Bundeskriminalamt

HERBST-TAGUNG 2013 BKA AUTUMN CONFERENCE

Cybercrime –

threat, intervention, defence

BKA Autumn Conference, 12 - 13 November 2013

Digital Threats

Abstract

Alexander Geschonneck

Partner and head of the Forensic Technology department of the KPMG AG auditing company in Berlin

The term "digital threats" covers numerous different threats, for example data espionage (cyber espionage), computer sabotage and violation of copyright law. In this context, an ICT system can be a target, a tool or both. Threats can exist for companies and authorities as well as for private individuals.

Digital threats are also relevant in the field of economic crime, the term used in this connection is e-crime. The latest e-crime survey by KPMG on losses caused to the German economy provides an overview from a commercial perspective.

According to this survey, a quarter of the 500 German companies questioned have been affected by e-crime in the past two years, with the threats increasingly being viewed as emerging from specific countries.

Prevention as a comprehensive measure to ward off internal and external threats

It must, however, not be disregarded that the perpetrators are often found in the immediate environment of the companies. Consequently, both internal and external threats have to be considered in the context of prevention.

In this connection, safeguarding against internal offenders must take account of an increasingly complex and networked environment of companies, including persons from their indirect surroundings such as staff of cloud computing or other outsourcing service providers or suppliers.

Carelessness as greatest weakness

It should also be noted that problems are not always caused by security vulnerabilities requiring sophisticated exploitation. In fact, companies still consider the carelessness of their staff as the greatest weakness with regard to e-crime.

Therefore, preventive measures should also comprise regular training and awareness-raising which can considerably reduce the probability of staff members accidentally causing IT security weaknesses. In this connection, security incident reporting within companies should also be improved since most cases are still reported on the basis of coincidence.

Evolution of threats

Once a desired protection level has been reached by means of appropriate preventive measures, this must not be regarded as a final achievement. In point of fact, the protection level can and will decrease in the future because existing threats will develop further and new ones will arise.

For instance, a professionalisation of the attacks and the tools involved can be observed. One business model is, for example, to create sophisticated attack tools and make them available to third parties for a fee. Even "ready-to-use" solutions are being offered as "cracking-as-a-service". The malware toolkit "Blackhole" serves as an example in this context.

Targeted attacks on companies and data stocks

The number of targeted attacks on companies and data stocks is also on the increase. Cracking is not the only method used in this context. Additionally, known methods of attack have been modified to facilitate targeted attacks.

In the form of "spear phishing", for example, the well-known phishing technique is turned into a targeted attack method. Methods of social engineering are used against selected persons, such as employees holding administration rights or members of a company's management ("whaling"). For the attackers this course of action promises greater success, profiling is often quite easy with the help of professional and private social networks. In comparison with sending thousands of phishing mails that are rejected by the security systems, such minimally invasive attacks allow the attackers to remain undetected for a longer time.

Development of new threats due to new technologies

New threats emerge from the increasing use of new technologies. Thus, mobile terminal devices become interesting targets as their performance increases. Functions like GPS tracking pave the way for new attack scenarios such as secret tracking of the users; the installation of Apps entails the risk of installing unwanted functions. There are smartphone platforms where most of the devices on the market using them are believed to have been successfully compromised.

In this regard, companies are particularly under threat when following the "bring-your-own-device" trend, i.e. permitting the use of private terminal devices within the company network to access sensitive data.

Adequate prevention as a competitive advantage

It can be stated that the number and intensity of digital threats continue to increase. Besides the evolution of existing threats, new ones are emerging - their impact cannot be sufficiently assessed yet because the technologies involved are so new. The perpetrators, who pursue great commercial interests, will keep trying to remain undetected for a long time.

For this reason, extensive prevention will grow into a competitive advantage for companies. Nevertheless, it is also indispensable that companies cooperate with each other, for instance with regard to the detection of attacks directed against specific industries. Successful attacks can incur considerable costs, including damage to a company's reputation.

In this context, prevention must not be restricted to implementing measures to identify attacks. Before damage is caused, it has to be checked whether a company is prepared for warding off and clearing up an active attack when detected. Since attacks (also successful ones) will be unavoidable, those companies that are able to respond adequately will succeed in the long run.