

Feil Rechtsanwälte

www.recht-freundlich.de



Der Hackerparagraph im StGB: Was nun?

Chemnitzer Linux-Tage 01. März 2008

Rechtsanwalt Thomas Feil

Fachanwalt für Informationstechnologierecht

Fachanwalt für Arbeitsrecht



Inhalt

- ▶ Hackerparagraf: Was ist neu?
- ▶ Auswirkung auf die Praxis

Computerstrafrecht im StGB

- ▶ In zwei Kapiteln des StGB
 - Verletzung des persönlichen Lebens- und Geheimbereichs
 - Sachbeschädigung

- ▶ Eingeführt durch das 2. Gesetz zur Bekämpfung der Wirtschaftskriminalität 1986

- ▶ NEU: 41. Strafrechtsänderungsgesetz zur Bekämpfung der Computerkriminalität 11.08.2007
 - Neufassung der §§ 202a, 303a, 303 b
 - Einführung der §§ 202b, 202c
 - Umsetzung
 - ♦ der Cybercrime Convention des Europarates
 - ♦ des EU-Rahmenbeschlusses 2003/577/JI

§ 202a StGB

Ausspähen von Daten

- (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.

§ 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 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.

§ 205 StGB Strafantrag

(1) In den Fällen des § 201 Abs. 1 und 2 und der §§ 201a, 202, 203 und 204 wird die Tat nur auf Antrag verfolgt. Dies gilt auch in den Fällen der §§ 202a und 202b, es sei denn, dass die Strafverfolgungsbehörde wegen des besonderen öffentlichen Interesses an der Strafverfolgung ein Einschreiten von Amts wegen für geboten hält.

...

§ 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.

§ 303b StGB

Computersabotage

- (1) 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 oder
 3. eine Datenverarbeitungsanlage oder einen Datenträger zerstört, beschädigt, unbrauchbar macht, beseitigt oder verändert,wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.
- (2) Handelt es sich um eine Datenverarbeitung, die für einen fremden Betrieb, ein fremdes Unternehmen oder eine Behörde von wesentlicher Bedeutung ist, ist die Strafe Freiheitsstrafe bis zu fünf Jahren oder Geldstrafe.

Fortsetzung § 303b

- (3) Der Versuch ist strafbar.
- (4) In besonders schweren Fällen des Absatzes 2 ist die Strafe Freiheitsstrafe von sechs Monaten bis zu zehn Jahren. Ein besonders schwerer Fall liegt in der Regel vor, wenn der Täter
 - 1. einen Vermögensverlust großen Ausmaßes herbeiführt,
 - 2. gewerbsmäßig oder als Mitglied einer Bande handelt, die sich zur fortgesetzten Begehung von Computersabotage verbunden hat,
 - 3. durch die Tat die Versorgung der Bevölkerung mit lebenswichtigen Gütern oder Dienstleistungen oder die Sicherheit der Bundesrepublik Deutschland beeinträchtigt.
- (5) Für die Vorbereitung einer Straftat nach Absatz 1 gilt § 202c entsprechend.

§ 202 c StGB

(1) Wer eine Straftat nach § 202 a oder § 202 b vorbereitet, indem er

1. Passwörter oder sonstige Sicherungscodes, die den Zugang zu Daten (§ 202 a 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.

(2) § 149 Abs. 2 und 3 gilt entsprechend.



Im Vorfeld

- ▶ Vorfeldkriminalisierung im Computerstrafrecht
- ▶ „bestimmte besonders gefährliche Vorbereitungshandlungen“ sollen kriminalisiert werden
 - ABER: Höchststrafe ein Jahr Freiheitsstrafe
 - Versuch zu §§ 202a und § 202b bleibt straflos



Worte des Gesetzgebers

- Drucksache 16/3656 vom 30.11.2006
- „Erfasst werden insbesondere die so genannten Hacker-Tools, die bereits nach der Art und Weise ihres Aufbaus darauf angelegt sind, illegalen Zwecken zu dienen, und die aus dem Internet weitgehend anonym geladen werden können. Insbesondere die durch das Internet mögliche Weiterverbreitung und leichte Verfügbarkeit der Hacker-Tools sowie ihre einfache Anwendung stellen eine erhebliche Gefahr dar, die nur dadurch effektiv bekämpft werden kann, dass bereits die Verbreitung solcher an sich gefährlichen Mittel unter Strafe gestellt wird.“
- „Somit ist sichergestellt, dass nur Hacker-Tools erfasst werden und die allgemeinen Programmier-Tools, -Sprachen oder sonstigen Anwendungsprogramme bereits nicht unter den objektiven Tatbestand der Strafvorschrift fallen. Das Programm muss aber nicht ausschließlich für die Begehung einer Computerstraftat bestimmt sein. Es reicht, wenn die objektive Zweckbestimmung des Tools auch die Begehung einer solchen Straftat ist.“



Optimismus der Regierung

- ▶ Sicht der Bundesregierung
- ▶ „Die Nichterfassung des gutwilligen Umgangs mit Softwareprogrammen zur Sicherheitsüberprüfung von IT-Systemen wird bereits auf Tatbestandsebene durch zwei gesetzliche Tatbestandsmerkmale abgesichert. Einerseits muss es sich objektiv um ein Computerprogramm handeln, dessen Zweck die Begehung einer Computerstraftat ist, und andererseits muss die Tathandlung – also das Herstellen, Verschaffen, Verkaufen, Überlassen, Verbreiten oder sonst Zugänglichmachen – zur Vorbereitung einer Computerstraftat erfolgen.“
- ▶ Dann ist „gutwillige“ Nutzung nicht strafbar!

ABER ...

- ▶ Abstraktes Gefährdungsdelikt, daher kein Antragsdelikt (dagegen fordern §§ 202a, 202b Strafantrag, obwohl Täter geschütztes Rechtsgut verletzt)
- ▶ Auffangtatbestand bei Beweisnot
- ▶ Objektiver Tatbestand
 - Computerprogramm
 - ♦ geeignet, Abläufe eines Computers zu steuern
 - ♦ Skripte, die Computerfunktionen steuern
 - ♦ Nicht Beschreibung von Algorithmen in Menschengsprache
 - ♦ Bloße Beschreibung von Sicherheitslücken, da kein Computerprogramm zugänglich gemacht wird.

Objektiver Tatbestand

- ▶ Zweck

„...deren Zweck die Begehung einer solchen Tat ist ...“

- ▶ Objektivierter Zweckbestimmung

Eindeutig bei Schadsoftware

Nicht Programmiersprachen, kommerzielle Sicherheitssoftware

Schwierig: Dual-use Programme

- ♦ Zweck wird durch den Anwender bestimmt

- ▶ Art 6 Cybercrime Convention *„... designed or adapted primarily for the purpose of committing...“*

Subjektiver Tatbestand

- ▶ bedingter Vorsatz“ genügt

Ein Täter muss zumindest billigend in Kauf nehmen, durch die Handlung eine Computerstraftat zu ermöglichen oder zu fördern.

- ▶ Selbständiges subjektives Tatbestandsmerkmal

„Wer eine Straftat nach ... vorbereitet, indem er ...“

Keine Kriminalisierung bei Einwilligung (z.B. Penetrationstest)

Überschießende Innentendenz: Täter oder Dritter muss eine Straftat in Aussicht nehmen

diese Tat muss in wesentlichen Umrissen konkretisiert sein, entsprechend muss auch der Vorsatz konkretisiert sein (umstritten; aA: Täter handelt in dem Bewusstsein, dass die Tatobjekte irgendwann einmal einer Computerstraftat dienen können)



Das Grundgesetz

- ▶ Aufgabe des Gesetzgebers: Überkriminalisierung durch hinreichend bestimmte Fassung von Straftatbeständen vorbeugen
- ▶ Art. 103 Abs. 2 GG
 - „Eine Tat kann nur bestraft werden, wenn die Strafbarkeit gesetzlich bestimmt war, bevor die Tat begangen wurde.“*

Ähnlich

- ▶ § 22b Abs. 1 Nr. 3 StVG
- ▶ Vorbereitung einer Manipulation von Wegstreckenzählern und Geschwindigkeitsbegrenzern in Kfz
- ▶ Hier auch rechtlich neutrale Tatobjekte („Dual Use“) umfasst
- ▶ Verfassungsbeschwerde - > Entscheidung BVerfG 09.05.2006

Restriktive Auslegung: Nur Programme erfasst, die nur ausschließlich deliktisch verwendbar sind

Es reicht nicht aus, wenn „das Computerprogramm lediglich zur Begehung der in Bezug genommenen Straftat geeignet ist oder im Einzelfall der Begehung solcher Straftaten dient“



Kritische Situationen

- ▶ Hacking Live-Demonstration
- ▶ Zeitschrift Hakin9
- ▶ Einsatz von dual-use-Programmen
- ▶ Öffentliche/halb-öffentliche Foren: Abwehrstrategien gegen Schadprogramme
- ▶ ...



Auswege?

► 4 Wege zeichnen sich ab:

Gutachten über Rechtslage

Verfassungsbeschwerde

„Kopf-in-den-Sand“

Strafanzeige gegen sich selbst? Eine Lösung?



Noch nicht alles..

- ▶ Auswirkung für Arbeitsverhältnisse

Risiken für IT-Administratoren und Mitarbeiter der IT-Abteilungen

- ▶ Wettbewerbskampf mit neuen Mitteln

- ▶ Risikomanagement neu justieren?

So entscheiden Arbeitsgerichte

LAG Hamm vom 04.02.2004 (Az.: 9 Sa 502/03)

1. Stellt der Arbeitgeber dem Arbeitnehmer einen Rechner zur Verfügung, der nur unter Verwendung eines Passworts in Betrieb genommen werden kann, welches der Arbeitnehmer selbst bestimmt, hat dies ohne Hinzutreten weiterer Umstände (z.B. Erlaubnis oder Duldung privater Nutzung) nicht die Folge, dass die auf der Festplatte oder im Server vom Arbeitnehmer abgespeicherten Dateien dessen "private" Dateien darstellen. Der Arbeitgeber kann jedenfalls aus begründetem Anlass ohne Einverständnis des betroffenen Arbeitnehmers Zugriff auf diese Dateien nehmen.
2. Das Speichern von 17 "Hacker"-Dateien, unter denen sich eine Datei zum Entschlüsseln des "BIOS"-Passworts befindet, stellt grundsätzlich einen Grund zur fristlosen Kündigung des Arbeitnehmers dar. Die abschließende Interessenabwägung kann auch dann zu Ungunsten des Arbeitnehmers ausfallen, wenn ein Schaden noch nicht eingetreten ist und der Mitarbeiter zuvor 24 Jahre seine Arbeitsleistung unbeanstandet erbracht hat.



Verhaltensempfehlungen

- ▶ Keine Hacker-Tools verwenden
- ▶ Sicherung von Hacker-Tools vor unberechtigten Zugriffen
- ▶ Klare Einwilligung holen
 - als Arbeitnehmer
 - als Dienstleister
- ▶ Verwendung von Hacker-Tools protokollieren
 - Beschaffung und beabsichtigter Zwecke sowie tatsächliche Verwendung
 - Unveränderbare Speicherung zu Beweis Zwecken

Weitergabe von Passwörter

► § 202 c StGB

Wer eine Straftat nach § 202 a oder § 202 b vorbereitet, indem er

1. Passwörter oder sonstige Sicherungscodes, die den Zugang zu Daten (§ 202 a Abs. 2) ermöglichen, oder

...

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.



Kritische Situationen

- ▶ Weitergabe von Passwörter bei Abwesenheit, z.B. Urlaub oder Krankheit
„billigend in Kauf nehmen“
- ▶ Weitergabe Passwörter an externe Dienstleister

Feil Rechtsanwälte

www.recht-freundlich.de



Haben Sie noch Fragen?

Feil Rechtsanwälte

www.recht-freundlich.de



Rechtsanwalt Thomas Feil

Fachanwalt für Informationstechnologierecht

Rechtsanwalt Martin Stabno

Dipl. Verwaltungswirt

Rechtsanwältin Dr. Andrea Töllner

Georgsplatz 9 · 30159 Hannover

Tel. 0511 / 473906-01

Fax 0511 / 473906-09

kanzlei@recht-freundlich.de