

Handle with care – but don't panic

Criminalisation of hacker tools in German criminal law and its effect on IT security professionals

Implementation of § 202c StGB

§ 202c StGB (StGB = Strafgesetzbuch, German Criminal Code) has been implemented by the 41st amendment to the Criminal Code (41. StrÄndG) and is in effect as of August 11, 2007. The 41. StrÄndG also amended §§ 202a, 202b, 303a and 303b StGB, which in substance criminalise illegal access to, and interception and interference of data and sabotage of computer systems and so make up the core computer crimes. § 202c criminalises the preparation of those computer crimes, as committed by the production, procurement or distribution of hacker tools. § 202c is Germany's transposition of Article 6 of the Council of Europe's Convention on Cybercrime, but the express exception for IT security tests, as in Article 6 (2) of the Convention, has not been transposed. Therefore, there is legal uncertainty among IT security professionals and concern about possible criminal proceedings.

These concerns are not without any reason, because Article 6 (2) was not transposed into the wording of § 202c and the German legislation could not be based on a constant legal practise, as there is no relevant higher jurisdiction about long existing similar preparation crimes (i.e. devices for counterfeit of banknotes or passports). Nevertheless, the risks of acting criminal can be minimised by complying with a few guidelines. So, in summary, there is no reason for panic, but hacker tools should be handled with care.

Avoid the use of hacker tools

§ 202c names two classes of hacker tools: Passwords (etc.) on the one hand and, on the other hand, computer programs that are primarily designed for committing computer crimes (§§ 202a, 202b, 303a, 303b). This is determined by an "objective intended purpose", which is the purpose that would become obvious to a neutral and competent person. Therefore, IT security tools that are commonly recognised are not hacker tools, even not if the tools can also be used with bad intent (dual use tools). On the other hand, malware and exploits are in the scope of § 202c, as the objective purpose of those programs is harmful, even though those tools can also be used for testing.

Also, sharing information in "human language" is not a crime; descriptions of algorithms and procedures can be legally distributed among IT security professionals. Therefore, common IT security tools and

descriptions in human language should be used preferably, if possible.

Get an explicit authorisation

If a hacker tool has to be used, an explicit authorisation is needed for justification. But, in German criminal law, § 202c protects against abstract endangerments already. When a crime is only prepared, there is no effect on any intended victim's individual rights. Therefore, a consent to the acts of § 202c *as such* is legally impossible.

Nevertheless, § 202c requires the preparation act to be promotive for an intended computer crime (§§ 202a, 202b, 303a, 303b). A justification by consent in terms of those sections is possible; if there is such consent, there cannot be any intent of committing a computer crime, and therefore, the preparation is legal. The authorisation has to be issued by a person with respective authority or procuration; if corporate computer systems may be used by staff for private use, the works council should also be involved.

Journalise and secure the usage

To be able to come up against any criminal proceedings, the procuration (including free downloads) and the intended use of hacker tools should be journalised as well as the actual use; the journal should be permanent and inalterable. Furthermore, unauthorised use of hacker tools should be avoided by secure storage and file access permissions.

There is no – and has never been – a way to prevent prosecutors from being overeager. But, by complying to this guidelines, IT security professionals can continue doing their jobs without worry.

Situation in other countries

The Cybercrime Convention has been signed by 43 member and observer states of the Council of Europe, including all EU member states, Japan and the US. Although the transpositions into national criminal law can be unique, it is likely that analogue problems occur and similar measures have to be taken by IT security professionals.

A detailed statement by the author (in German) can be downloaded at http://www.eicar.org/press/infomaterial/JLUSSI_LEITFADEN_web.pdf