Teil I:
Rechtliche Rahmenbedingungen

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

24. November 2016

Aufgabe 1

Welche Gesetze sich mit dem Thema befassen

Zum Thema Netzwerksicherheit bzw. auch Internetsicherheit, befassen sich mehrere verschiedene Gesetze. Diese lassen sich grob in drei Kategorien unterteilen:

- EU-Gesetze
- Deutschlandweite Gesetze
- Hochschulgesetze

Auf EU-Ebene greift zu diesem Thema nur die Grundrechtecharta. Doch dort fehlt es an genaueren Gesetzten und es heißt lediglich nach *Artikel 8 der Grundrechtecharta*:

> (1) Jede Person hat das Recht auf Schutz der sie betreffenden personenbezogenen Daten.
> (2) Diese Daten dürfen nur nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden. Jede Person hat das Recht, Auskunft über die sie betreffenden erhobenen Daten zu erhalten und die Berichtigung der Daten zu erwirken.
> (3) Die Einhaltung dieser Vorschriften wird von einer unabhängigen Stelle überwacht.

Was genau unter „Recht auf Schutz“ gemeint ist und der genauere rechtliche Rahmen wird den einzelnen Ländern überlassen. In Deutschland befassen sich das Bundesdatenschutzgesetz (BDSG) und das Gesetz über den Schutz von zugangskontrollierten Diensten und von Zugangskontrolldiensten (ZKDSG) mit diesem Thema.
Das BDSG umfasst alles was die Privatsphäre personenbezogener Daten betrifft auch im Kontext polizeilicher Überwachung. Einzelne Paragraphen können hier leider nicht aufgezählt werden, da dass BDSG einen zu großen Umfang besitzt. Daher lässt sich das BDSG in sechs Abschnitte unterteilen:

- In (§§ 1–11) werden allgemeine und gemeinsame Bestimmungen erläutert.
- In (§§ 12–26) wird die Datenverarbeitung für öffentliche Stellen geregelt.
- In (§§ 27–38a) wird die Datenverarbeitung für private Stellen geregelt.
- In (§§ 39–42) werden Sondervorschriften geregelt.
- In (§§ 43–44) werden Straf- und Bußgeldvorschriften geregelt.
- In (§§ 45–48) werden Übergangsvorschriften genannt.

Als letzter Punkt muss für den Fall der Forschung und Lehre auch noch das Hochschulgesetz für Rheinland-Pfalz berücksichtigt werden.

- §3 Freiheit von Kunst und Wissenschaft, Forschung, Lehre und Studium

Dort heißt es, dass die Gesetze des Landes und Bundes die Rahmenbedingungen für Forschung und Lehre bilden. Das heißt, dass neben den bereits erwähnten Gesetzen keine weiteren rechtlichen Bedingungen oder Gesetze hinzukommen. Viel mehr ist eine Hochschule auch nach XXX dazu verpflichtet ihrem Lehrauftrag nachzukommen. Es lässt sich also festhalten, dass die Uni selbst wenig Grenzen was die Thematik belangt setzen darf.

Welche Strafrechtlichen Vorschriften es gibt

Im Strafgesetzbuch (StGB) gibt es einige Paragraphen die sich mit dem Thema Datensicherheit befassen. Zuerst folgt eine Auflistung von diesen Paragraphen und anschließend folgt eine detaillierte Erklärung. Im StGB befassen sich folgende Paragraphen mit dem Thema:

- §202 Verletzung des Briefgeheimnisses
- §202a Ausspähen von Daten

- §202b Abfangen von Daten
- §202c Vorbereiten des Ausspähen und Abfangen von Daten (auch bekannt als "Hackerparagraph") in Verbindung mit §149 Wertzeichenfälschung
- §202d Datenhehlerei
- §303a Datenveränderung
- §303b Computersabotage
- §303c Strafantrag

Begonnen wird mit einer Erläuterung zu Paragraph §202 (Briefgeheimnis). In diesem steht:

> (1) Wer unbefugt
>
> 1. einen verschlossenen Brief oder ein anderes verschlossenes Schriftstück, die nicht zu seiner Kenntnis bestimmt sind, öffnet oder
> 2. sich vom Inhalt eines solchen Schriftstücks ohne Öffnung des Verschlusses unter Anwendung technischer Mittel Kenntnis verschafft,
>
> wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft, wenn die Tat nicht in § 206 mit Strafe bedroht ist.
> (2) Ebenso wird bestraft, wer sich unbefugt vom Inhalt eines Schriftstücks, das nicht zu seiner Kenntnis bestimmt und durch ein verschlossenes Behältnis gegen Kenntnisnahme besonders gesichert ist, Kenntnis verschafft, nachdem er dazu das Behältnis geöffnet hat.
> (3) Einem Schriftstück im Sinne der Absätze 1 und 2 steht eine Abbildung gleich.

Wenn man in Artikel 10 des Grundgesetzes (GG) nachschlägt, kann man lesen dass als Brief jede schriftliche Mitteilung zwischen einem Absender und einem Empfänger angesehen wird. Daher unterliegen (neben einer Postkarte) auch E-Mails dem Briefgeheimnis gemäß einer Entscheidung des Oberlandesgerichts Karlsruhe [OLG Karlsruhe, 10.01.2005, 1 W 152/04]. Es kann jedoch auch Ausnahmeregeln geben wie beispielsweise Firmen-Mails. Ist im Vertrag geregelt, dass die E-Mails ausschließlich zum Firmenbetrieb dienen und nicht privat genutzt werden dürfen, darf ein Arbeitgeber die E-Mails mitlesen.
Der nächste Paragraph im StGB ist §202a (Ausspähen von Daten). In diesem heißt es:

> (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. Somit ist es also Strafbar sich mittels SQL-Injection zugriff auf eine Datenbank zu verschaffen. Das liegt daran, dass man die Zugangssicherung umgehen musste. Auch wenn diese sehr schwach ist, reicht vom StGB her um eine gültige Sicherung vor dem Zugriff Anderer darzustellen. Ebenfalls zählen hier Verfahren wie Keylogger. Dabei handelt es sich um nichts anderes als sich Zugang zu Daten zu beschaffen, in dem man das Opfer infiziert, und anschließend dessen Passwörter ausspäht.
Der Absatz (2) grenzt den Begriff der Daten ein, in dem es diese als elektronisch oder magnetisch festschreibt und somit auf den Computer fixiert.
Als nächstes wird auf Paragraph §202b (Abfangen von Daten) eingegangen. Dieser lautet:

> 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.

Unter „unbefugter Beschaffung“ versteht man das Beschaffen von Daten ohne vorherige Erlaubnis des Eigentümers. Des Weiteren ist von „nichtöffentliche Datenübermittlung“die Rede. Darunter versteht man verschlüsselte Funknetzwerke und auch Übertragungen durch Kabel oder andere Wege. Das bedeutet aber auch, dass das mitlesen von unverschlüsselten Daten nicht Strafbar ist, da es sich hierbei um eine „öffentliche Datenübermittlung“ handelt. Ausnahmen in welchen man auch „öffentliche Datenübermittlungen“ nicht mitlesen oder abfangen darf, bilden Datenverarbeitungsanlagen. Das heißt ein Router, welcher offenes WLAN-Netz betreibt, kann im weitesten Sinne als Datenverarbeitungsanlage bezeichnet werden, da es die Daten zwischen den Computern und den Servern regelt.
Der eigentliche „Hackerparagraph“ ist §202c und besteht aus zwei Absätzen. Der Paragraph lautet wie folgt:

> (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) 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.

Absatz 1 besagt, dass wer sich auf irgendeinem Weg mittels Überwindung der Zugangssicherung zu einem System zugriff verschafft, macht sich Strafbar. Des Weiteren ist auch das Verkaufen der Mittel für den Zugang oder das Herstellen solcher Mittel unter Strafe. Was vor allem ein Problem bei sogenannten „Hackertools“ darstellen könnte. Laut StGB gilt hier, wenn die Tools dazu genutzt wurden um einen Angriff auszuführen, so waren die Tools vorbereitender Natur. Dadurch haben sich auch die Entwickler solcher Tools in Deutschland strafbar gemacht. Was auch dazu führt, dass Gruppen wie der Chaos Computer Clubs (CCC) gegen dieses Gesetz sind. Schließlich werden solche Tools auch dazu verwenden, um die eigene Netzstruktur auf Sicherheit zu überprüfen. Vor allem ist zu kritisieren, dass allein entscheidend sei, dass ein Programm oder eine Information genutzt werden könnte, in fremde Computer einzudringen und keine Ausnahmeregelungen bestehen, die den Einsatz für legale Zwecke erlaubt. Nach Absatz 2 gilt, wer eine Tat anfängt diese aber nicht zu Ende führt, das heißt bevor er Daten stiehlt, manipuliert, sich unerlaubt Zugang verschafft etc., macht sich nicht strafbar. Wird der Angriff jedoch nicht erfolgreich ausgeführt oder andere Angreifer führen den Angriff fort, macht man sich dennoch strafbar. Auch hier lässt sich wieder die Problematik von „Hackertools“ erkennen, da der Zweck solcher Tools nicht berücksichtigt wird.
Als nächstes wird §149 (Wertzeichenfälschung) genauer Betrachtet. Hierbei wird unter anderem gesagt, dass das entwickeln eines Computerprogramms zum fälschen von Geldmitteln oder Wertzeichen unter Strafe steht. Auch hier gilt, dass die reine Herstellung eines solches Tools strafbar ist, nicht nur die Ausführung der Fälschung. Hier gibt es, wie bereits zuvor, keine Unterscheidung für den Zweck der Tools. Wenn beispielsweise BitCoin als legitimes Geldmittel anerkannt wären, würde und sich Strafbar machen wenn man Tools entwickelt um diese auf Sicherheit zu überprüfen. Dadurch wird auch hier Sicherheit nicht zwangsläufig gefördert sondern vielmehr verhindert, dass eine erhöhte Sicherheit gewährleistet wird.
Ein weiterer Paragraph der sich mit dem Schutz von Benutzerdaten befasst ist §202d (Datenhehlerei). Dieser besagt, dass auch das verkaufen von rechtswidrig erlangten Daten strafbar ist. Bei der Wahl des

Strafmaßes muss jedoch darauf geachtet werden, dass dieses nicht höher ist als das Strafmaß für das illegale erlangen der Daten.
Auch §303a (Datenveränderung) ist ein wichtiger Paragraph für die Datensicherheit. Er besagt, dass jegliches Abänderung von Daten, die nach §202a rechtswidrig ist, strafbar ist. Hier zählt wie bisher auch wieder, dass allein der Versuch dazu schon strafbar ist. Was die Vorbereitung einer Tat angeht greift die Regelung wie bei §202c.
Computersabotage nach §303b ist das Stören einer fremden Datenverarbeitungsanlage (DVA), die für einen anderen von wesentlicher Bedeutung ist. Hierbei ist sowohl der betriebliche Sinn als auch der private Sinn einer DVA gemeint. Unter einer betrieblichen DVA könnte beispielsweise ein Server verstanden werden wohingegen eine private DVA bereits ein Router sein kann.
In §303c (Strafantrag) wird geregelt wie die Straftat verfolgt wird. Dort heißt es, dass nur in Fällen mit „besonderem öffentlichen Interesse“ die Strafverfolgungsbehörde die Tat selbstständig verfolgt. In allen anderen Fällen muss ein Geschädigter einen Antrag stellen. Zwar bezieht sich §303c nur auf §303, §303a und §303b jedoch unter Berücksichtigung von §202a. Somit handelt es sich in den oben aufgezählten Fällen um ein Antragsdelikt.

Besondere Bedingungen für die Universität Trier

Für die Universität Trier gelten neben den Hochschulgesetzen keine weiteren besonderen Bedingungen. Im Bezug auf die Datensicherheit gibt es dort einen speziellen Paragraphen:

- §3 Freiheit von Kunst und Wissenschaft, Forschung, Lehre und Studium

Dort heißt es, dass die Gesetze des Landes und Bundes die Rahmenbedingungen für Forschung und Lehre bilden. Das heißt, dass neben den bereits erwähnten Gesetzen keine weiteren rechtlichen Bedingungen oder Gesetze hinzukommen. Viel mehr ist eine Hochschule auch nach XXX dazu verpflichtet ihrem Lehrauftrag nachzukommen. Es lässt sich also festhalten, dass die Uni selbst wenig Grenzen was die Thematik belangt setzen darf und nur durch das geltende Gesetz eingeschränkt werden darf.

Welche Bedingungen die Universität selbst stellt

Die besonderen Bedingungen gehen aus der Teilgrundordnung der Universität Trier, Der Benutzerordnung der CIP- und Poolrechner der Abteilung Informatik, sowie der Dienstanweisung über den Datenschutz und die Datensicherung an der Universität Trier hervor.

Aufgabe 2

Rechtlicher Schutz von Funknetzwerken gegenüber der Nutzung Dritter

Abhören von verschlüsselten Funkdaten