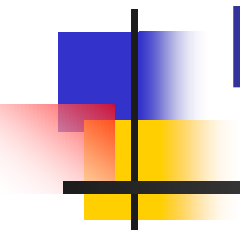

Strafrechtliche Aspekte der Betriebssystemadministration

Ein Überblick

Katja Tröger

Allgemein

1. „Drei Juristen – fünf Meinungen“
2. „Das kommt darauf an“
3. Neben strafrechtlicher Komponente immer auch eine zivilrechtliche (= Schadensersatz)
4. Die meisten Normen durch 2. Gesetz zur Bekämpfung der Wirtschaftskriminalität 1986 in das Strafgesetzbuch eingeführt
5. bundesrecht.juris.de

Grundsätzliches zu Begriffsbestimmung

1. Begriffsbestimmung geht grundsätzlich vom juristischen Laien aus
2. Juristische Bedeutung eines Begriffs zum Teil anders als die der Informatik (idR weiter gefasst)
3. Auslegung (= Begriffsbestimmung) in den Händen des Richters

Voraussetzungen für die Strafbarkeit einer Handlung

Vollendete Tat

- Objektive Erfüllung des gesetzlichen Tatbestands der entsprechenden Norm
- Vorsatz (= Wissen und Wollen des tatbestandlichen Erfolges)
- Rechtswidrigkeit
- Schuld

Daneben ggf. Strafbarkeit des Versuchs

Überblick über die Strafnormen

I. Schutzgut „Daten“
II. Schutzgut „technische Aufzeichnung“
III. Fernmeldegeheimnis und Datenschutzstrafrecht
IV. Sonstige Schutzgüter
V. Cybercrime Convention des Europarats (http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm)

Begriffsbestimmung – Daten und technische Aufzeichnung

→ Daten (Begriff nicht vom Gesetzgeber definiert):

- alle speicherbaren Informationen
- Programme
- Passwörter

→ Technische Aufzeichnung – Legaldefinition in § 268 Abs. 2 StGB

§ 202 a StGB
Ausspähen von Daten

- nicht für den Täter bestimmt (= entgegen dem Willen des Berechtigten)
- besonders gesichert (= Verhindern oder Erschweren des Zugriffs)
- sich verschaffen (= Kenntnis nehmen, teilweise genügt die Möglichkeit)
- Problem: Hacking zu Demonstrationszwecken

§ 303 a StGB Datenveränderung

- Löschen (auf konkretem Datenträger)
- Unterdrücken (= Verhindern der Zugriffsmöglichkeit)
- Unbrauchbarmachen (z.B. Teillöschung, Überschreiben, inhaltliche Umgestaltung, Hinzufügung von Daten)
- Verändern (= neuer Dateninhalt)
- Problem: Entfernung von Viren bei eingehenden E-Mails

§ 303 b StGB Computersabotage (1)

- Datenverarbeitung (= gesamter Arbeitsbereich, der sich auf die Speicherung und Verarbeitung von Daten mittels EDV bezieht)
- Einzelner Datenverarbeitungsvorgang nur, wenn Beeinträchtigung der gesamten Datenverarbeitung

§ 303 b StGB Computersabotage (2)

- von wesentlicher Bedeutung (= idR wenn von solcher Bedeutung, dass von ihrem störungsfreiem Ablauf die Funktionstüchtigkeit der Einrichtung im Ganzen oder in wesentlichen Betriebsteilen abhängt)
- Störung (= nicht unerhebliche Beeinträchtigung des reibungslosen Ablaufs)

Urkundsdelikte §§ 268, 269 StGB

- Ziel: Sicherheit und Zuverlässigkeit des Rechts- und Beweisverkehrs
- Urkunde (= Erklärung, die geeignet oder bestimmt ist, für ein Rechtsverhältnis Beweis zu erbringen, und die ihren Aussteller erkennen lässt)
- Unecht (= nicht von dem, der als Aussteller bezeichnet ist), keine schriftliche Lüge
- Verfälschung (= nachträgliche Veränderung)

§ 268 StGB Fälschung technischer Aufzeichnungen

- Technische Aufzeichnung ist eine Darstellung von Daten, Mess- oder Rechenwerten, Zuständen oder Geschehensabläufen, die durch ein technisches Gerät ganz oder zum Teil selbsttätig bewirkt wird
- Herstellen = Nachahmen einer technischen Aufzeichnung
- Verfälschen = nachträgliche Veränderung
- Auch hier Täuschungsabsicht erforderlich

§ 269 StGB Fälschung beweiserheblicher Daten

- Beweiserheblich = inhaltliche Anforderung
- Speichern oder Verändern, so dass es der Herstellung einer unechten Urkunde bzw. Verfälschung einer echten Urkunde entspricht
- Darüber hinaus genügt der Gebrauch einer so entstandenen Urkunde
- Zusätzliches subjektives Element: die Täuschungsabsicht

§ 274 StGB Urkundsunterdrückung

- Ziel: Schutz der Integrität und Authentizität sowie der Verfügbarkeit beweiserheblicher Daten und technischer Aufzeichnungen
- Persönliches Erfordernis: Verfügen dürfen über die Daten bzw. techn. Aufzeichnung
- Tathandlung: Vernichten, Beschädigen, Unterdrücken
- Zusätzliches subjektives Element: die Nachteilszufügungsabsicht

§ 206 StGB Verletzung des Post- oder Fernmeldegeheimnisses

- Täter = nur Inhaber oder Beschäftigte eines Unternehmens, das geschäftsmäßig Telekommunikationsdienste erbringt
- Tatobjekt = Tatsachen, die dem Fernmeldegeheimnis unterliegen
- Ausgangspunkt für Fernmeldegeheimnis ist das Briefgeheimnis (strafbare Beispiele sind u.a. Öffnen von Post, Lesen von dieser)

Bundesdatenschutzgesetz

- Täter =
  1. Öffentliche Stellen
  2. Nicht-Öffentliche Stellen gemäß § 1 Abs. 2 Nr. 3 BDSG
- Tatobjekt = personenbezogene Daten, die vor unbefugten Zugriffen geschützt werden sollen
- Tathandlung z.B. unbefugte Verarbeitung, Erhebung etc. (siehe Handout)

Tatbestände im Bereich „Sonstige Schutzgüter“

- § 263 a StGB Computerbetrug
- § 317 StGB Störung von Telekommunikationsanlagen

Vielen Dank für Ihre Aufmerksamkeit

Wer für sich jetzt rechtliche Probleme sieht, wende sich an eine Rechtsanwalt ;-)