



Institut für Rechtsinformatik

§ 202c StGB und seine Auswirkungen

Dennis Jlussi

EICAR, BSI Bonn, 15.04.2008



<http://creativecommons.org/licenses/by-nd/3.0/>



Leibniz
Universität
Hannover



§ 202c StGB und seine Auswirkungen

- I. Computerstrafrecht 1986-heute
- II. Der Hackerparagraf 202c
- III. Die vorzubereitenden Erfolgsdelikte (§§ 202a, 202b, 303a, 303b)
- IV. Anforderungen an die Einverständniserklärung
- V. Fazit / Best Practice



I. Computerstrafrecht 1986 – heute

- Eingeführt durch das 2. Gesetz zur Bekämpfung der Wirtschaftskriminalität 1986
- Im Wesentlichen in zwei Abschnitten des StGB
 - Verletzung des persönlichen Lebens- und Geheimbereichs
 - Sachbeschädigung
- NEU: 41. Strafrechtsänderungsgesetz zur Bekämpfung der Computerkriminalität (11.08.2007)
 - Umsetzung
 - der Cybercrime Convention des Europarates
 - des EU-Rahmenbeschlusses 2005/222/JI (nicht § 202c)



Hackerparagraf & Co. – Zum Umgang mit IT-Sicherheitstools

II. Der Hackerparagraf 202c StGB



Der „Hackerparagraf“ 202c StGB

- *§ 202c: Vorbereiten des Ausspähens und Abfangens von Daten*

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 einem Jahr oder mit Geldstrafe bestraft.



Art. 6 Cybercrime Convention

1. Each Party shall [...] establish as criminal offences [...], when committed intentionally and *without right*:
 - a. *the production, sale, procurement for use, import, distribution or otherwise making available* of:
 - i. a device, including a *computer program, designed or adapted primarily for the purpose of committing* any of the offences established in accordance with Articles 2 through 5;
 - ii. a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed,

with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5; and [...]
2. This article shall *not be interpreted* as imposing criminal liability [...] for the *authorised testing or protection of a computer system*. [...]



Wesen und Probleme des § 202c StGB

- § 202c ist selbständiges Vorbereitungsdelikt
- § 202c ist abstraktes Gefährdungsdelikt
 - → Es gibt keinen Geschädigten
 - § 202c daher kein Antragsdelikt!
- Probleme
 - § 202c ist „Waffenrecht“ → Gewaltmonopol des Staates im Internet?
 - Auffangtatbestand bei Beweisnot
 - Praktisch keine Rechtsprechung zu ähnlichen Delikten (Geräte zur Geld-/Passfälschung) seit 45 Jahren!



Hackertool?

- „2. *Computerprogramme*, deren Zweck die Begehung einer solchen Tat ist, [...]“
- **Computerprogramm**
 - Nirgends legal definiert
 - Geeignet, Abläufe eines Computers zu steuern
 - Skripte, die Computerfunktionen steuern (+)
 - Verweise, die eigenständig interpretiert werden müssen (z. B. HTML-Embedding) (-)
 - Beschreibung von Algorithmen in „Menschensprache“ (-)



Hackertool?

- „2. Computerprogramme, deren *Zweck die Begehung einer solchen Tat ist, [...]*“
- Zweck
 - Eignung für Straftaten (202a/b, 303a/b) nicht hinreichend.
 - Neu: „Objektivierte Zweckbestimmung“.
 - Schadsoftware (Viren, Trojaner, Spyware...) (+)
 - Toolkits, Programmiersprachen, kommerzielle Sicherheitssoftware (-)
 - Dual Use Tools (Zweck neutral, wird erst durch Anwender bestimmt)
 - Allein die Möglichkeit, Schadsoftware zu Testzwecken einzusetzen, begründet keinen dual use.
 - Wohl (-)

Vorbereitung einer Straftat

- „Wer eine Straftat nach § 202a oder § 202b *vorbereitet*, indem [...]“ (§§ 303a, 303b verweisen auf § 202c)
- „indem“ bedeutet nicht, dass Vorbereitung bereits in der Tathandlung besteht → eigenständiges Tatbestandsmerkmal.
- Es genügt, wenn der Täter die Förderung einer Straftat für möglich hält und billigend in Kauf nimmt (dem entgegen: Cybercrime Convention erfordert direkten Vorsatz = Wollen).
 - → Fraglich bei (halb-)öffentlicher Verbreitung
- „Inaussichtnahme“ einer Straftat erforderlich: Zumindest einige wesentliche Umstände der Tat müssen bereits feststehen.
- Rechtfertigung für §§ 202a/b, 303a/b schließt auch Strafbarkeit nach § 202c aus! → nicht „without right“



Hackerparagraf & Co. – Zum Umgang mit IT-Sicherheitstools

III. Die vorzubereitenden Delikte §§ 202a, 202b, 303a, 303b



§ 202a StGB – Ausspähen von Daten

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 [...] bestraft.

- Neu: Für Zugang genügt Möglichkeit des Abrufs
 - Früher: Tatsächlicher Abruf erforderlich
- Zugangssicherung: Passwörter etc.
- Einverständnis des Berechtigten schließt Strafbarkeit aus.
- Wer ist Berechtigter? Arbeitnehmer/Arbeitgeber?



§ 202b StGB – 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 [...] verschafft, wird [...] bestraft [...]“

- Auffangtatbestand
- Einwilligung beider Kommunikationspartner erforderlich?
- Rechtfertigung aus TKG?



§ 303a - Datenveränderung

Wer rechtswidrig Daten (§ 202a Abs. 2) löscht, unterdrückt, unbrauchbar macht oder verändert, wird [...] bestraft.

- Einwilligung/Einverständnis des Berechtigten schließt Strafbarkeit aus



§ 303b StGB - Computersabotage

„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 [...]

wird [...] bestraft.“

- Neu: Wesentliche Bedeutung auch für Privatpersonen
- Neu: DDoS-Attacken
- Berechtigter ist, wer über die DV-Anlage verfügt.



Hackerparagraf & Co. – Zum Umgang mit IT-Sicherheitstools

V. Anforderungen an die Einverständniserklärung



Einverständniserklärung

- Durch das Unternehmen
 - IT-Sicherheitsüberprüfungen nur schriftlich vereinbaren
 - Einverständnis ausdrücklich
 - Auf geschlossene Legitimationskette achten (ist derjenige, der Einverständnis erklärt, dazu befugt?)
- Durch die Arbeitnehmer
- Beteiligung des Betriebsrats? Sehr strittig.
 - Bei Privatnutzung wohl nein
 - Ohne Privatnutzung eher nein

V. Rechtliche Anforderungen an die Einverständniserklärung

- Zeitpunkt und Form: aus Beweisgründen schriftlich vor Beginn der Überprüfung (ggf. Annex zum Vertrag)
- Individuell oder generell durch unternehmensinterne Regelung
- Inhalt:
 - Zu überprüfende Systeme
 - Ggf. bestehende Risiken
 - Art und Umfang der Tests (ggf. als Cluster)
- Generell gilt: je intensiver der Eingriff und je höher das Risiko, desto präziser und umfangreicher die Einverständniserklärung



Hackerparagraf & Co. – Zum Umgang mit IT-Sicherheitstools

VI. Fazit / Best Practice



Fazit

- Angeblich „lückenloses“ Strafrecht auf Kosten der Rechtssicherheit der IT-Sicherheitsbranche
- VisuKom-Verfassungsbeschwerde
- TecChannel-Strafanzeige
- Strafbarkeitsrisiken aber minimierbar



Best Practice – warum eigentlich?

- Strafbarkeitsrisiken (für das Unternehmen und persönlich)
- Wirtschaftliche Strafverfahrensrisiken (z.B. Beschlagnahme von Computern)
- Image- und Vertrauensverlust
- Strafanzeigen als Wettbewerbsverhalten?

- Andererseits:
Unterlassung notwendiger/sinnvoller Maßnahmen aus Angst vor Strafbarkeit ist Verlust an IT-Sicherheit



Zusammenfassung: Verhaltensempfehlungen

- Keine Hacker-Tools verwenden, soweit möglich
 - Informationen in „Menschensprache“ austauschen
 - Anerkannte IT-Sicherheitstools verwenden
- Sicherung von Hacker Tools
 - Datenträger unter Verschluss halten
 - Zugriffsberechtigungen beschränken
 - Verbreitung nur in geschlossenen Gruppen (mögl. mit NDA)
- Klare Einwilligung einholen
 - Schriftlich
 - Geschlossene Legitimationskette, evtl. auch Arbeitnehmer(-vertretung)
- Verwendung von Hacker-Tools protokollieren
 - Beschaffung und beabsichtigter Zweck sowie tatsächliche Verwendung
 - Dauerhaft und veränderungssicher protokollieren



Weiterführend:

- *Dennis Jlussi / Christian Hawellek*
IT-Sicherheit im Lichte des Strafrechts
unter besonderer Berücksichtigung des 41. Strafrechtsänderungsgesetzes zur Bekämpfung der Computerkriminalität
Grin Verlag, München 2007, ISBN 978-3638854443
- *Dennis Jlussi*
IT-Sicherheit und § 202c (EICAR Leitfaden)
Strafbarkeit beim Umgang mit IT-Sicherheitstools nach dem
41. Strafrechtsänderungsgesetz zur Bekämpfung der Computerkriminalität
http://www.eicar.org/press/infomaterial/JLUSSI_LEITFADEN_web.pdf
- Kontakt:
 - jlussi (at) iri (dot) uni-hannover (dot) de

Vielen Dank für Ihre Aufmerksamkeit!
Noch Fragen?



"Which one of you is being held
on computer hacking charges?"