

Hacking & Computerstrafrecht

SAE Multimedia Workshop Tag

Lukas Feiler

lukas.feiler@lukasfeiler.com
<http://teaching.lukasfeiler.com>

Abstract:

Behandelt werden unterschiedliche Angriffsvarianten auf Computersysteme und ihre Beurteilung nach österreichischem Strafrecht. Ebenso Gegenstand des Vortrages ist die Cyber-Crime-Konvention des Europarates. Angriffsvarianten wie Buffer Overflows und SQL-Injection werden praktisch demonstriert!

Inhalt:

1. Österreichische Strafrechtsdogmatik
 - a. Zweck des Strafrechts: Spezial -und Generalprävention
 - b. Der fragmentarische Charakter des Strafrechts
 - c. Der objektive & subjektive Tatbestand
 - d. Rechtswidrigkeit und Verschulden
 - e. Die wichtigsten Tatbestände des Computerstrafrechts
 - i. § 118a StGB Widerrechtlicher Zugriff auf ein Computersystem
 - ii. § 119 StGB Verletzung des Telekommunikationsgeheimnisses
 - iii. § 119a StGB Missbräuchliches Abfangen von Daten
 - iv. § 126a StGB Datenbeschädigung
 - v. § 126b StGB Störung der Funktionsfähigkeit eines Computersystems
 - vi. § 126c StGB Missbrauch von Computerprogrammen oder Zugangsdaten
 - vii. § 51 DSGVO Datenverwendung in Gewinn- oder Schädigungsabsicht
2. Die Cyber-Crime-Konvention des Europarates
3. Angriffe auf Computersysteme und ihre rechtliche Beurteilung
 - a. Die Anatomie eines Angriffs
 - b. Tätergruppen: von Script Kiddies zu Underground-Hackern
 - c. Angriffe auf die Vertraulichkeit von Daten
 - i. Password Guessing & Bruteforce Attacks
 - ii. Buffer Overflows
 - iii. Sniffing
 - iv. Phishing & Social Engineering
 - d. Angriffe auf die Integrität von Daten
 - i. SQL-Injection
 - e. Angriffe auf die Verfügbarkeit von Daten
 - i. Denial of Service Attacks (DoS)
 - ii. Distributed Denial of Service Attacks (DDoS)
 - f. Strafbarkeit erfolgloser/unterbliebener Angriffe?
 - i. Der Versuch
 - ii. Port Scanning & Vulnerability Scanning
 - iii. Das Besitzen von Exploits und Sniffern
 - g. Rechtspolitische Überlegungen

Allgemeine Bestimmungen des StGB

Keine Strafe ohne Gesetz

§ 1. (1) Eine Strafe oder eine vorbeugende Maßnahme darf nur wegen einer Tat verhängt werden, die unter eine ausdrückliche gesetzliche Strafdrohung fällt und schon zur Zeit ihrer Begehung mit Strafe bedroht war.

Keine Strafe ohne Schuld

§ 4. Strafbar ist nur, wer schuldhaft handelt.

Vorsatz

§ 5. (1) Vorsätzlich handelt, wer einen Sachverhalt verwirklichen will, der einem gesetzlichen Tatbild entspricht; dazu genügt es, daß der Täter diese Verwirklichung ernstlich für möglich hält und sich mit ihr abfindet.

(2) Der Täter handelt absichtlich, wenn es ihm darauf ankommt, den Umstand oder Erfolg zu verwirklichen, für den das Gesetz absichtliches Handeln voraussetzt.

(3) *hier nicht abgedruckt*

Strafbarkeit vorsätzlichen und fahrlässigen Handelns

§ 7. (1) Wenn das Gesetz nichts anderes bestimmt, ist nur vorsätzliches Handeln strafbar.

Hausfriedensbruch

§ 109 Abs. 1 StGB. Wer [vorsätzlich] den Eintritt in die Wohnstätte eines anderen mit Gewalt oder durch Drohung mit Gewalt erzwingt, ist mit Freiheitsstrafe bis zu einem Jahr zu bestrafen.

Sachbeschädigung

§ 125 StGB. Wer [vorsätzlich] eine fremde Sache zerstört, beschädigt, verunstaltet oder unbrauchbar macht, ist mit Freiheitsstrafe bis zu sechs Monaten oder mit Geldstrafe bis zu 360 Tagessätzen zu bestrafen.

Convention on Cybercrime

Chapter II, Title 1 - Offences against the confidentiality, integrity and availability of computer data and systems

Article 2 - Illegal access

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.

Article 3 - Illegal interception

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system.

Article 4 - Data interference

1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right.

2. A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.

Article 5 - System interference

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.

Article 6 - Misuse of devices

1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, 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 Article 2 - 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 - 5; and

b. the possession of an item referred to in paragraphs (a)(1) or (2) above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 - 5. A Party may require by law that a number of such items be possessed before criminal liability attaches.

2. This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 of this Article is not for the purpose of committing an offence established in accordance with articles 2 through 5 of this Convention, such as for the authorised testing or protection of a computer system.

3. Each Party may reserve the right not to apply paragraph 1 of this Article, provided that the reservation does not concern the sale, distribution or otherwise making available of the items referred to in paragraph 1 (a) (2).

Delikte im Bereich des Computerstrafrechts

Widerrechtlicher Zugriff auf ein Computersystem

§ 118a StGB. (1) Wer sich in der Absicht sich oder einem anderen Unbefugten von in einem Computersystem gespeicherten und nicht für ihn bestimmten Daten Kenntnis zu verschaffen und dadurch, dass er die Daten selbst benützt, einem anderen, für den sie nicht bestimmt sind, zugänglich macht oder veröffentlicht, [und] sich oder einem anderen einen Vermögensvorteil zuzuwenden oder einem anderen einen Nachteil zuzufügen, [vorsätzlich] zu einem Computersystem, über das er nicht oder nicht allein verfügen darf, oder zu einem Teil eines solchen Zugang verschafft, indem er spezifische Sicherheitsvorkehrungen im Computersystem verletzt,

ist mit Freiheitsstrafe bis zu sechs Monaten oder mit Geldstrafe bis zu 360 Tagessätzen zu bestrafen.

(2) Der Täter ist nur mit Ermächtigung des Verletzten zu verfolgen.

Verletzung des Telekommunikationsgeheimnisses

§ 119 StGB. (1) Wer in der Absicht, sich oder einem anderen Unbefugten vom Inhalt einer im Wege einer Telekommunikation (§ 3 Z 13 TKG) oder eines Computersystems übermittelten und nicht für ihn bestimmten Nachricht Kenntnis zu verschaffen, [vorsätzlich] eine Vorrichtung, die an der Telekommunikationsanlage oder an dem Computersystem angebracht oder sonst empfangsbereit gemacht wurde, benützt,

ist mit Freiheitsstrafe bis zu sechs Monaten oder mit Geldstrafe bis zu 360 Tagessätzen zu bestrafen.

(2) Der Täter ist nur mit Ermächtigung des Verletzten zu verfolgen.

Missbräuchliches Abfangen von Daten

§ 119a StGB. (1) Wer in der Absicht,
sich oder einem anderen Unbefugten von im Wege eines Computersystems übermittelten und nicht für ihn bestimmten Daten Kenntnis zu verschaffen
und
dadurch, dass er die Daten selbst benützt, einem anderen, für den sie nicht bestimmt sind, zugänglich macht oder veröffentlicht,
[und]
sich oder einem anderen einen Vermögensvorteil zuzuwenden oder einem anderen einen Nachteil zuzufügen,

[vorsätzlich]

eine Vorrichtung, die an dem Computersystem angebracht oder sonst empfangsbereit gemacht wurde, benützt
oder
die elektromagnetische Abstrahlung eines Computersystems auffängt,

ist, wenn die Tat nicht nach § 119 mit Strafe bedroht ist, mit Freiheitsstrafe bis zu sechs Monaten oder mit Geldstrafe bis zu 360 Tagessätzen zu bestrafen.

(2) Der Täter ist nur mit Ermächtigung des Verletzten zu verfolgen.

Datenverwendung in Gewinn- oder Schädigungsabsicht

§ 51 DSGVO. (1) Wer in der Absicht,
sich einen Vermögensvorteil zu verschaffen oder einem anderen einen Nachteil zuzufügen,

[vorsätzlich] personenbezogene Daten,
die ihm ausschließlich auf Grund seiner berufsmäßigen Beschäftigung anvertraut oder zugänglich geworden sind oder die er sich widerrechtlich verschafft hat,
selbst benützt, einem anderen zugänglich macht oder veröffentlicht,
obwohl der Betroffene an diesen Daten ein schutzwürdiges Geheimhaltungsinteresse hat,

ist, wenn die Tat nicht nach einer anderen Bestimmung mit strengerer Strafe bedroht ist, vom Gericht mit Freiheitsstrafe bis zu einem Jahr zu bestrafen.

(2) Der Täter ist nur mit Ermächtigung des Verletzten zu verfolgen.

Mißbrauch von Tonaufnahme- oder Abhörgeräten

§ 120 StGB. (1) Wer
[vorsätzlich] ein Tonaufnahmegerät oder ein Abhörgerät benützt,
um sich oder einem anderen Unbefugten von einer nicht öffentlichen und
nicht zu seiner Kenntnisnahme bestimmten Äußerung eines anderen
Kenntnis zu verschaffen,

ist mit Freiheitsstrafe bis zu einem Jahr
oder mit Geldstrafe bis zu 360 Tagessätzen zu bestrafen.

(2) Ebenso ist zu bestrafen, wer ohne Einverständnis des
Sprechenden die Tonaufnahme einer nicht öffentlichen Äußerung eines
anderen einem Dritten, für den sie nicht bestimmt ist, zugänglich
macht oder eine solche Aufnahme veröffentlicht.

(2a) Wer
eine im Wege einer Telekommunikation (§ 3 Z 13 TKG) übermittelte und nicht
für ihn bestimmte Nachricht
in der Absicht,
sich oder einem anderen Unbefugten vom Inhalt dieser Nachricht
Kenntnis zu verschaffen,
aufzeichnet, einem anderen Unbefugten zugänglich macht oder veröffentlicht,

ist, wenn die Tat nicht nach den vorstehenden Bestimmungen oder nach einer
anderen Bestimmung mit strengerer Strafe bedroht ist, mit Freiheitsstrafe
bis zu drei Monaten oder mit Geldstrafe bis zu 180 Tagessätzen zu
bestrafen.

(3) Der Täter ist nur mit Ermächtigung des Verletzten zu verfolgen.

Auskundschaftung eines Geschäfts- oder Betriebsgeheimnisses

§ 123 StGB. (1) Wer
[vorsätzlich] ein Geschäfts- oder Betriebsgeheimnis
mit dem Vorsatz auskundschaftet,
es zu verwerten, einem anderen zur Verwertung zu überlassen oder der
Öffentlichkeit preiszugeben,

ist mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bis zu 360
Tagessätzen zu bestrafen. Beide Strafen können auch nebeneinander verhängt
werden.

(2) Der Täter ist nur auf Verlangen des Verletzten zu verfolgen.

Datenbeschädigung

§ 126a StGB. (1) Wer
einen anderen dadurch [vorsätzlich] schädigt,
daß er automationsunterstützt verarbeitete, übermittelte oder überlassene
Daten, über die er nicht oder nicht allein verfügen darf, verändert,
löscht oder sonst unbrauchbar macht oder unterdrückt,

ist mit Freiheitsstrafe bis zu sechs Monaten oder mit Geldstrafe bis zu 360
Tagessätzen zu bestrafen.

(2) Wer durch die Tat an den Daten einen 3 000 Euro übersteigenden
Schaden herbeiführt, ist mit Freiheitsstrafe bis zu zwei Jahren oder
mit Geldstrafe bis zu 360 Tagessätzen, wer einen 50 000 Euro
übersteigenden Schaden herbeiführt, mit Freiheitsstrafe von sechs
Monaten bis zu fünf Jahren zu bestrafen.

Störung der Funktionsfähigkeit eines Computersystems

§ 126b StGB. Wer
[vorsätzlich] die Funktionsfähigkeit eines Computersystems,
über das er nicht oder nicht allein verfügen darf, dadurch schwer stört,
dass er Daten eingibt oder übermittelt,

ist, wenn die Tat nicht nach § 126a mit Strafe bedroht ist, mit
Freiheitsstrafe bis zu sechs Monaten oder mit Geldstrafe bis zu 360
Tagessätzen zu bestrafen.

Missbrauch von Computerprogrammen oder Zugangsdaten

§ 126c StGB. (1) Wer

1. ein Computerprogramm, das nach seiner besonderen Beschaffenheit
ersichtlich zur Begehung eines widerrechtlichen Zugriffs auf
ein Computersystem (§ 118a), einer Verletzung des
Telekommunikationsgeheimnisses (§ 119), eines missbräuchlichen
Abfangens von Daten (§ 119a), einer Datenbeschädigung (§ 126a),
einer Störung der Funktionsfähigkeit eines Computersystems
(§ 126b) oder eines betrügerischen Datenverarbeitungsmissbrauchs
(§ 148a) geschaffen oder adaptiert worden ist, oder eine
vergleichbare solche Vorrichtung oder
2. ein Computerpasswort, einen Zugangscode oder vergleichbare
Daten, die den Zugriff auf ein Computersystem oder einen Teil
davon ermöglichen,
mit dem Vorsatz
herstellt, einführt, vertreibt, veräußert, sonst zugänglich macht,
sich verschafft oder besitzt,
dass sie zur Begehung einer der in Z 1 genannten strafbaren Handlungen
gebraucht werden,

ist mit Freiheitsstrafe bis zu sechs Monaten oder mit Geldstrafe bis zu 360
Tagessätzen zu bestrafen.

(2) Nach Abs. 1 ist nicht zu bestrafen, wer freiwillig verhindert,
dass das in Abs. 1 genannte Computerprogramm oder die damit
vergleichbare Vorrichtung oder das Passwort, der Zugangscode oder
die damit vergleichbaren Daten in der in den §§ 118a, 119, 119a,
126a, 126b oder 148a bezeichneten Weise gebraucht werden. Besteht
die Gefahr eines solchen Gebrauches nicht oder ist sie ohne Zutun
des Täters beseitigt worden, so ist er nicht zu bestrafen, wenn er
sich in Unkenntnis dessen freiwillig und ernstlich bemüht, sie zu
beseitigen.

Rechtsquellen selbst finden

StGB u. DSG:

Rechtsinformationssystem des Bundes: <http://ris.bka.gv.at/bundesrecht/>
Bei Kurztitel/Abkürzung „StGB“ bzw. „DSG“ und bei Paragraph „0“ eingeben; erhaltenes Ergebnis anklicken und dann (rechts oben) „Geltende Fassung“ wählen.

Cyber-Crime-Konvention (CyCC)

<http://www.coe.int> bzw. <http://www.lukasfeiler.com/CyCC/>

Weiterführende Literatur/Quellen

Auf Verweise auf allgemeine Strafrechtswissenschaften wird an dieser Stelle verzichtet.

Reindl, Computerstrafrecht im Überblick, WUV, 2004

Garfinkel/Spafford, Practical Unix and Internet Security, 3rd Edition, O'Reilly & Associates, 2003

Northcutt/Zeltser/Winters/Fredrick/Ritchey, Inside Network Perimeter Security: The Definitive Guide to Firewalls, VPNs, Routers, and Intrusion Detection Systems, New Riders Publishing, 2002

McNab, Network Security Assessment, O'Reilly & Associates, 2004

Northcutt/Cooper/Fearnow/Frederick, Intrusion Signatures and Analysis, New Riders Publishing, 2001

Peikari/Chuvakin, Security Warrior, O'Reilly & Associates, 2004

Cox/Gerg, Managing Security with Snort and IDS Tools, O'Reilly & Associates, 2004

Barman, Writing Information Security Policies, New Riders Publishing, 2002

Elledge, Phishing: An Analysis of a Growing Problem, GIAC Security Essentials Certification (GSEC) Practical, Version 1.4b, Option 1, SANS Institute 2004,
<http://www.sans.org/rr/whitepapers/threats/1417.php>

Feiler, Sicherheitsrisiken im Internet, 2004,
http://www.lukasfeiler.com/Sicherheitsrisiken_im_Internet.pdf