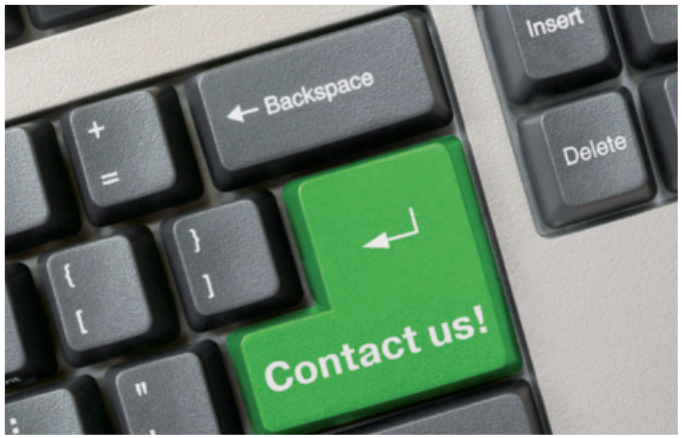
Recommended action

- Be careful when disclosing personal data on the Internet
- Pay attention to terms and conditions. You possibly accept that your data can be extensively used
- Check the rights of access. Include only little freely accessible information for "unknown users" in your profile
- You as the employer: Add a "Social Media" passage to your internal security regulations
- Raise your employees' awareness regarding the handling of company-related information

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



Your points of contact in economic security

initiative wirtschaftsschutz

Protecting values in a concerted effort

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: © Nmedia - Fotolia.com
© ccvision.de
© buchachon - Fotolia.com
© Nikolai Sorokin - Fotolia.com

DOI: March 2016

Domestic intelligence service

Federal Republic of Germany
Federal States

Economic Security

Risks posed by social networks

Social Media

Prevention through Dialogue and Information

Social Media – a natural means of communication

The Internet has considerably changed many people's everyday behaviour. Social networks as modern communication platforms have become enormously popular. All over the world, millions of people exchange information on their hobbies, common interests, or even work aspects via networks such as Facebook or Xing.

A security risk for your company?

Yes, since 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.

By analysing and combining such information, attackers can identify and exploit points for attack within the company.

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

Criminal single perpetrators, professional intelligence mongers and competing companies collect specific information about company members. Even foreign intelligence services know that social networks can be a real treasure trove.

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

Foreign intelligence services use this openness to contact and to approach staff members as sources of information.

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

Possible negative consequences

Attackers misuse this information e.g. for:

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