



Institut für Rechtsinformatik

Hackerparagraf & Co. Zum Umgang mit IT-Sicherheitstools

Dennis Jlussi | Christian Hawellek

CeBIT Hannover, 7.03.2008



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





Hackerparagraf & Co. – Zum Umgang mit IT-Sicherheitstools

- I. Computerstrafrecht 1986–heute
- II. Der Hackerparagraf 202c:
Strafbarkeit der Vorbereitung
- III. Die vorzubereitenden Erfolgsdelikte
(§§ 202a, 202b, 303a, 303b)
- IV. Strafbarkeit in der Praxis
- V. Rechtliche Anforderungen an die Einverständniserklärung
- VI. Fazit / Best Practice



Hackerparagraf & Co. – Zum Umgang mit IT-Sicherheitstools

I. Computerstrafrecht 1986 – heute



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 Ausspäehens 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**
 - 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).
- „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



III. Die vorzubereitenden Delikte

Überblick:

- § 202a StGB (Ausspähen von Daten)
- § 202b StGB (Abfangen von Daten)
- § 303a StGB (Datenveränderung)
- § 303b StGB (Computersabotage)



III. Die vorzubereitenden Delikte

- § 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 mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.“ [...]

- „Zugang“: Möglichkeit des Abrufs

- Früher: lediglich *tatsächlicher* Abruf

- „Zugangssicherung“: Passwortsperrre, RFID-Karten, Verschlüsselung einer Datei etc.



III. Die vorzubereitenden Delikte

- § 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 mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.“ [...]

- „Daten“: alle elektronisch codierten Informationen in Informationssystemen, ganz gleich wie marginal der Informationsgehalt ist

- Unerheblich ist, ob die Daten gespeichert sind oder gerade übertragen werden



III. Die vorzubereitenden Delikte

- § 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 mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.“ [...]

- Einverständnis des Berechtigten: → Tatbestandsausschluss!
- Problem: Wer ist Berechtigter?

III. Die vorzubereitenden Delikte

- § 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 mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft, wenn die Tat nicht in anderen Vorschriften mit schwererer Strafe bedroht ist.“

- 2007: Schließung der Strafbarkeitslücke des § 202a StGB

- Schutz des „Rechts auf Nicht-Öffentlichkeit der Kommunikation“ im Allgemeinen

- Problematisch beim Einsatz von „Sniffen“ zur Sicherstellung der Netzwerkfunktionalität



III. Die vorzubereitenden Delikte

- § 303a StGB – Datenveränderung

„(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.“

- Recht auf unversehrte Verwendbarkeit der in den Daten enthaltenen Informationen (auch: Sperrung von Daten etc.)
- Typisch: Einsatz von Viren- oder Trojanersoftware

III. Die vorzubereitenden Delikte

- § 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 mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.“

[...]

- „schwere“ Datenveränderung
- seit 2007: DDOS-Attacken
- Von untergeordneter Bedeutung im Bereich der IT-Sicherheit



Hackerparagraf & Co. – Zum Umgang mit IT-Sicherheitstools

IV. Strafbarkeit in der Praxis



IV. Strafbarkeit in der Praxis

Straffrei:

- Rein passive Scans mit Scantools

IV. Strafbarkeit in der Praxis

Ausnutzen gefundener Sicherheitslücken

- entsprechender Funktionen in Scansoftware (etwa AppScan)
 - Eigener / fremder Exploits
 - XSS, SQL-Injections etc.
 - Ebenso: Einsatz von Trojanersoftware
-
- Strafbarkeit nach § 202a StGB
 - Einverständnis des Berechtigten erforderlich



IV. Strafbarkeit in der Praxis

Passwordcracks, mittels

- Wörterbuchattacke
 - Brut-Force-Attacke
 - Cracken der Hashwerte mit Hilfe von Rainbowtables
 - (im Übrigen auch manuelles Ausprobieren)
-
- Strafbarkeit nach § 202a StGB
 - Einverständnis des Berechtigten erforderlich



IV. Strafbarkeit in der Praxis

Überprüfung der Leistungsfähigkeit von Virenabwehrprogrammen

(Einsatz von eigenen oder fremden Viren)

- i. A. Datenveränderung i. S. d. § 303a StGB
- Einverständnis des Berechtigten erforderlich
- Programmierung / Sich-Verschaffen von Viren zum (legalen) Test von Abwehrsoftware ist dann nicht strafbar



IV. Strafbarkeit in der Praxis

Einsatz von Sniffersoftware

- Abfangen von Daten i. S. d. § 202b StGB
 - Problem: Einverständnis des Berechtigten nicht im Voraus zu erlangen!
 - Rechtfertigung aus § 88 III TKG
 - Zulässig soweit zur Sicherstellung der Netzwerkfunktionalität notwendig



Hackerparagraf & Co. – Zum Umgang mit IT-Sicherheitstools

V. Rechtliche Anforderungen an die Einverständniserklärung

V. Rechtliche Anforderungen an die Einverständniserklärung

➤ Testsystem oder Produktivsystem?

- Testsystem: rechtlich unproblematisch (eigenes System oder konkludente Einverständniserklärung)
- Produktivsystem: Einverständnis des Rechtsgutsträgers!

➤ Unternehmensdaten oder private Daten?

- Unternehmensdaten: gesetzlicher Vertreter des Unternehmens (Vorstand der AG, Geschäftsführer der GmbH etc.)
- Recht kann im Rahmen der Unternehmensorganisation delegiert werden (z.B. Gestattung durch IT-Sicherheitsabteilung)



V. Rechtliche Anforderungen an die Einverständniserklärung

- **Problem**: zulässig gespeicherte private Daten (Browser-History etc.)
- Zugangssicherung ist keine des Arbeitnehmers, sondern ausschließlich eine solche des Unternehmens
- Kein Einverständnis des Arbeitnehmers erforderlich

- Gegenansicht: Arbeitnehmer ist selbst auch Rechtsgutsträger
- Einverständniserklärung des Arbeitnehmers erforderlich (ggf. Betriebsvereinbarung)

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
 - hawellek (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?"