

New German cybercrime law threatens IT industry

During this year's summer break a new set of rules entered into force on August 11th, 2007 aiming to ban certain activities of hacking and other cybercrimes in Germany. The laws under which the production and distribution of software capable to spy out or intercept data is punishable have tightened considerably.

The legislative procedure amending the German Criminal Code ("GCC") faced strong opposition not only by experts from the IT industry but also by lawyers. These experts criticized among other things the danger of criminalizing the daily work of network administrators or IT security advisers when analysing a network or computer environment they would like to protect as well as the software distributors. As a consequence all dual use software tools need to be questioned.

One provision of the revised criminal code in particular has attracted much of the criticism. Section 202c GCC determines that, *inter alia*, the production and distribution of computer programs which are able to spy-out or intercept data as well as the making available of such programs to oneself or to others can be prosecuted..

It is noteworthy that by criminalizing "making available to oneself" such information or programs, in fact, even the possession of said software is punishable.

In particular, the following activities or programs are critical and might, *inter alia*, be considered illegal pursuant to the new legislation:

- Password scanning – Applied to test the security of passwords, password scanners can also be used to find out passwords of third parties and to abuse them.
- Port scanning – Administrators can find open ports in networks and close them by using port scanning software. Hackers could also use this information and launch their illegal attacks at these ports.
- Network sniffing – Network sniffers control the whole traffic on a network card. They diagnose errors and enable fixing. These programs can also record all traffic or sensitive data. Attackers, on the other hand, can use such software to infiltrate malware.
- Remote maintenance systems – Such systems enable remote maintenance and remote control of a computer system. Helpdesk applications, for instance, are a legal method to use such software; however, remote control can also be used for illegal purposes.

Once faced by prosecution, the requirements for a defence are rather unclear. Of course, offences according to sec. 202c GCC must be intentional. However, contingent intent (*dolus eventualis*) is sufficient to establish the criminal nature. Hence, for IT security advisers it will be difficult to argue that they did not know that a certain program, e.g. a port scanner, could also be used for the infiltration of malicious software.

The afore described revision of the German Criminal Code is currently under scrutiny by the German Constitutional Court (*Bundesverfassungsgericht*) on grounds of violation of the right of freedom of profession. Thus, it remains to be seen whether the Federal Constitutional Court is more open to the criticism raised by IT and legal circles or whether it turns a blind eye to the experts' arguments like the legislator did after hearings had taken place in the *Bundestag's* legal committee. The court could affirm the provisions or declare them void. However, until such decision is rendered it will be necessary for the IT businesses affected by these laws to work out individual solutions – based on, *inter alia*, the place of business, the software tools concerned, and the distribution methods used.

Since the amendments to the German Criminal Code go back to the European Council Convention on Cybercrime, signed at Budapest on 23 November 2001, and the EU Council Framework Decision of 24 February 2005 (2005/222/JHA, Official Journal no. L 69/67) on attacks against information systems, similar legislative initiatives are to be expected in other (not only EU) countries as well. Hopefully, they do not overshoot the mark, too.

For further information please contact:

Dr. Alexander Niethammer
Senior Associate
Heisse Kursawe Eversheds, Munich
Email: a.niethammer@heisse-kursawe.com

Michael Tegethoff
Associate
Heisse Kursawe Eversheds, Munich
Email: m.tegethoff@heisse-kursawe.com