SUMMARY

FACTS AND FIGURES

In Austria the number of complaints involving cybercrime rose from 10,010 in 2015 to 13,103 in 2016, which is an increase by about 31 per cent. The number of cases requiring special technical knowhow has shown the biggest rise of over 55 percent.

The principal causes are
- the global spread of offenders, resources (servers, etc.), victims and money flows,
- the increasing use of the Darknet by criminals,
- the global spread of malicious software
- the lack of threat awareness
- the weaknesses of IT systems such as outstanding security updates

MEASURES

To counter the massive increase in ransomware, a special investigation team termed CLAVIS was set up in June 2016. It is composed of experts who centrally process all ransomware cases. In the field of IT forensics, new technological fields have been introduced and expanded, in particular vehicle forensics and multimedia forensics.

In order to improve police training, new programs were launched in 2016, focusing on IT investigators in the field. The project „CyberKids“ is aimed at empowering children of eight to twelve years to safely handle the Internet in its final phase [2018].

TRENDS

Ransomware continues to be at the top of criminal trends. There is an increasing emphasis on specific objectives and target groups such as personnel departments and small and medium-sized enterprises. Virtual currencies such as bitcoins are increasingly used by criminals to conceal their criminal proceeds and money flows from the investigative authorities. The Darknet has facilitated and accelerated the emergence of criminal service providers in the form of „cybercrime as a service“. Criminal tools make it possible for virtually everyone to execute, for instance, technically sophisticated cyberattacks. An growing threat is the shifting of conventional crime such as drug or arms trade to the Internet, in particular to the Darknet.

OUTLOOK

Cybercrime is a global phenomenon and no country can shield itself from its global developments. New technologies open up new targets for criminals. The Internet of things will be of particular relevance in this context. By 2020, some 20 billion devices are expected to be connected to the Internet in this way. Already today, 4.9 billion devices have a connection with the Internet according to an estimate by market researcher Gartner [www.gartner.com]. Most of these devices are unprotected against attacks. The DDoS attacks on the US company „DynDNS“ in the autumn of 2016, using the „Mirai-Botnet“, have gone to show the potential threat involved in the IOT – the Internet of Things.