

# Kapitel: Rechtliche Aspekte

# Vertrag

- Für den Vertrag eines Security Assessments, insbesondere beim Penetration Test sind folgende Aspekte zu beachten
  - Schriftliche Form (auch Änderungen bei Durchführung)
  - Genaue Bezeichnung der Vertragspartner und einen Ansprechpartner pro Partei (Unterlieferanten?)
  - Genaue Bezeichnung des Vertragsgegenstand. Insbesondere von Ziel, Verfahren, eingesetzten Technologien
  - Vertraulichkeitserklärungen
  - Einverständniserklärung für ein Security Assessment

# Besonders zu beachten (Erfahrungsbericht)

- Einverständniserklärungen einholen vom Serverbetreiber, wenn der zu penetrierende Server nicht dem Auftraggeber gehört. Abklären ob auf den Servern noch Services von anderen Kunden installiert sind
- Siehe Beilage CDROM: Musterreglement für die Internet- und E-Mail Überwachung am Arbeitsplatz  
(<http://www.edsb.ch/d/doku/leitfaeden/internet/index.htm>)

# Schweizerisches Recht (auf einen Blick)

- Datenschutzgesetz (DSG) vom 19. Juni 1992
  - Art. 7: Datensicherheit
- Strafgesetzbuch (StGB)
  - Art. 143: Unbefugte Datenbeschaffung
  - Art. 143: Unbefugtes Eindringen in ein Datenverarbeitungssystem
  - Art. 143: Datenbeschädigung
  - Art. 179 novies 142 : Unbefugtes Beschaffen von Personendaten
- Obligationenrecht (OR)
  - Allgemeines Vertragsrecht

# Datenschutzgesetz (DSG) vom 19. Juni 1992

- Art. 7: Datensicherheit

<sup>1</sup> Personendaten müssen durch angemessene technische und organisatorische Massnahmen gegen unbefugtes Bearbeiten geschützt werden.

# Strafgesetzbuch (StGB)

- Art. 143: Unbefugte Datenbeschaffung

<sup>1</sup> Wer in der Absicht, sich oder einen andern unrechtmässig zu bereichern, sich oder einem andern elektronisch oder in vergleichbarer Weise gespeicherte oder übermittelte Daten beschafft, die nicht für ihn bestimmt und gegen seinen unbefugten Zugriff besonders gesichert sind, wird mit Zuchthaus bis zu fünf Jahren oder mit Gefängnis bestraft.

<sup>2</sup> Die unbefugte Datenbeschaffung zum Nachteil eines Angehörigen oder Familiengenossen wird nur auf Antrag verfolgt.

# Strafgesetzbuch (StGB)

- Art. 143: Unbefugtes Eindringen in ein Datenverarbeitungssystem

Wer ohne Bereicherungsabsicht auf dem Wege von Datenübertragungseinrichtungen unbefugterweise in ein fremdes, gegen seinen Zugriff besonders gesichertes Datenverarbeitungssystem eindringt, wird, auf Antrag, mit Gefängnis oder mit Busse bestraft.

# Strafgesetzbuch (StGB)

- Art. 143: Datenbeschädigung

1. Wer unbefugt elektronisch oder in vergleichbarer Weise gespeicherte oder übermittelte Daten verändert, löscht oder unbrauchbar macht, wird, auf Antrag, mit Gefängnis oder mit Busse bestraft.

Hat der Täter einen grossen Schaden verursacht, so kann auf Zuchthaus bis zu fünf Jahren erkannt werden. Die Tat wird von Amtes wegen verfolgt.

2. Wer Programme, von denen er weiss oder annehmen muss, dass sie zu den in Ziffer 1 genannten Zwecken verwendet werden sollen, herstellt, einführt, in Verkehr bringt, anpreist, anbietet oder sonstwie zugänglich macht oder zu ihrer Herstellung Anleitung gibt, wird mit Gefängnis oder mit Busse bestraft.

Handelt der Täter gewerbsmässig, so kann auf Zuchthaus bis zu fünf Jahren erkannt werden.

# Strafgesetzbuch (StGB)

- Art. 179 novies 142: Unbefugtes Beschaffen von Personendaten

Wer unbefugt besonders schützenswerte Personendaten oder Persönlichkeitsprofile, die nicht frei zugänglich sind, aus einer Datensammlung beschafft, wird auf Antrag mit Gefängnis oder mit Busse bestraft.

# Anhang: Leitfaden Eidg. Datenschutzbeauftragter.

- Eidgenössischer Datenschutzbeauftragter  
Leitfaden über Internet- und E-Mail-Überwachung am Arbeitsplatz  
<http://www.edsb.ch/d/doku/leitfaeden/internet/index.htm>
- Leitfaden zu den technischen und organisatorischen Massnahmen des Datenschutzes  
<http://www.edsb.ch/d/doku/leitfaeden/tom.pdf>

# Anhang: Links

- Sicherheitsüberprüfungen von IT-Systemen mit Hilfe von “Tiger-Teams”  
<http://www.isaca.ch/download/tigerteam/tigerteam.pdf>
- Eidgenössisches Justiz- und Polizeidepartement  
Rechtsinformatik und Informatikrecht  
<http://www.ofj.admin.ch/d/index.html>
- Eidgenössischer Datenschutzbeauftragter  
<http://www.edsb.ch/>  
Fallbeispiele: <http://www.edsb.ch/d/themen/internet/bsp.htm>
- Bundesgesetz vom 19. Juni 1992 über den Datenschutz (DSG)  
[http://www.admin.ch/ch/d/sr/c235\\_1.html](http://www.admin.ch/ch/d/sr/c235_1.html)
- Schweizerisches Strafgesetzbuch  
<http://www.admin.ch/ch/d/sr/31.html#311.0>

Compass Security AG  
Glärnischstrasse 7  
Postfach 1671  
8640 Rapperswil

info@csnc.ch

<http://www.csnc.ch/>

Tel: 055 214 41 60

Fax: 055 214 41 61