§ 202a
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.

§ 202b
Abfangen von Daten

Wer unbefugt sich oder einem anderen unter Anwendung von technischen Mitteln nicht für ihn bestimmte Daten (§202a Abs. 2) aus einer nichtöffentlichen Datenübermittlung oder aus der elektromagnetischen Abstrahlung einer Datenverarbeitungsanlage verschafft, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft, wenn die Tat nicht in anderen Vorschriften mit schwererer Strafe bedroht ist.

§ 202c
Vorbereiten des Ausspähens und Abfangens von Daten

(1) Wer eine Straftat nach § 202a oder § 202b vorbereitet, indem er

1. Passwörter oder sonstige Sicherungscodes, die den Zugang zu Daten (§ 202a Abs. 2) ermöglichen, oder
2. 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.

§ 149
Vorbereitung der Fälschung von Geld und Wertzeichen

(2) Nach Absatz 1 wird nicht bestraft, wer freiwillig

1. die Ausführung der vorbereiteten Tat aufgibt und eine von ihm verursachte Gefahr, daß andere die Tat weiter vorbereiten oder sie ausführen, abwendet oder die Vollendung der Tat verhindert und
2. die Fälschungsmittel, soweit sie noch vorhanden und zur Fälschung brauchbar sind, vernichtet, unbrauchbar macht, ihr Vorhandensein einer Behörde anzeigt oder sie dort abliefert.

(3) Wird ohne Zutun des Täters die Gefahr, daß andere die Tat weiter vorbereiten oder sie ausführen, abgewendet oder die Vollendung der Tat verhindert, so genügt an Stelle der Voraussetzungen des Absatzes 2 Nr. 1 das freiwillige und ernsthafte Bemühen des Täters, dieses Ziel zu erreichen.

Was ist der Hackerparagraph?

Den allzu berüchtigten Hackerparagraph findet man im Strafgesetzbuch des deutschen Rechts. Genauer gesagt ist damit oft der Paragraph $202c gemeint, welcher den Titel "Vorbereiten des Ausspähens und Abfangens von Daten" trägt. In diesem steht geschrieben:

> (1) Wer eine Straftat nach § 202a oder § 202b vorbereitet, indem er
>
> 1. Passwörter oder sonstige Sicherungscodes, die den Zugang zu Daten (§ 202a Abs. 2) ermöglichen, oder
> 2. 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 einem Jahr oder mit Geldstrafe bestraft.
>
> (2) § 149 Abs. 2 und 3 gilt entsprechend.

Was steht in Paragraph §202a bzw. $202b geschrieben?

Paragraph $202a lautet folgendermaßen:

> (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.

Wie man Punkt (1) entnehmen kann, ist es verboten sich Zugang zu Inhalten zu verschaffen, welche normalerweise nicht für einen bestimmt wären. Wenn man dies überträgt, macht man sich strafbar, wenn man über SQL Injection auf die Daten einer Datenbank zugreift, denn man könnte bzw. man sieht Daten welche nicht für einen bestimmt wären (z.B. Tabellennamen, Nutzerdaten, etc). Nun könnte man sich ausreden, die "Zugangssicherung" sei der Benutzerlogin, und diesen hätte man ja nicht überwunden. Wenn man aber etwas weiter denkt, dann hat man durch die manipulierten Abfragen auf einer bestimmten Seite sich Daten beschafft, in dem man den Login nicht nutzte, welche man nutzen müsste. Somit ist dies trotzdem eine Straftat.

Ebenfalls zählen hier solche Machenschaften, wie Stealer/Rats-Spreading, etc rein, denn dies ist nichts anderes als sich Zugang zu Daten zu beschaffen, in dem man das Opfer infiziert, und danach dessen Passwörter ausspäht bzw. seine Laufwerke durchsuchen kann.

Der Absatz (2) grenzt den Begriff der "Daten" ein, in dem es diese als elektronisch, magnetisch festschreibt, somit auf den Computer fixiert. Wer also über einen Stealer oder ein Rat, falls diese nicht

zufällig dabei einen Ordnernamen liest, oder irgendwelche anderen Benutzerdaten mitbekommt, den Zahlencode für das Fahrradschloss seines Nachbarn herausfindet, würde nicht über den Hackerparagraph anzeigbar sein.

Paragraph $202b (Abfangen von Daten) lautet folgendermaßen:

> Wer unbefugt sich oder einem anderen unter Anwendung von technischen Mitteln nicht für ihn bestimmte Daten (§202a Abs. 2) aus einer nichtöffentlichen Datenübermittlung oder aus der elektromagnetischen Abstrahlung einer Datenverarbeitungsanlage verschafft, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft, wenn die Tat nicht in anderen Vorschriften mit schwererer Strafe bedroht ist.

Wieder geht es um Daten, die nicht für einen bestimmt sind, welche jedoch über andere Datenwege besorgt werden können. Unter "nichtöffentliche Datenübermittlung" verstehe ~~ch offene WLAN-Netze~~, das Radio, etc auf diese man ohne weitere technische Mittel zugreifen kann, und sich dabei nicht strafbar macht. Strafbar hingegen ist das "Knacken" von verschlüsselten WLAN- Netzen, welche über eine WEP bzw. WPA(2)-Verschlüsselung besitzen.

Wenn man das zweite Satzteil nochmal genau liest, dann könnte man einen WLAN-Router, welcher ein offenes WLAN-Netz betreibt, als eine Datenverarbeitungsanlage bezeichnen kann, da es die Daten zwischen den Computern und den Servern regelt, dann ist das Surfen in einem solchen Netz auch nicht legal.

Das deutsche Recht ist doch so toll.

Wenn man den Paragraphen noch zum dritten Mal liest, dann fällt auf, das lediglich die Beschaffung von nicht bestimmten Daten in solchen Netzen illegal sei. Dies würde wiederum bedeuten, das wenn man in solchen Netzen surft (zumindest offenes WLAN, da man bei WEP/WPA wieder eine Zugangssicherung überschreitet, und danach laut $202a sich strafbar macht), sich nicht strafbar macht, so lange man nicht zufällig auf Daten dritter stößt, welche nicht für einen bestimmt sind.

Was verbietet nun der Hackerparagraph?

Wer schon wieder vergessen hat, wie dieser lautete, darf nochmal hoch scrollen.

Dort steht nun zusammenfassend geschrieben, das wenn man Software herstellt, vertreibt, nutzt, etc. welche eine o.g. Straftat ermöglich kann, sich damit selbst strafbar macht.

Diese Regelung war zur Einführung sehr diskutiert, da Sicherheitsexperten bzw. WhiteHat-Hacker diese Dual-Use-Tools benutzen durften, um Schwachstellen in einem Computer aufzufinden, und sie diese ggf. zu beheben.

Kurz darauf, gab es eine kleine Revision, welche besagte, das diese Tools eingesetzt werden dürfen, wenn man eine ausdrückliche Erlaubnis des Eigentümers besitzt oder das Programm nicht nur darauf ausgelegt ist, Schaden anzurichten.

Was erlaubt der Hackerparagraph?

Absatz (2) des $202c besagt folgendes:

> (2) Nach Absatz 1 wird nicht bestraft, wer freiwillig
>
> 1. die Ausführung der vorbereiteten Tat aufgibt und eine von ihm verursachte Gefahr, daß andere die Tat weiter vorbereiten oder sie ausführen, abwendet oder die Vollendung der Tat verhindert und
> 2. die Fälschungsmittel, soweit sie noch vorhanden und zur Fälschung brauchbar sind, vernichtet, unbrauchbar macht, ihr Vorhandensein einer Behörde anzeigt oder sie dort abliefert.
>
> (3) Wird ohne Zutun des Täters die Gefahr, daß andere die Tat weiter vorbereiten oder sie ausführen, abgewendet oder die Vollendung der Tat verhindert, so genügt an Stelle der Voraussetzungen des Absatzes 2 Nr. 1 das freiwillige und ernsthafte Bemühen des Täters, dieses Ziel zu erreichen.

Wer also eine Tat anfängt diese aber nicht zu Ende durchführt, was auch immer als "Ende" definiert werden mag, oder diese Durchführung durch andere verhindert, macht sich nicht strafbar. Falls dieser mögliche Beweismittel den Behörden vorzeigt oder Mittel, welche diese Beweise fälschen könnten vernichtet, macht sich nicht strafbar.

Beim Schreiben des letzten Satz kam mir ein genialer Gedanke. Wenn ich über ein VPN-Server surfe, verberge ich als Angreifer nun meine IP-Adresse, welche ein Beweis sein könnte, und dadurch verfälscht wird. Als sicherheitsbewusster IT-Nutzer darf ich nun also Ausschau nach solchen Servern halten und diese, z.B. mit einer Bombe vernichten.

Das grenzt etwas an Spinnerei, deswegen diese Idee einfach nicht weiter beachten, bzw. ignorieren, denn die Beschädigung von Sachgegenständen von anderen Personen wird bestimmt in einem weiteren Gesetzestext geregelt.

Ich hoffe, ich konnte etwas Klarheit in die ganze Sache bringen, ansonsten müsst ihr euren Rechtsanwalt fragen, denn Jurist werde ich auf alle Fälle nicht werden.

Links

https://www.telemedicus.info/article/1130-Das-Computerstrafrecht-und-die-Forschung.html

http://www.golem.de/0807/61198.html

ZIMK-Nutzerordnung:
https://www.uni-trier.de/index.php?id=6397

Informatik-Nutzerordnung:
http://cip.uni-trier.de/?id=0.1