HACKERPRAKTIKUM
PART I: RECHTLICHE GRUNDLAGEN

Lukas Jung, Marc Narres-Schulz, Oliver Sänger, Tobias Zeimetz

Aufgabe 1

- Welche Gesetze befassen sich mit dem Thema?
- Welche strafrechtlichen Vorschriften gibt es?
- Gibt es besondere Bedingungen, die auf die Universität zutreffen?
- Welche Bedingungen stellt die Universität selbst?

Welche Gesetze es gibt

Aufteilung in Ebenen

- EU-Gesetze
- Deutschlandweite Gesetze
- Hochschulgesetze

Welche Gesetze es gibt

EU-Ebene

- Grundrechtecharta
- Allgemein gehalten
- Recht auf Schutz personenbezogener Daten
- Einwilligung von Personen ist zwingend notwendig
- Einhaltung der Vorschriften durch unabhängige Stellen

Welche Gesetze es gibt

Gesetze in Deutschland

- Bundesdatenschutzgesetz (BDSG)
- Gesetz über den Schutz von zugangskontrollierten Diensten und von Zugangskontrolldiensten (ZKDSG)

Welche Gesetze es gibt

Bundesdatenschutzgesetz (BDSG)

- Allgemeine und gemeinsame Bestimmungen
- Datenverarbeitung für öffentliche Stellen
- Datenverarbeitung für private Stellen
- Straf- und Bußgeldvorschriften
- Sondervorschriften & Übergangsvorschriften

Welche Gesetze es gibt

Das ZKDSG

- Rechtlicher Schutz gegen unerlaubte Eingriffe
- Zugangskontrollierte Dienste
  - Rundfunkarbeiten, Teledienste, Mediendienste
- Zugangskontrolldienste
  - Technische Verfahren oder Vorrichtungen, gegen unerblaubte Nutzung

Strafrechtliche Vorschriften

Geregelt im Strafgesetzbuch (StGB)

- §202 Verletzung des Briefgeheimnisses
- §202a Ausspähen von Daten
- §202b Abfangen von Daten
- §202c Vorbereiten des Ausspähen und Abfangen von Daten in Verbindung mit §149 Wertzeichenfälschung
- §202d Datenhehlerei

Strafrechtliche Vorschriften

Geregelt im Strafgesetzbuch (StGB)

- §303a Datenveränderung
- §303b Computersabotage
- §303c Strafantrag

Strafrechtliche Vorschriften

Geregelt im Strafgesetzbuch (StGB)

- §202 Verletzung des Briefgeheimnisses
  - E-Mail zählt als Brief
  - Unabhänging von Verschlüsselung
  - Oberlandesgericht Karlsruhe 2005
  - Firmen-Mails können per Vertrag entbunden werden

Strafrechtliche Vorschriften

Geregelt im Strafgesetzbuch (StGB)

- §202a Ausspähen von Daten
  - Daten die nicht für andere Bestimmt sind
  - Überwindung einer Zugangskontrollsicherung
    - Hier ist nicht Verschlüsselung gemeint
  - Qualität oder aktuelle Standards zählen vor Gericht nicht
  - Beispiel: SQL-Injection

Strafrechtliche Vorschriften

Geregelt im Strafgesetzbuch (StGB)

- §202b Abfangen von Daten
  - Unbefugter Zugriff
  - Nicht für Andere bestimmte Daten
  - Nichtöffentliche Datenübermittlung
    - Verschlüsselt

Strafrechtliche Vorschriften

Geregelt im Strafgesetzbuch (StGB)

- §202c Hackerparagraph
  - Vorbereiten der Straftat
    - Zugang zu Daten ermöglicht
    - Entwicklung von Programmen die den Zugang ermöglichen
  - Keine Strafe
    - Aufgeben der Vorbereitung
    - Programme und technische Hilfsmittel zerstört oder einer Behörde übergibt

Strafrechtliche Vorschriften

Geregelt im Strafgesetzbuch (StGB)

- §149 Wertzeichenfälschung
  - Vorbereitung von Programmen zur Fälschung von Geldmitteln oder Wertzeichen
  - Ausführen der Tat ist natürlich auch Strafbar

- §202d Datenhelerei
  - Der Verkauf von rechtswidrig erlangten Daten ist strafbar

Strafrechtliche Vorschriften

Geregelt im Strafgesetzbuch (StGB)

- §303a Datenveränderung
  - Eine Abänderung, Unterdrückung, Unbrauchbarmachung und Löschung von Daten ist strafbar
  - Nicht als Eigentümer

- §303b Computersabotage
  - Absichtliches Stören einer Datenverarbeitungs-anlage (DVA)
  - DVAs reichen von Server bis Router

Besondere Bedingungen für die Universität Trier

- Bisherige Gesetze und Verordnungen
- Gelten ist das Hochschulgesetz (HG)
  - §3 Freiheit von Kunst und Wissenschaft, Forschung, Lehre und Studium
  - Bisher genannte Gesetze bilden den Rahmen
  - Beschlüsse sind zulässig wenn Forschung und Lehre nicht behindert werden

Bedingungen der Universität Trier

- Teilgrundordnung vom ZIMK
- Benutzerordnung der CIP-Pools
- Dienstanweisungen über Datenschutz und die Datensicherung

Aufgabe 2

- Wie sind Funknetzwerke gegen die Nutzung von Dritten rechtlich Geschützt?
- Inwiefern ist das Abhören von verschlüsselten Funkdaten rechtlich verboten?

Rechtlicher Schutz von Funknetzwerken

- Die §§202-202d und §§303a-303c
- Telekommunikationsgesetz (TKG)
  - Verschlüsselt und unverschlüsselt

Rechtlicher Schutz von Funknetzwerken

Verschlüsselt

- Eindringen in ein gesichtertes Netzwerk
- §202a Ausspähen von Daten
- Unbefugt und Zugangssicherung

Rechtlicher Schutz von Funknetzwerken

Unverschlüsselt

- Keine Datensicherung bzw. Zugriffssicherung
- §202a gilt somit nicht
- Computerbetrug und Schadensersatz kann nicht geltend gemacht werden

Abhören verschlüsselter Daten

- Es greift §202b Abfangen von Daten
  - Unbefugt und nichtöffentliche Datenübertragung
  - §202a ist die Definition für Daten

- Telekommunikationsgesetz (TKG)
  - §89 TKG Abhören von Nachrichten einer Funkanlage
  - Nur vorsätzliches Abhören