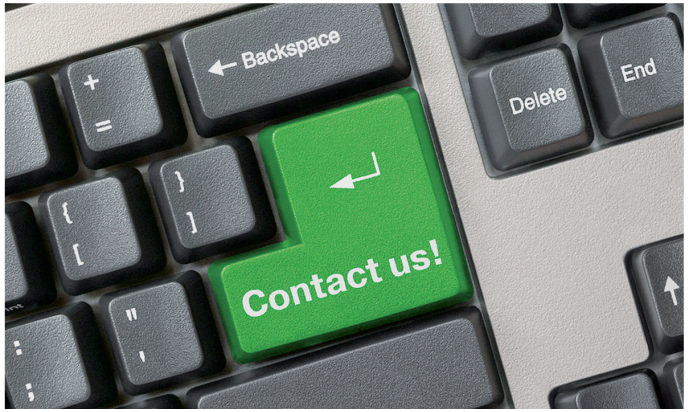
"Only a physical separation of the company network from the Internet can provide ideal protection against electronic attacks."

How to protect yourself against such attacks?

Have you got, for example:

- guidelines for your employees how to handle emails?
- protection against malware?
- emergency plans?
- access and use restrictions?

Please contact us and make an appointment for confidential awareness talks.



Your points of contact

www.verfassungsschutz.de

www.verfassungsschutz-bw.de

www.verfassungsschutz.bayern.de

www.verfassungsschutz-berlin.de

www.verfassungsschutz-brandenburg.de

www.verfassungsschutz.bremen.de

www.hamburg.de/verfassungsschutz

www.verfassungsschutz.hessen.de

www.verfassungsschutz-mv.de

www.verfassungsschutz.niedersachsen.de

www.mik.nrw.de/verfassungsschutz

www.verfassungsschutz.rlp.de

www.saarland.de/verfassungsschutz.htm

www.verfassungsschutz.sachsen.de

www.mi.sachsen-anhalt.de/verfassungsschutz

www.verfassungsschutz.schleswig-holstein.de

www.thueringen.de/de/verfassungsschutz

Imprint:	BfV (German federal domestic intelligence service) for the domestic intelligence services of the Federation and the federal states
Pictures:	© ktsdesign - Fotolia.com © Fotolia.com © Nikolai Sorokin - Fotolia.com
Print:	INFOX GmbH&Co. Informationslogistik KG, Troisdorf
DOI:	August 2010

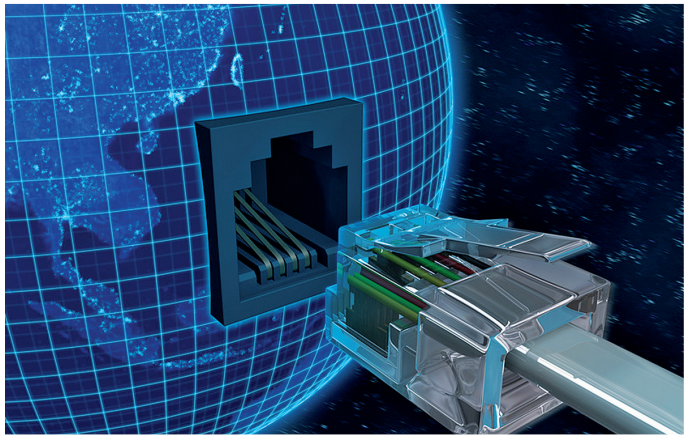
Domestic intelligence service

Federal Republic of Germany
Federal States

Electronic Attacks on Information and Communication Technologies

Domestic intelligence service: neutral free of charge confidential

"The connection of a company's network to the Internet is what every attacker is dreaming of."



The threats emanating from electronic attacks have been on the rise for years. And due to ever more sophisticated techniques, they have become a massive threat to IT systems and communication structures of commercial, governmental, and private users.
Viruses, worms, Trojans or whole botnets are used for attacks serving espionage as well as sabotage purposes. The originators of such attacks may be single individuals, political or criminal associations, competitors, and even foreign states. Each year, German companies alone suffer losses amounting to sums beyond ten million euros.

Examples for methods of attack:

- malware in emails
- infected websites
- phishing
- hacking with USB Trojans
- keylogger
- interception of VoIP
- bluetooth and WLAN hacking
- manipulation of hardware

"The worldwide web allows everybody everywhere in the world to get an ever faster access to sensitive information."

"It takes much less effort to launch an electronic attack than to prevent it."

Electronic attacks with emails:

Sending emails with infected attached files to specifically selected recipients is one method of attack that is used quite often.
The purpose of the attack is to tempt the "victim" to open the attached file.
Interesting topics and false information on a supposedly trustworthy sender are used to allay doubts.
The malware "introduced" with the email has a hardly to be recognised signature, and as soon as the email attachment is opened, it will be installed and started without being noticed.
The programme then independently contacts the originator via the Internet and gets further commands for espionage or sabotage.
The system regards the established connection as safe and accepts it.

"At the moment, there is no stand-alone security product offering sufficient protection against specifically adjusted malware."

BSI (Federal Office for Information Security)