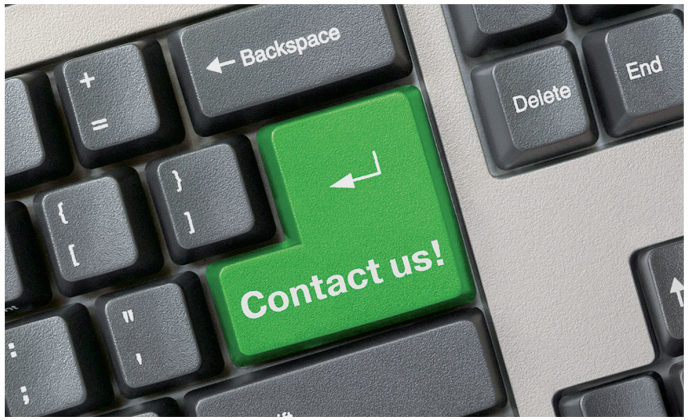
Recommendations:

- Be careful with the disclosure of personal data on the Internet.
- Pay attention to the terms and conditions of the respective social network. With your registration, you possibly accept that the operator can further use your personal data or pictures without any restrictions, even when you delete your profile.
- Include only little freely accessible information for "unknown users" in your profile. Configure the access settings before creating a profile.
- Avoid giving details about your current employer or talk to your company first.
- You as the employer: Add a "social network passage" to your internal security regulations and raise your employees' awareness regarding the handling of company-related information.



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 intelligence services of the Federation and the federal states

Pictures: © Nmedia - 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

Unlimited openness – "social networks" on the Internet

Social networks – a natural means of communication

The Web 2.0 has considerably changed many people's everyday behaviour. Social networks as modern communication platforms enjoy an enormous popularity. All over the world, millions of people exchange information on their hobbies, common interests, or even work aspects via networks such as Facebook, MySpace, Xing, werkennt-wen or StudiVZ.

A security risk for your own company?

Yes, as many users of such platforms disclose sensitive information without being aware of it. Apart from personal data, their information often contains details about their employers and their positions in their companies.

Taken individually, this information is harmless, but combined, it may become the company's weak point and serve as a point for attack.

The more information is disclosed, the higher are an attacker's chances of success.

Criminal single perpetrators, professional intelligence monger and competing companies collect specific information about company members. Even foreign intelligence services know that social networks as an open source may be a real treasure trove.

People search engines scan profile accounts. That way, comprehensive personal profiles are created with "one click".

Possible consequences of unlimited openness

Attackers misuse this information e.g. for:

- stealing data or identities
- spam and phishing attacks
- social engineering
- illegal trade in data

Foreign intelligence services use this openness for contacting and approaching staff members as sources of information.

This cannot only have negative consequences for staff members as the ones being responsible, but also for companies themselves. Apart from financial losses, damage to the companies' image may also be a result.