

Horst Speichert

e|s|b Rechtsanwälte Stuttgart

Attorney
Assistant Professor at
Stuttgart University
Data Protection Officer

- •IT Law
- Data Protection Law
- IT Security Law
- Media Law
- software contracts
- privacy agreements

E-Mail: horst@speichert.de

Internet: http://www.kanzlei.de

http://www.speichert.de

reference

Speichert, Horst Praxis des IT-Rechts -

Praktische Rechtsfragen der IT-Sicherheit und Internetnutzung

Vieweg Verlag, 2. Auflage, Mai 2007, geb. KES-Reihe ISBN: 3-528-05815-3 €49,90



overview

- german legislation, european background
- legal situation
 - wording of § 202c StGB
 - basic principles
 - objective purpose
- negative consequences
 - criminalization of vulnerability analysis
 - legal uncertainty for admins and penetration testing
- recent trials
 - criminal complaint
 - constitutional complaint
- avoidance strategie
 - reasonable limitation
 - agreement

legislation

- 41. Criminal Law Amendatory Act
- coming into effect on 11 August 2007
- introduction of the new article § 202c StGB (Penal Code)
- the origin of § 202c StGB is Art. 6 of the "Convention on Cybercrime" of the Council of Europe on 23 November 2001
- this convention was transfered by the German Legislature into German Criminal Law on 11 August 2007



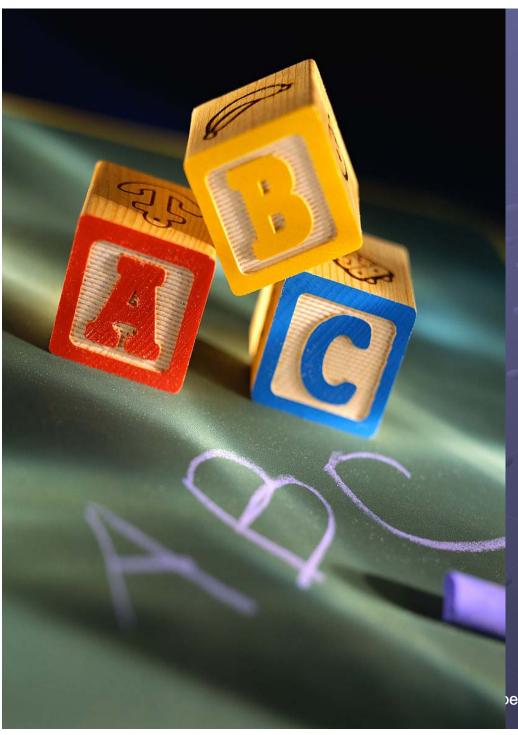
wording of § 202c StGB

"Preparing a criminal offence acc. §202a StGB (spying of data) or acc. §202b StGB (interception of data)

as he produces, procures, sells, distributes or makes otherwise available

- 1st passwords or other safety codes which provide access to data (§ 202a II StGB), or
- 2nd computer programme whose purpose is the perpetration of such act,

will be punished with imprisonment up to one year or be fined."





Basics

basic requirements

- § 202c StGB is designed as an abstract threat against possible offenders to prevent actual criminality previously
- subjects acc. § 202 c StGB
 - passwords
 - other security codes which provide access to data
 - computer programs whose purpose is to commit a cybercrime (= hackertools)
- unlawful activity acc. § 202 c StGB
 - to produce
 - to procure
 - to sell
 - to distribute
 - to make otherwise available

basic requirements

- addtitional reguirement
 a preparing act for committing a cybercrime (acc. § 202c StGB and because of the link in § 303a III, § 303b V StGB)
 - spying of data acc. §202a StGB
 - interception of data acc. §202b StGB
 - data alteration acc. § 303a StGB
 - computer sabotage acc. § 303b StGB

objective purpose

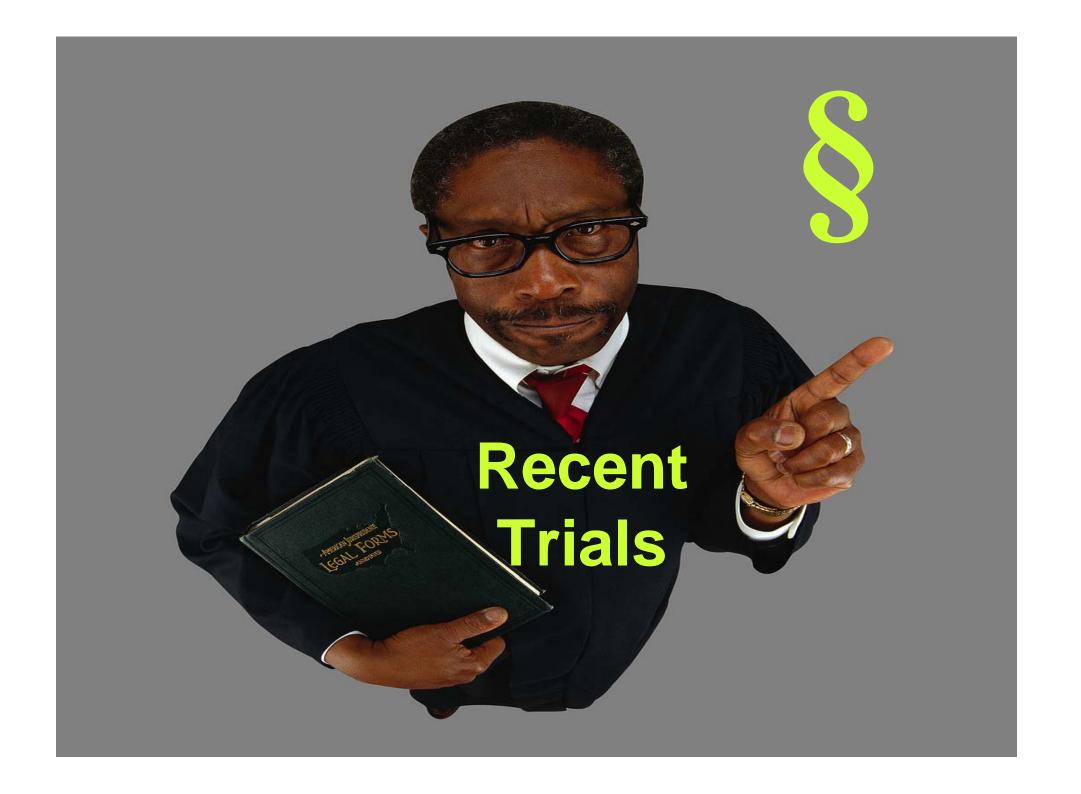
- according to the text of § 202c StGB: decisive is the requirement "objective purpose" of the computer program to commit a crime
- but problem: it is unclear how this objective purpose is to be determined
- particularly problematic in respect of the objective purpose are the "dual-use tools" which can be used legally and illegally at the same time
- the developer will probably rarely identify his software as a hacker tool
- a judge can define the objective purpose only with the help of experts
- even experts face great difficulties to define the doubtless objective purpose

objective purpose

- a supervisory authority which defines the objective purpose of computer programs does not exist
- regularly only the specific user can determine the specific purpose of the programme in use by his acting
- the objective purpose is unsuitable to differ general programming (securitiy tools) from hacker tools
- so far there is a lack of court decisions, so there are no ruling principles
- therefore only case-by-case judgments are possible with the risk of disposal

negative consequences

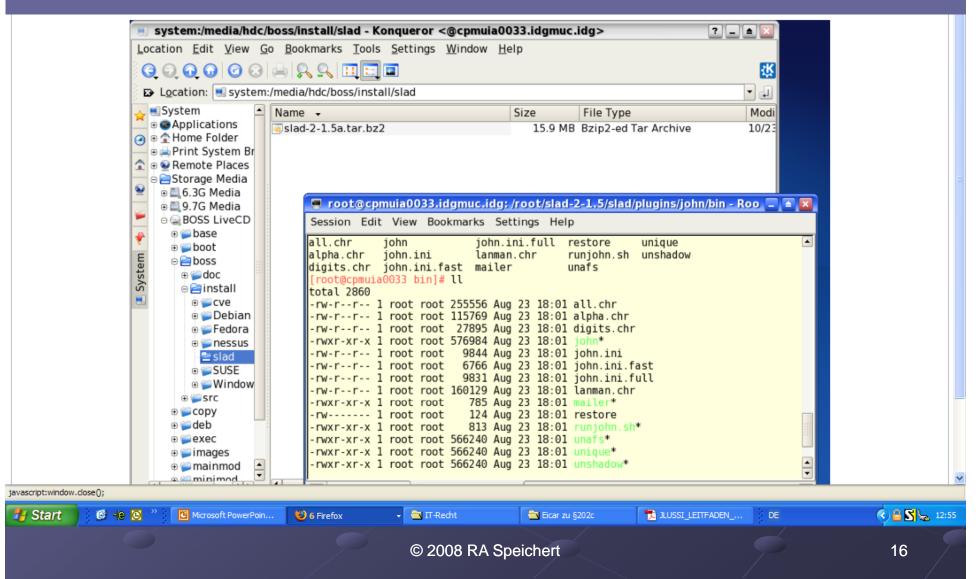
- risk of criminalization of security software
- many IT officers and IT service provider own programs acc. § 202c StGB
- to perform realistic penetration tests in IT systems
- this leads to uncertainty regarding the IT managers
- so maybe in the consequence required security action is omitted
- the real criminals with intention to commit computer crimes will not be prevented because they have worse plans
- opportunities for a reasonable limitation of possible criminal breaches are needed



criminal complaint against BSI

- editorial office of the online magazine "Tec-Channel" reported an offence to the prosecution at 14
 September 2007 against the "Federal Office for Security in Information Technology" (BSI)
- allegation: direct link to an offerer who has provided password crackers on the website
- but: Prosecution Bonn has stopped the investigations
- reasons: regarding its tasks BSI is lacking intention to violate the law according to § 202 c StGB

Hackertool BSI



constitutional complaint

- the IT security service provider "Visukom" has brought in an constitutional complaint to the Federal Constitutional Court against § 202c StGB
- reasons for constitutional offence:
 - the vague wording of § 202c StGB may violate the sufficient certainty
 - which is required for penal law according to Article 103
 Paragraph 2 GG (Grundgesetz Basic Law)
- the decision is not yet available



interim summary

- the testing of networks with computer programs for IT security reasons is imperative
- hacker tools can not be devided in good or evil by objective criteria
- due to the lack of legal certainty there is a danger of arbitrariness

reasonable limitation

- the lawmaker acknowledges in different public statements that
 - the testing of networks for IT security reasons is imperative
 - that the activity of IT security department and service provider mustn't be disturbed
- therefore reasonable limitation is necessary
- intention (=willful action) in respect of the future computer crime is required
 - according to the legislative reasons of the lawmaker
 - also according to the reasons of the Prosecution Bonn
- thereby the lawmaker aims to limit the application of § 202c StGB in a reasonable way

limitation by intention

- regarding the text of § 202c StGB a preparing act for committing a cybercrime is the decisive criteria
- that means an objective criteria
- nevertheless the lawmaker decides to use the subjective criteria "intention" to limit the application
- therefore § 202c StGB is only applicable if the actor intends to prepare a future cybercrime with his activity concerning the software tool
- therefore the illegality is deleted in the case of
 - explicit work instructions for IT officers
 - explicit agreement with service providers
- effect: unauthorised activity concerning the used software tools is not possible

suggested solutions

- explicit confirmation (contract clause)
 - which determines the use of specific software tools
 - in written form
 - granted by the employer or supervisor
 - to hedge the IT officers resp. service providers
- global confirmation/agreement for the entire contract of labor or service should be sufficient, but more details grant always more legal certainty
- only then gains the contractor or employee the necessary flexibility for risk analysis in the IT environment, without constantly fear of criminal actions
- advisable is a complete documentation which demonstrates that the contractor or employee remains in the limits of his authority

suggested solutions

- process descriptions make sense
 - regarding regular risk analysis
 - which guide contractors or employees legally for their activities
- no transfer of hacker tool to a third party, but only to known reliable partner, no indefinite audience
- safe storage of hacker tools so that no unauthorized access
- Documentation for the procurement or production of hacker tools which proves that no malicious intent is involved
- future prospects no counterproductive law, security vulnerability

Horst Speichert

e|s|b Rechtsanwälte Stuttgart

Attorney
Assistant Professor at
Stuttgart University
Data Protection Officer

- •IT Law
- Data Protection Law
- IT Security Law
- Media Law
- software contracts
- privacy agreements

E-Mail: horst@speichert.de

Internet: http://www.kanzlei.de

http://www.speichert.de