Ein Überblick über deutsches Hackerstrafrecht

§202c Any% Speedrun

> Machst du Hacki, wirst du Knacki

CTFs bedeuten Hacking im kontrollierten Umfeld.

> Machst du Hacki, wirst du Knacki

CTFs bedeuten Hacking im kontrollierten Umfeld.

Hacking mit Einverständnis.

> Machst du Hacki, wirst du Knacki

CTFs bedeuten Hacking im kontrollierten Umfeld.

Hacking mit Einverständnis.

Wir lernen hier Skills, die ggf. anderswo auch dazu verwendet werden können um Straftaten zu begehen.

> Machst du Hacki, wirst du Knacki

CTFs bedeuten Hacking im kontrollierten Umfeld.

Hacking mit Einverständnis.

Wir lernen hier Skills, die ggf. anderswo auch dazu verwendet werden können um Straftaten zu begehen.

Zeit für etwas Aufklärung!

Disclaimer: Ich weiß nichts über Jura. Ich kann nur lesen.

> Vergangene Fälle

Name	Gericht & Jahr	Alter	§	Strafe
"Mixter"	LG Hannover, 2000	Jugendl.	§303b	6 Mon. Jugendstrafe, Bew.
ZZb00t / Maik D.	Bielefeld, 2019	24	§303b, +	1 J. 10 Mon., Bewährung
Schüler, Niederbayern	Jugendgericht, 2019	minderjährig	§202a	nicht öffentlich
IT-Experte (Mod. Sol.)	AG Jülich / LG Aachen, 2024	Erwachsen	§202a	Geldstrafe 3.000 €

IT-Experte / Modern Solution (2024)

Findet Klartext-Passwort in kompilierter Software. Greift auf DB mit 700k Kundendaten zu. Meldet Lücke per Responsible Disclosure. **Ergebnis: Geldstrafe wegen §202a.** Verfassungsbeschwerde läuft.

Schüler, Niederbayern (2019)

Gymnasiasten verschaffen sich Admin-Zugang zum Schulnetz per BeRoot. Erbeuten Passwörter und Dateien. **Informieren danach selbst den Sysadmin** über die Lücke. Trotzdem angeklagt.

> Background: Sicherheitsziele

C

Confidentiality

Vertraulichkeit

I

Integrity

Integrität

A

Availability

Verfügbarkeit

> §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.

> §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.

C I A

> §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.

> §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.

C I A

> §202c Vorbereiten…

(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.

> §202c Vorbereiten…

(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.

C I A

…und noch mehr?

> Einschub: §149


```
# Rücktrittsklausel — gilt via §202c Abs. 2 auch für Hackerwerkzeuge
```

> §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.

> §202d Datenhehlerei

(1) Wer Daten (§202a Absatz 2), die **nicht allgemein zugänglich** sind und die **ein anderer** durch eine **rechtswidrige Tat** erlangt hat, sich oder einem anderen verschafft, einem anderen überlässt, **verbreitet** oder sonst zugänglich macht, **um sich oder einen Dritten zu bereichern** oder einen anderen **zu schädigen**, wird mit Freiheitsstrafe **bis zu drei Jahren oder mit Geldstrafe** bestraft.

(2) Die Strafe darf nicht schwerer sein als die für die Vortat angedrohte Strafe.

> §202d Datenhehlerei

(1) Wer Daten (§202a Absatz 2), die **nicht allgemein zugänglich** sind und die **ein anderer** durch eine **rechtswidrige Tat** erlangt hat, sich oder einem anderen verschafft, einem anderen überlässt, **verbreitet** oder sonst zugänglich macht, **um sich oder einen Dritten zu bereichern** oder einen anderen **zu schädigen**, wird mit Freiheitsstrafe **bis zu drei Jahren oder mit Geldstrafe** bestraft.

(2) Die Strafe darf nicht schwerer sein als die für die Vortat angedrohte Strafe.

C I A

> §202d Datenhehlerei (Fortsetzung)

(3) Absatz 1 gilt nicht für Handlungen, die ausschließlich der Erfüllung **rechtmäßiger dienstlicher oder beruflicher Pflichten** dienen. Dazu gehören insbesondere

1. solche Handlungen von Amtsträgern oder deren Beauftragten, mit denen Daten ausschließlich der Verwertung in einem Besteuerungsverfahren, einem Strafverfahren oder einem Ordnungswidrigkeitenverfahren zugeführt werden sollen, sowie
2. solche beruflichen Handlungen der in §53 Absatz 1 Satz 1 Nummer 5 der Strafprozessordnung genannten Personen, mit denen Daten entgegengenommen, ausgewertet oder veröffentlicht werden.

> §303a Datenveränderung

(1) Wer **rechtswidrig** Daten (§202a Abs. 2) **löscht, unterdrückt, unbrauchbar macht oder verändert**, wird mit Freiheitsstrafe **bis zu zwei Jahren oder mit Geldstrafe** bestraft. (2) Der **Versuch** ist strafbar. (3) Für die **Vorbereitung** einer Straftat nach Absatz 1 gilt **§202c** entsprechend.

> §303a Datenveränderung

(1) Wer **rechtswidrig** Daten (§202a Abs. 2) **löscht, unterdrückt, unbrauchbar macht oder verändert**, wird mit Freiheitsstrafe **bis zu zwei Jahren oder mit Geldstrafe** bestraft. (2) Der **Versuch** ist strafbar. (3) Für die **Vorbereitung** einer Straftat nach Absatz 1 gilt **§202c** entsprechend.

C **I** **A**

> §303b Computersabotage

(1) Wer eine **Datenverarbeitung**, die für einen anderen von **wesentlicher Bedeutung** ist, dadurch **erheblich stört**, dass er

1. eine Tat nach **§303a** Abs. 1 begeht,
2. Daten (§202a Abs. 2) in der **Absicht**, einem anderen **Nachteil zuzufügen**, **eingibt oder übermittelt** oder
3. eine Datenverarbeitungsanlage oder einen **Datenträger zerstört, beschädigt, unbrauchbar macht, beseitigt oder verändert**,

wird mit Freiheitsstrafe **bis zu drei Jahren oder mit Geldstrafe** bestraft.

> §303b Computersabotage (Fortsetzung)

(2) Handelt es sich um eine Datenverarbeitung, die für einen **fremden Betrieb, ein fremdes Unternehmen oder eine Behörde von wesentlicher Bedeutung** ist, ist die Strafe Freiheitsstrafe bis zu **fünf Jahren** oder Geldstrafe.

(3) Der **Versuch** ist strafbar.

(4) In besonders **schweren Fällen** des Absatzes 2 ist die Strafe Freiheitsstrafe **von sechs Monaten** bis zu **zehn Jahren**. Ein besonders schwerer Fall liegt in der Regel vor, wenn der Täter

1. einen **Vermögensverlust großen Ausmaßes** herbeiführt,
2. **gewerbsmäßig** oder als **Mitglied einer Bande** handelt, die sich zur fortgesetzten Begehung von Computersabotage verbunden hat,
3. durch die Tat die Versorgung der Bevölkerung mit **lebenswichtigen Gütern oder Dienstleistungen** oder die **Sicherheit der Bundesrepublik Deutschland** beeinträchtigt.

(5) Für die Vorbereitung einer Straftat nach Absatz 1 gilt **§202c** entsprechend.

> §303b Computersabotage (Fortsetzung)

(2) Handelt es sich um eine Datenverarbeitung, die für einen **fremden Betrieb, ein fremdes Unternehmen oder eine Behörde von wesentlicher Bedeutung** ist, ist die Strafe Freiheitsstrafe bis zu **fünf Jahren** oder Geldstrafe.

(3) Der **Versuch** ist strafbar.

(4) In besonders **schweren Fällen** des Absatzes 2 ist die Strafe Freiheitsstrafe **von sechs Monaten** bis zu **zehn Jahren**. Ein besonders schwerer Fall liegt in der Regel vor, wenn der Täter

1. einen **Vermögensverlust großen Ausmaßes** herbeiführt,
2. **gewerbsmäßig** oder als **Mitglied einer Bande** handelt, die sich zur fortgesetzten Begehung von Computersabotage verbunden hat,
3. durch die Tat die Versorgung der Bevölkerung mit **lebenswichtigen Gütern oder Dienstleistungen** oder die **Sicherheit der Bundesrepublik Deutschland** beeinträchtigt.

(5) Für die Vorbereitung einer Straftat nach Absatz 1 gilt **§202c** entsprechend.

C I A

Fallbeispiele / Diskussion

> CTF-Wettbewerb

Alice nimmt an einem online CTF der Uni teil. Die Challenges laufen auf dedizierten Servern des Veranstalters – extra für den Wettbewerb aufgesetzt. Um eine Flag zu bekommen, muss sie eine bekannte Buffer-Overflow-Schwachstelle ausnutzen, sich Root-Zugang verschaffen und eine Datei aus `/root/` auslesen.

Hat Alice etwas Strafbares getan?

> Default-Credentials

Bob konfiguriert bei einem neuen Job die Firmen-Infrastruktur und stößt dabei auf ein altes NAS, das noch im Netz hängt. Neugierig ruft er die Web-UI auf — und probiert aus einer Laune heraus `admin` / `admin`. Er ist sofort drin. Er sieht Backups, Zugangsdaten, interne Dokumente. Er loggt sich wieder aus und sagt niemandem etwas.

Hat Bob sich unbefugt Zugang verschafft, oder war das System gar nicht geschützt?

> Port-Scan

Charlie schreibt seine Bachelorarbeit über Angriffsflächen im Heimnetz und scannt dafür mit Nmap eine /24-Range seines Wohnheim-Netzwerks. Er versucht nicht, sich irgendwo einzuloggen — er will nur wissen, welche Geräte und Dienste sichtbar sind.

Hat Charlie auf etwas zugegriffen, oder nur geschaut?

> Responsible Disclosure

Diana verwendet eine Fitness-App und bemerkt, dass die API-Anfragen in den Dev-Tools seltsam aussehen. Sie probiert einen Endpunkt ohne Auth-Token aus — und bekommt die kompletten Profildaten eines fremden Nutzers zurück. Sie ruft den Endpunkt einmal mit einer zufälligen User-ID auf, macht einen Screenshot als Beweis, und schreibt dann eine E-Mail an den Support.

Hat Diana eine Grenze überschritten? Ändert ihre Meldung an das Unternehmen etwas daran?

> Freund-Pentest

Jonas hat einen Webshop für handgemachte Keramik gebaut und bittet seinen Kumpel Erik beim nächsten Treffen: **“Guck mal ob du da irgendwas findest, ich will das sicher haben.”** Eine Woche später findet Erik eine SQL-Injection im Suchfeld und zieht damit zur Demo die komplette Kundentabelle — Namen, Adressen, Bestellhistorie.

Hat Jonas Erik ausreichend autorisiert? Gilt das auch für die Kundendaten?

> DDoS als Protest

Ein Konzern wird beschuldigt, Nutzerdaten illegal weiterzuverkaufen. Eine Telegram-Gruppe organisiert eine koordinierte Aktion: alle starten gleichzeitig ein einfaches Script, das in einer Schleife HTTP-Anfragen an die Firmen-Website schickt. Franziska macht mit — das Script läuft zwei Stunden auf ihrem Laptop.

Hat Franziska etwas Strafbares getan? Spielt ihre Motivation eine Rolle?

> Datenleck herunterladen

Eine bekannte Gaming-Plattform wurde gehackt. Im einschlägigen Forum kursiert ein 2 GB Dump: Nutzernamen, E-Mail-Adressen, gesalzene Passwort-Hashes. Gregor hat dort einen Account und lädt den Dump herunter, um zu prüfen ob seine Daten dabei sind.

Hat Gregor etwas Strafbares getan, obwohl er nur seine eigenen Daten suchen wollte?

> Hacking-Tool veröffentlichen

Hannah schreibt im Rahmen eines IT-Security-Seminars ein Python-Script, das automatisiert Passwörter gegen einen SSH-Login ausprobiert — als Demonstration wie Brute-Force-Angriffe funktionieren. Sie veröffentlicht das Script mit einer kurzen README auf ihrem GitHub-Profil.

Hat Hannah sich strafbar gemacht? Kommt es auf den Zweck oder die Funktion des Scripts an?

> Hack-Back

Idas Laptop wurde mit einem Infostealer kompromittiert. Sie analysiert die Malware, findet die hartcodierte IP des C2-Servers, und stellt fest: der Server ist noch aktiv und schlecht gesichert. Sie verschafft sich Zugang, findet ein Verzeichnis mit gestohlenen Daten von vielen Opfern – darunter ihre eigenen – und löscht alles.

Gegen welche Paragraphen könnte Ida verstoßen haben?

> Bluetooth-Jamming

Jakobs Nachbar feiert jeden Freitagabend lautstark mit einem Bluetooth-Lautsprecher. Nach dem dritten erfolglosen Gespräch bastelt Jakob aus einem Raspberry Pi Zero und einer billigen Antenne einen Bluetooth-Jammer, der gezielt die 2,4-GHz-Frequenz des Lautsprechers flutet. Freitagabends läuft das Ding einfach durch.

Hat Jakob etwas Strafbares getan, und wenn ja womit?