ein Auslesen des Passworts erforderte jedenfalls spezielle Kenntnisse und war nicht für jedermann ohne weiteres möglich. So wäre es einem IT-technischen Laien ohne weitere Recherche voraussichtlich bereits nicht bekannt, mittels welcher Programme überhaupt der Quellcode einer Software ausgelesen werden kann; darüber hinaus müsste ein entsprechendes Programm auch korrekt verwendet werden. Darauf, dass dies jedenfalls gewisse IT-Kenntnisse voraussetzt, deutet auch die Email des Angeklagten an den gesondert verfolgten MU., in welcher er erwähnt, dass man sich „die Daten aller Kunden des Anbieters (…) *mit etwas SQL-Kenntnis* anschauen und kopieren könnte“. Jedenfalls aber würde ein Laie wohl kaum über das Wissen verfügen, dass sich in dem Quellcode der Software – so er denn aufgefunden und ausgelesen werden könnte - an einer bestimmten Stelle ein Passwort befinden könnte. Selbst wenn ein Laie auch über dieses Wissen theoretisch verfügen würde, müsste das Passwort zudem an einer konkreten Stelle innerhalb des Codes aufgefunden werden. Jedenfalls dies hält die Kammer auch bei Betrachtung des kleinen Auszugs des Quellcodes, welcher dem seitens des Angeklagten gestellten Beweisantrag angehängt ist, für einen Laien ohne längere Recherche und ohne spezielles Wissen für kaum möglich. 47

Das Auffinden des Passwortes und die Überwindung des damit verbundenen Schutzes war – worauf bereits das Amtsgericht zutreffend hingewiesen hat – damit gerade nicht für jedermann ohne weiteres möglich, sondern erforderte die Kenntnis und Anwendung einer bestimmten Software sowie zumindest Grundkenntnisse über die Bedeutung und Funktion von Datenbanksprachen, über die ein technischer Laie nicht verfügt. 48

Eine Rechtfertigung des Angeklagte – etwa eine solche gemäß § 34 StGB – ist nicht ersichtlich. Der Modernisierung des Tatbestandes des § 202a StGB im Jahr 2007 lag die 49

Überlegung zugrunde, dass böswillig handelnde Hacker – sog. Black Hats – generell strafbar und die sog. White Hats, die im Auftrag des Verfügungsberechtigten handeln, straffrei sein sollten (BT-Drs. 16/3656, 10; Mansdörfer, in: BeckOK IT-Recht, 15. Ed. 1.7.2024, StGB § 202a, Rn. 29, beck-online). Dass er im Auftrag der Berechtigten – der R. F. – mit der Suche nach IT-Sicherheitslücken beauftragt gewesen sei, behauptet der Angeklagte indes nicht.

Ein sog. Grey-Hat-Hacker kann sich nicht auf eine Einwilligung des Verfügungsberechtigten berufen, handelt aber nicht böswillig. Für ihn kommt unter Umständen auch eine Rechtfertigung gemäß § 34 StGB in Betracht. Voraussetzung hierfür ist indes, dass die Sicherheitslücke schon vor dem Eindringen in das System bekannt ist. Ein verdachtsmäßiges Eindringen in ein Informationssystem wird von § 34 StGB regelmäßig nicht erfasst (Mansdörfer, in: BeckOK IT-Recht, 15. Ed. 1.7.2024, StGB § 202a, Rn. 30 f., beck-online). Vorliegend scheidet eine Rechtfertigung nach Ansicht der Kammer allerdings bereits deshalb aus, weil jedenfalls mildere Mittel als die Anfertigung von Screenshots der fremden Daten bestanden hätten; insoweit ist als naheliegende von vieler Möglichkeiten etwa ein schlichter Hinweis auf das – nach den Angaben des Angeklagten zufällig vorgefundene – NR. zu nennen. Lediglich ergänzend ist in diesem Zusammenhang darauf hinzuweisen, dass die Emailadresse, unter welcher der Angeklagte die R. F. kontaktierte, um sie unter Hinweis auf die gefertigten Screenshots mit dem NR. zu konfrontieren - E-Mail01 – durchaus bei entsprechender Umstellung der Buchstaben als „OQ.“ gelesen werden kann. Dies lässt – ohne dass es hierauf im Ergebnis ankäme – an redlichen Motiven des Angeklagten jedenfalls gewisse Zweifel aufkommen. 50

Der Angeklagte handelt schließlich auch schuldhaft; Entschuldigungsgründe sind nicht ersichtlich. 51

VI. 52

Bei der Strafzumessung hat sich die Kammer im Wesentlichen von folgenden Erwägungen leiten lassen: 53

Auszugehen war vom Strafrahmen des § 202a Abs. 1 StGB, welcher Freiheitsstrafe bis zu drei Jahren oder Geldstrafe vorsieht. 54

Zugunsten des Angeklagten sprach im vorliegenden Fall, dass er sich jedenfalls teilgeständig eingelassen hat. Die Geschädigte hat die Tat zudem durch ein besonders nachlässiges Vorgehen im Rahmen der Sicherung ihrer Daten zudem erheblich begünstigt. Der Angeklagte ist nicht vorbestraft. Zu seinen Gunsten wirkt sich zudem aus, dass er die Daten zwar durch Screenshots gesichert, jedoch nicht in sonstiger Weise zweckwidrig verwendet hat. Strafmildernd ist weiterhin zu berücksichtigen, dass die Tat bereits mehr als drei Jahre zurückliegt. Der Angeklagte ist überdies durch im Rahmen des Ermittlungsverfahrens ergriffene Maßnahmen, insbesondere die bei ihm vollzogene Wohnungsdurchsuchung, erheblich belastet. Sichergestellte Gegenstände, insbesondere Notebooks, Computer und Festplatten, sind erst etwa eineinhalb Jahre später wieder an den Angeklagten zurückgelangt, wobei die Kammer zu seinen Gunsten davon ausgeht, dass hierdurch auch die berufliche Tätigkeit des Angeklagten nachteilig beeinflusst wurde. Auch mag zugunsten des Angeklagten davon ausgegangen werden, dass sein Verhalten letztlich zu besseren Sicherheitspraktiken geführt und somit letztlich auch der Datensicherheit von Endkundendaten gedient haben mag. Soweit das Amtsgericht davon ausgegangen ist, die R. F. habe durch das Verhalten des Angeklagten einen erheblichen Imageschaden erlitten und dieser habe ihr nicht ausreichend Zeit eingeräumt, um die Sicherheitslücke zu schließen, hat die Kammer die entsprechenden Aspekte nicht zum Nachteil des Angeklagten berücksichtigt. 55

Denn die Veröffentlichung des Datenlecks ist maßgeblich nicht auf das Verhalten des Angeklagten, sondern dasjenige des früheren Mitbeschuldigten MU. zurückzuführen. Dennoch hält die Kammer in Anbetracht der Vielzahl potentiell betroffener Daten die seitens des Amtsgerichts verhängte, am unteren Rand des Vertretbaren bemessene Geldstrafe von 50 Tagessätzen für tat- und schuldangemessen. Mangels konkreter Angaben des Angeklagten zu seinen Einkommensverhältnissen hat die Kammer diese gemäß § 40 Abs. 3 StGB geschätzt. Unter Berücksichtigung eines Gehaltsvergleichs des Statistische Bundesamtes ist von einem durchschnittlichen Brutto-Monatsverdienst eines angestellten Programmierers in Nordrhein-Westfalen im ungefähren Alter es Angeklagten von circa 4.600 Euro auszugehen. Dies entspricht einem Nettogehalt von circa 2.926,00 € und führt zu einer deutlich höheren Tagessatzhöhe. Selbst unter der Annahme, dass der Angeklagte ein weit unterdurchschnittliches Gehalt bezieht und relevante, aber unbekannte Zahlungsverpflichtungen bestehen, ist eine Tagessatzhöhe von 60,00 € daher jedenfalls angemessen. An einer Erhöhung ist die Kammer im Übrigen auch aufgrund des Verschlechterungsverbots zugunsten des Angeklagten gehindert.

VII. 56

Die Kostenentscheidung beruht auf § 473 Abs. 1 StPO. 57
