Bild: KI Midjourney | Collage c't

Unversehens kriminell

„Hackerparagrafen“ und warum sie problematisch sind

Ein aktueller Fall beleuchtet, wie bedenklich und strittig in der Auslegung die sogenannten Hackerparagrafen sind. IT-Dienstleister sollten die Risiken genau kennen: Auch mit guten Absichten kann man sich strafbar machen.

Von Sylvester Tremmel

Mitte Januar dieses Jahres wurde ein Programmierer nach Paragraf 202a des Strafgesetzbuches (StGB) verurteilt. Obwohl es um die Entscheidung eines Amtsgerichts geht, also den Anfang der Instanzenkette, obwohl der Programmierer zu einer Geld- und nicht zu einer Haftstrafe verurteilt wurde und obwohl die Entscheidung noch nicht rechtskräftig ist (der Angeklagte hat Berufung eingelegt), zog der Fall weite Kreise. Denn in ihm scheint sich die lange gehegte Befürchtung zu verwirklichen, dass wohlmeinende Softwareentwickler bei der normalen Ausübung ihrer Arbeit straffällig werden.

Im konkreten Fall sollte der Angeklagte für einen seiner Kunden ein Softwareproblem lösen. Die fragliche Software stammte von der Modern Solution GmbH & Co. KG aus Gladbeck. Der Angeklagte bemerkte, dass sie eine MySQL-Verbindung zu einem Server dieser Firma unterhielt, und griff ebenfalls auf die Datenbank zu, mit der die Software kommunizierte. Nach eigenen Angaben tat er das in der Annahme, dass es sich um eine Datenbank spezifisch für seinen Kunden handele, die nur dessen Daten enthalte. Für den Zugriff nutzte er offenbar das bekannte DB-Admin-Tool phpMyAdmin; das nötige Passwort hatte er aus dem Binärcode der Modern-Solution-Software extrahiert. Nach Darstellung der Staatsanwaltschaft nutzte er dafür einen Decompiler. Der Angeklagte gab an, die Programmdatei lediglich in einem Texteditor geöffnet zu haben. Der zeigte dann neben binärem Kauderwelsch auch Verbindungsdaten und Passwort in Textform und nahe beieinander an.

Fatalerweise enthielt die Datenbank die Informationen von etwa 700.000 Kunden der Gladbecker Firma, auf die der Angeklagte mit dem Passwort zugreifen konnte. Aus IT-Sicherheitsperspektive ist das ein massives Versagen von Modern Solution: Niemals sollte ein Kunde über Zugangsdaten verfügen, die auch den Zugriff auf Daten anderer Kunden ermöglichen. Um die technische Perspektive und auch die Art und Weise, wie das Problem öffentlich gemacht wurde, soll es hier aber nicht gehen. Heise online hat mehrfach darüber berichtet [1, 2].

Rechtlich begab sich der Angeklagte bereits durch die Extraktion und Verwendung des Passworts auf ganz dünnes Eis: Er verschaffte sich damit „Zugang zu Daten, die nicht für ihn bestimmt“ waren. Genau das stellt – unter Einschränkungen, um die es gleich noch gehen wird – § 202a StGB seit 2007 unter Strafe. Damals wurde dieser Paragraf neu gefasst und das Strafgesetzbuch um §§ 202b und 202c ergänzt (siehe Kasten).

Begleitet wurde diese Änderung von massiver Kritik. Damals kam auch der Begriff „Hackerparagrafen“ auf. Die Kritik richtete sich primär gegen den neuen § 202c: Man fürchtete, dass er alle möglichen Werkzeuge von Admins und Sicherheitstestern erfassen würde, mit denen man auch Illegales tun kann („Dual use“). Das hätte sowohl Hersteller als auch Anwender dieser Werkzeuge kriminalisiert.

So weit kam es letztlich nicht, auch weil das Bundesverfassungsgericht zwei Jahre später klarstellte, dass es nicht reichte, wenn ein Programm „für die Begehung der genannten Computerstraftaten lediglich geeignet oder auch besonders geeignet ist.“ Es muss stattdessen mit der Absicht entwickelt worden sein, „es zur Ausspähung oder zum Abfangen von Daten einzusetzen“ und diese Absicht müsse sich „objektiv manifestiert haben“. Werkzeuge wie das vom Angeklagten eingesetzte phpMyAdmin oder den angeblich genutzten Decompiler erfasst § 202c daher nicht.

Besonders gesichert

Folgerichtig wurde der Betroffene im aktuellen Fall auch nach § 202a angeklagt. Die Kritik an diesem Paragrafen richtet sich gegen eine Einschränkung, die sich schon

© Copyright by Heise Medien.
Persönliches PDF für alle Leser der c't aus 30625 Hannover

in der Urfassung findet: Die fraglichen Daten müssen „gegen unberechtigten Zugang besonders gesichert“ sein. Aber ab wann gilt etwas als „besonders gesichert“?

Im konkreten Fall vertrat die Staatsanwaltschaft vor dem Amtsgericht Jülich die Auffassung, dass ein Passwortschutz dafür grundsätzlich ausreiche – und scheiterte damit im Mai 2023, als das Gericht den Antrag auf Erlass eines Strafbefehls ablehnte [3]. Ein Passwort bewirke nicht in jedem Fall eine effektive Datensicherung, etwa wenn es allzu simpel sei oder für bestimmte Anwendungen standardisiert verwendet werde. Das Gericht ging davon aus, dass der Angeklagte die Software dekompiliert hatte, aber wenn die „Rückübersetzung mittels gängiger Hilfsprogramme möglich“ sei, scheide eine Strafbarkeit wegen Ausspähens von Daten aus.

Damit hätte der Fall Geschichte sein können, aber die Staatsanwaltschaft legte Beschwerde beim Landgericht Aachen ein. Und das sah die Sache ganz anders [4]: „Bei einem Passwort handelt es sich um eine typische Software-Sicherung, die das Interesse an einer Zugangssicherung eindeutig dokumentiert. Maßgeblich ist, ob die Sicherung geeignet erscheint, einen wirksamen, wenn auch nicht absoluten Schutz zu erreichen.“

Nach der Gesetzesbegründung würde der Paragraf zwar nur greifen, wenn ein nicht unerheblicher zeitlicher oder technischer Aufwand erforderlich sei, um die Sicherung zu überwinden. Aber dieser Aufwand müsse nur „typischerweise“ erforderlich sein, „also unabhängig von spezifischen Möglichkeiten oder Kenntnissen des konkreten Täters“. Der Tatbestand sei daher auch dann erfüllt, wenn man eine Zugangssicherung „auf Grund besonderer Kenntnisse, Fähigkeiten oder Möglichkeiten schnell und ohne besonderen Aufwand“ überwindet, erklärte das Landgericht und verwies auf einen so argumentierenden Beschluss des Bundesgerichtshofs [5].

Mit anderen Worten: Wenn IT-Fachleute einen Schutz leicht überwinden können, heißt das noch nicht, dass Daten nicht „besonders gesichert“ sind. Mit diesen Maßgaben verwies das Landgericht die Sache zurück ans Amtsgericht Jülich, das der Auffassung nun offenbar gefolgt ist. (Die Entscheidung des Amtsgerichts vom 17. Januar 2024 war zu Redaktionsschluss noch nicht verschriftlicht.)

Paragrafenreform

Nachdem der Angeklagte in Berufung gegangen ist, geht der aktuelle Fall noch weiter, wie auch die Geschichte der Hackerparagrafen insgesamt: In der Vergangenheit standen immer wieder weitere Verschärfungen oder auch die Schaffung eines neuen §202e zu digitalem Hausfriedensbruch zur Diskussion. Zumindest der Bundesregierung gehen die bestehenden Regelungen aber offenbar eher zu weit; immerhin stellen sie ein erhebliches Risiko für jeden dar, der Sicherheitsprobleme und Datenschutzlücken entdeckt und verantwortungsvoll melden will.

Tatsächlich plant die Regierung eine Reform der §§ 202a ff., denn „das Identifizieren, Melden und Schließen von Sicherheitslücken in einem verantwortlichen Verfahren“ soll laut Koalitionsvertrag „legal durchführbar“ sein. Man habe dazu bereits zwei Symposien mit Experten durchgeführt, ein Gesetzentwurf soll in der ersten Jahreshälfte 2024 folgen. Weitere Auskünfte, insbesondere darüber, zu welchen Ergebnissen die erwähnten Symposien geführt haben, wollte das Bundesministerium der Justiz c’t nicht geben.

Einstweilen kann man IT-Profis nur raten, sich mit der Rechtslage vertraut zu machen und Nachforschungen lieber zu früh als zu spät abzubrechen, auch wenn sie einem interessanten Fehler oder einem schwerwiegenden Problem auf der Spur sind.

Im Zweifelsfall sollte man eine Lücke lieber nicht selbst melden, sondern über Dritte gehen, etwa den Chaos Computer Club unter ccc.de/disclosure oder Journalisten wie die des heise-Investigativteams (siehe Kasten). Denn Medienschaffende können und dürfen ihre Quellen schützen und geheim halten. *(syt@ct.de)* **c't**

„Hackerparagrafen“

§ 202a StGB Ausspähen von Daten:
(1) Wer unbefugt sich oder einem anderen Zugang zu Daten, die nicht für ihn bestimmt und die gegen unberechtigten Zugang besonders gesichert sind, unter Überwindung der Zugangssicherung verschafft, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.
(2) Daten im Sinne des Absatzes 1 sind nur solche, die elektronisch, magnetisch oder sonst nicht unmittelbar wahrnehmbar gespeichert sind oder übermittelt werden.

§ 202c StGB Vorbereiten des Ausspähens und Abfangens von Daten:
(1) Wer eine Straftat nach § 202a oder § 202b vorbereitet, indem er
- Passwörter oder sonstige Sicherungscodes, die den Zugang zu Daten (§ 202a Abs. 2) ermöglichen, oder
- Computerprogramme, deren Zweck die Begehung einer solchen Tat ist,

herstellt, sich oder einem anderen verschafft, verkauft, einem anderen überlässt, verbreitet oder sonst zugänglich macht, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.
(2) § 149 Abs. 2 und 3 gilt entsprechend.

heise Investigativ

Sicher melden

Wer Sicherheitslücken oder Datenlecks melden will, ohne sich selbst zu exponieren, kann sich beispielsweise ans Investigativteam von heise wenden [6]: Unter heise.de/investigativ/ betreiben wir sowohl ein einfach zu nutzendes anonymes Kontaktformular als auch einen aufwendig gesicherten Briefkasten im Tor-Netzwerk für höchste Ansprüche an Anonymität.

Journalisten haben nach § 53 StPO ein Zeugnisverweigerungsrecht und können ihre Quellen damit effektiv schützen, auch wenn möglicherweise strafbares Verhalten im Raum steht.

Literatur

[1] Fabian A. Scherschel, Datenleck: Anzeige gegen IT-Experte kam von Modern Solution: heise.de/-6254839
[2] Fabian A. Scherschel, Gericht sieht Nutzung von Klartext-Passwörtern als Hacken an: heise.de/-9601392
[3] AG Jülich, Beschluss vom 10.05.2023, Az. 17 Cs-230 Js 99/21-55/23: heise.de/s/PZOBk
[4] LG Aachen, Urteil vom 27.07.2023, Az. 60 Qs 16/23: heise.de/s/L1Z4l
[5] BGH, Beschluss vom 13.05.2020, Az. 5 StR 614/19: heise.de/s/bl2OA
[6] Holger Bleich und Sylvester Tremmel, Dateninspektoren: Das c’t-Investigativteam, c’t 12/2023, S. 86

© Copyright by Heise Medien.
Persönliches PDF für alle Leser der c't aus 30625 Hannover