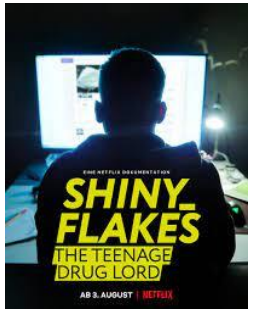
IT-Sicherheit
WiSe 2021/22

Übungsvorbereitung: Ethik und Recht

Nicht Klausurrelevant

Motivation

- Einstieg in die Kriminalität beginnt häufig klein
  - Am Anfang Interesse an Technik und Suche nach Herausforderung
  - Kleine Gesetzesübertretungen werden nicht bemerkt oder bestraft
  - Hemmschwelle für Gesetzesübertretungen wird langsam verschoben



- In dieser LVA behandeln wir Techniken, die zu illegalen und unethischen Zwecken genutzt werden können
  - Gefahr der Trivialisierung von Angriffen

- Große rechtliche Grauzonen im Bereich IT-Sicherheit
  - Ethisch korrektes Verhalten kann strafrechtlich verfolgt werden

Lernziele

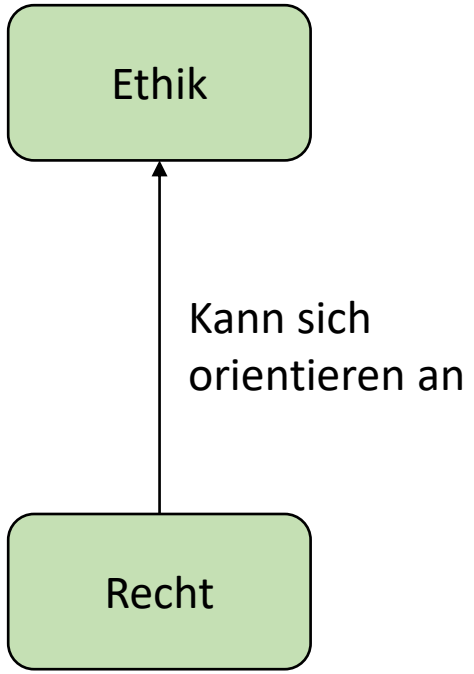
- Diese Lerneinheit soll ein Verständnis schaffen für die Grenzen beim Durchführen von Sicherheitstests zwischen:
  - Ethisch vertretbarem vs. nicht vertretbarem Verhalten
  - Rechtlich legalem vs. illegalem Verhalten

- Es sollen ein Bewusstsein für Gefahren beim Durchführen von Sicherheitstests geschaffen werden

- Die Bonuspunkte aus den Übungen sind gekoppelt an ein erfolgreiches Bestehen des Moodle Tests im Anschluss an die Übung

Definition Ethik und Recht

- **Ethik** beschäftigt sich mit der Frage nach dem „rechten“ menschlichen Handeln.
- **Recht** ist die menschliche Instanz um das Miteinander zu beeinflussen. Recht **kann** sich an der Ethik orientieren.
- Allerdings sind beide nicht deckungsgleich:
  - Ethisch korrektes Handeln wird nicht immer vom Recht geschützt. Beispiele: ....
  - Ethisch korrektes Handeln wird manchmal sogar vom Recht bestraft. Beispiele: ….



Personenbezogene Daten

Der Begriff personenbezogene Daten bezeichnet „…alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann“ [DSGVO]

- Weitere Beispiele für personenbezogene Daten?

IP, Name Vorname, Kombination von Daten, Bilder,

Hacker*innen Ethik [CCC_Ethik]

Ethik Richtlinien des CCC:

1. Der Zugang zu Computern und allem, was einem zeigen kann, wie diese Welt funktioniert, sollte unbegrenzt und vollständig sein.
2. Alle Informationen müssen frei sein.
3. Mißtraue Autoritäten – fördere Dezentralisierung.
4. Beurteile einen Hacker nach dem, was er tut, und nicht nach üblichen Kriterien wie Aussehen, Alter, Herkunft, Spezies, Geschlecht oder gesellschaftliche Stellung.
5. Man kann mit einem Computer Kunst und Schönheit schaffen.
6. Computer können dein Leben zum Besseren verändern.
7. **Mülle nicht in den Daten anderer Leute.**
8. **Öffentliche Daten nützen, private Daten schützen.**

Google map, map öffentlich,
aber directions private

Ethische Grundsätze für Sicherheitstests [Z. ECC]

- Bewahren Sie die Privatheit und Geheimhaltung von Informationen, die Sie während Ihrer Sicherheitstests erhalten haben
- Geben Sie potentielle Gefahren an die relevanten Interessensgruppen weiter
- Nutzen Sie keine Software oder Vorgehen, die als illegal oder unethisch gelten
- Stellen Sie sicher, dass Ihre Sicherheitstests gut gemanaged werden
- Fördern Sie keine kriminellen Aktivitäten
- Beachten Sie die Gesetze des jeweiligen Landes

Die CDUconnect App [CDU]

Hochschule Fulda
University of Applied Sciences

1. Die CDUconnect App erfasst Daten von politischen Haustürgesprächen

2. Aufgrund von Zweifeln am Datenschutz analysiert eine IT-Sicherheitsforscherin die App
   - Sie erhält Zugriff auf private Daten : Adresse, Alter, Geschlecht, …
   - Sie informiert die zuständigen Stellen (BSI, CERT, Datenschutzbeauftragte und CDU)

3. Die CDU nimmt die App offline und informiert die Betroffenen

4. Die Forscherin veröffentlicht einen Tag später Details zur Sicherheitslücke
   - Später findet Sie die gleiche Sicherheitslücke auch in den Apps der CSU und ÖVP

5. Die Datenschutzbeauftragte eröffnet ein Prüfverfahren gegen CDUconnect

6. Die Forscherin erhält die Information, dass Anzeige gegen sie erstattet wurde


```
{
    "age": 50,
    "campaignId": 38,
    "city": "Hameln",
    "createdAt": "2021-01-15 14:19:51",
    "doorOpened": 1,
    "gender": "male",
    "id": 859957,
    "isReplica": 0,
    "latitude": 52.125612,
    "locationId": 1734,
    "longitude": 9.3481377,
    "opinion": 3,
    "similarAddresses": 1,
    "street": "Froschk\u00f6nigweg",
    "teamId": null,
    "topics": "Bundesparteitag 2021",
    "updatedAt": "2021-01-15 14:20:32",
    "userId": 12984,
    "validSurveyTime": 1,
    "zip": "31787"
},
```


Beispiele zu privaten Daten [CDU]

7. Die Anzeige gegen die Forscherin wurde eingestellt. Das Prüfverfahren gegen CDUconnect läuft weiterhin

Deutsche Gesetze im Bereich Computerkriminalität

- Gesetze im Strafgesetzbuch
  - §202a: Ausspähen von Daten
  - §202b: Abfangen von Daten
  - §202c: Vorbereiten des Ausspähens und Abfangens von Daten
  - §202d: Datenhehlerei
  - §303a: Datenveränderung
  - §303b: Computersabotage
  - §263a: Computerbetrug

- Wichtig: Keine rechtliche Kompetenz, nur offene Diskussion

§ 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.

§ 202b StGB: Abfangen von Daten

(1) 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 StGB: Vorbereiten des Ausspähens und Abfangens von Daten (Hacker*innenparagraph) [REIS]

Hochschule Fulda
University of Applied Sciences

(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. (Regelungen zu Straflosigkeit durch Rücktritt und zur Verhinderung sowie ernsthafte Verhinderung bei passiver Teilnahme als straffrei)

- §202c sorgt für viel Unsicherheit in der IT-Sicherheitsszene
- Computerprogramme sind nicht inhärent gut oder böse, da sie für beides genutzt werden können
- Reaktion auf Anfrage bei Einführung: Gutwilliger Umgang mit solchen Programmen wird nicht von §202c erfasst
- Mehrere Selbstanzeigen bei Einführung wurden abgelehnt
- Weitere Unsicherheiten bestehen allerdings:
  - Wo ist die Grenze für Herstellung und Verbreitung der Programme?

§ 202d StGB: 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.

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

§ 303a StGB: Verändern von Daten

*(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.

§ 303b StGB: 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 Datenverarbeitungnsanlage oder einen Datenträger zerstört, beschädigt, unbrauchbar macht, beseitigt oder verändert,

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

*(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.

§ 263a StGB: Computerbetrug

Hochschule Fulda
University of Applied Sciences

*(1) Wer in der Absicht, sich oder einem Dritten einen **rechtswidrigen Vermögensvorteil zu verschaffen**, das Vermögen eines anderen dadurch beschädigt, daß er **das Ergebnis eines Datenverarbeitungsvorgangs durch unrichtige Gestaltung des Programms, durch Verwendung unrichtiger oder unvollständiger Daten, durch unbefugte Verwendung von Daten oder sonst durch unbefugte Einwirkung auf den Ablauf beeinflußt**, wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft.*

(2) § 263 Abs. 2 bis 6 gilt entsprechend.

(3) Wer eine Straftat nach Absatz 1 vorbereitet, indem er

1. *Computerprogramme, deren Zweck die Begehung einer solchen Tat ist, herstellt, sich oder einem anderen verschafft, feilhält, verwahrt oder einem anderen überlässt oder*
2. *Passwörter oder sonstige Sicherungscodes, die zur Begehung einer solchen Tat geeignet sind, herstellt, sich oder einem anderen verschafft, feilhält, verwahrt oder einem anderen überlässt,*

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

(4) In den Fällen des Absatzes 3 gilt § 149 Abs. 2 und 3 entsprechend.

Beispielanalyse Phishing [PHI]

- Phishing wird in verschiedene Phasen unterteilt

1. **Versenden der Phishing eMail:** Strafhandlung nach §202c, Absatz 1, Nr. 1 – da Täter*in auf PIN und TAN abzielt. Falls das Opfer nicht reagiert, bleibt §202c aus.

2. **Erstellen einer gefälschten Webseite:** Kein Betrug. Höchstens Kennzeichenverletzung bei Verwendung geschützten Designs.

3. **Kontodiebstahl mit erlangten Informationen:** Strafhandlung nach §263a, Absatz 1 und §202a.

Beispiel Ransomware [RAN]

1. **Infektion mit Ransomware und Sperrbildschirm**: Straftat nach §303b Absatz 1 Nr. 1

2. **Ändern der Windows Registry Einträge zur Beibehaltung des Sperrbildschirms:** Straftat nach §303b Absatz 1 Nr. 1

3. **Sperrbildschirm nicht umgehbar**: §303a Absatz 1

- Angeklagter hatte Ransomwaregruppe als IT-Administrator unterstützt und daher auf Beihilfe angeklagt.

Verurteilungszahlen Deutschland

Straftat	2011	2012	2013	2014	2015	2016	2017	2018	2019
§202a: Ausspähen von Daten	80	73	64	84	70	48	64	59	53
§202b: Abfangen von Daten	1	5	3	1	2	4	1	1	3
§202c: Vorbereiten des Ausspähens oder Abfangens	2	2	1	4	9	12	11	5	3
§202d: Datenhehlerei	-	-	-	-	-	-	2	3	2
§303a: Verändern von Daten	50	59	53	46	64	56	56	57	60
§303b: Computersabotage	18	28	26	22	26	21	16	18	49
§263a: Computerbetrug	3439	3393	3252	3241	3203	3195	3126	2996	3156

https://www.destatis.de/DE/Themen/Staat/Justiz-Rechtspflege/Publikationen/Downloads-Strafverfolgung-Strafvollzug/strafverfolgung-2100300197004.html

Rechtliche Abdeckung von Sicherheitstests

- In Deutschland sind Sicherheitstests ohne vorherigen Vertrag nicht rechtlich abgedeckt
  - Abläufe beruhen auf „Gentleman/woman‘s Agreement“
  - Ethische Hacker*innen sind bei Ausnutzung nicht von Kriminellen unterscheidbar
- Betreiber*in kann Anzeige bei Entdeckung, Meldung oder Veröffentlichung erstatten
  - Erfolg hängt davon ab, ob ein Nachweis auf Gesetzesverletzung erbracht werden kann
  - Fall CDUconnect: §202a wurde nicht verletzt, da CDUconnect keine Sicherheitsmechanismen hatte
  - Liste von Fällen mit strafrechtlichen Konsequenzen: [Threat]
- Unternehmen nutzen die „Disclosure Policy“ um freiwillig einen rechtlichen Rahmen zu schaffen
  - Der rechtliche Rahmen deckt allerdings nicht alle Handlungen ab!
- Vor einem Sicherheitstests [OWASP]:
  - Stellen Sie sicher, dass Ihre Sicherheitstests vom Unternehmen autorisiert wurden und legal sind
  - Suchen Sie bei Grauzonen rechtlichen Beistand oder den CCC

Möglichkeiten zur Offenlegung (Disclosure)

- Verschiedene Möglichkeiten zur Handhabung von Schwachstellen:
  - **Non Disclosure:** Informationen zur Schwachstelle werden nicht veröffentlicht
  - **Responsible Disclosure:** Dem Unternehmen wird Zeit gegeben um die Schwachstelle zu beheben bevor Informationen veröffentlicht werden
  - **Full Disclosure:** Informationen zur Schwachstelle werden veröffentlicht bevor sie behoben ist
- Responsible Disclosure ist oft der ethisch vertretbarste Weg
  - **Non Disclosure:** Schwachstelle wird evtl. aufgrund fehlenden Drucks nicht gebehoben
  - **Full Disclosure:** Sensible und evtl. personenbezogene Daten werden gefährdet
- Full Disclosure als letztes Mittel wenn eine Schwachstelle nicht behoben wird

LVA IT-Sicherheit Disclosure Policy

- Bei Meldung von Schwachstellen im Übungssetting:
  - Analyse und, bei Bedarf, Behebung der Schwachstelle
  - Bei Anerkennung: Aushändigung einer Packung Schokolade oder Club Mate
  - Falls gewünscht einen Eintrag in der Moodle HallOfFame zu verfassen

- Rahmenbedingung:
  - Schwachstelle wird nicht ausgenutzt um Bonuspunkte zu erschleichen
  - Es werden keine personenbezogenen Daten weitergegeben

- Außerhalb der LVA ist die Sicherheitsrichtlinie der HS Fulda zu beachten: https://www2.hs-fulda.de/it-sicherheit/

Zusammenfassung

- **Ethik:** „Handle nur nach derjenigen Maxime, durch die du zugleich wollen kannst, daß sie ein allgemeines Gesetz werde.“ Immanuel Kant.
- **Recht:** Zu beachten sind §202a-d, §263a und §303a-b
- Ethik und Recht sind **nicht deckungsgleich** und stehen manchmal im **Widerspruch**
- Beim Durchführen von Sicherheitstests:
  - Halten Sie sich an **ethische Richtlinien**
  - Vermeiden Sie zum Eigenschutz **Gesetzesübertretungen**
  - Suchen Sie sich rechtlichen Beistand, falls Sie Gesetzesübertretungen nicht vermeiden können
- Falls möglich, melden Sie Sicherheitslücken via **Responsible Disclosure**

Referenzen

- [CDU]: Lilith Wittmann: https://www.heise.de/news/Luecken-in-der-connect-App-Wenn-eine-Hackerin-bei-der-CDU-anruft-6156624.html. https://www.heise.de/news/Verfahren-gegen-Lilith-Wittmann-eingestellt-weil-CDU-connect-ungeschuetzt-war-6194222.html
- [IT-Sec2.0]: https://netzpolitik.org/2020/eine-vertane-chance-fuer-die-it-sicherheit-in-deutschland/
- [202c]: https://media.ccc.de/v/36c3-10977-hackerparagraph_202c_stgb_reality_check
- [CCC_Ethik]: https://www.ccc.de/de/hackerethik
- [PHI]: Analyse der Strafbarkeit von Phishing: https://rsw.beck.de/cms/?toc=mmr.120&docid=304689
- [RAN]: Urteil zum Einsatz von Ransomware: https://www.hrr-strafrecht.de/hrr/1/21/1-78-21.php?referer=db
- [REIS]: https://www.nm.ifi.lmu.de/teaching/Vorlesungen/2016ws/itsec/_skript/itsec-k5-v12.0.pdf
- [OWASP]: https://cheatsheetseries.owasp.org/cheatsheets/Vulnerability_Disclosure_Cheat_Sheet.html
- [ECC]: https://www.eccouncil.org/code-of-ethics/
- [Threat]: https://github.com/disclose/research-threats
- [DSGVO]: https://dsgvo-gesetz.de/themen/personenbezogene-daten/