Recommended action

- Physical separation between the company network and the Internet
- Guidelines how to handle e-mails
- Your points of contact in economic security
- Protection against malware
- Drawing up of emergency plans
- Backup management
- Restriction of access and rights of use
- Awareness training for staff and management

Your points of contact in economic security

Do not hesitate to contact us and make an appointment for confidential awareness talks

For additional information and your local contacts’ communication data, please visit the website

www.wirtschaftsschutz.info

Imprint
Publisher: BfV (German federal domestic intelligence service) for the community of the domestic intelligence services of the Federation and the federal states

Pictures: © vchalup - Fotolia.com
        © Nikolai Sorokin - Fotolia.com

DOI: March 2016
Threats emanating from electronic attacks

Due to ever more sophisticated technologies, electronic attacks have become a massive threat to IT systems, communication structures and data.

Viruses, worms, Trojans or powerful botnets are used for espionage and sabotage purposes. The originators of such attacks may be single individuals, criminal organisations, competitors, and even foreign states.

Possible methods of attack

- Distribution of malware by
  - infected websites
  - e-mails
  - USB Trojans
  - (spear) phishing
  - unprotected network accesses
- Leak of information by
  - keyloggers
  - interception of VoIP
  - bluetooth and WLAN hacking
  - Trojans
  - bugging devices
- Hardware manipulation
- Exploitation of software vulnerabilities (exploits)

Electronic attacks with e-mails

The purpose of this classic form of attack is to tempt the recipient to open the infected e-mails/attached files (phishing). False senders and the inclusion of personal data serve to allay doubts (spear phishing).

For instance, through a false sender address an e-mail can give the impression of coming from a real business partner. Through the use of personalised contents, the recipient shall be pressurised into opening the attached file or link, resulting in the hidden malware being installed and started unnoticed.

Then the malware independently contacts the attacker’s provider via the Internet and gets further commands for espionage or sabotage.

APT (Advanced Persistent Threat)

A targeted, complex and long-term, mostly very elaborate attack to infiltrate computer networks.

Exemplary modus operandi

- Comprehensive investigations into companies and individuals (*)
- Planning the electronic attack by considering the investigation results (*)
- Carrying out the attack
  - infecting the computer network with viruses/Trojans
  - establishing a connection with the attacker
  - exploring the network
  - maximising the rights of access
  - obtaining and using further information through repeating and modifying this kind of attack

* cf. leaflet “Social Engineering”