Cyber security
3 QUESTIONS TO... RALF BENZMÜLLER, HEAD OF G DATA SECURITYLABS

1. Mr Benzmüller, what current developments are there in relation to virus protection and cyber crime?
Adware and potentially unwanted programs (PUP) are the most widely distributed types. They account for around a third of all infections. Displaying advertising banners is lucrative for criminals, but it is not regarded as malicious by the majority of users. This makes it a profitable business.

The most conspicuous change is in the area of ransomware. More and more varieties of Crypto-Trojans are appearing and the procedure varies. There is ransomware that encrypts every possible file in the personal environment. Other variants are aimed at companies and distribute themselves on the local network. Some encrypt the website and only enable users to access a page with a ransom note. Yet others encrypt access to the local network memory (aka NAS, Network Attached Storage). Or access to the Internet is disabled and a ransom is imposed.

A flourishing cyber crime economy has become established in the past 15 to 20 years, the turnover from which has long exceeded that of the drugs trade. The money obtained is invested in new attacks that are more and more frequently being planned and implemented professionally. Nowadays there is hardly a single aspect of our everyday lives where a computer is not used. The consequences of attacks are correspondingly more serious. Hence protection against attacks on computers is becoming more and more important for society.

2. What types of cyber crime can virus protection offer protection against?
Traditional virus protection is designed to detect automated attacks and fend them off, especially when they occur en masse. With its various components, virus protection software can protect against infections via traditional paths such as email, manipulated websites and via local networks and USB data media. Good virus protection software will prevent the computer becoming infected with adware or becoming part of a botnet and will stop sensitive data being lost. Special dynamic detection processes also offer protection against attacks via security holes and monitor online accounts during online banking.

Both, users of private computers and users in a business environment, are exposed to these risks. Other functions are important in companies, such as backups, patch management and mobile device management.

3. How can companies protect themselves from attacks most effectively, besides by using antivirus software?
Antivirus software is an important basic component of a malware protection concept. However, it is not sufficient for comprehensive protection from attacks. Virus protection is only effective if it is embedded into a full-fledged protection concept. This begins with access control to rooms and buildings and continues with the selection of the hardware, operating system and software. Furthermore there is the clean separation of network segments and the issuing of access permissions for users. Additional detection and protection technologies should be deployed for especially sensitive areas. The employees also play a particular role. No protection concept can be practically implemented without their cooperation. Hence it is essential to develop healthy security awareness among the staff through regular training.