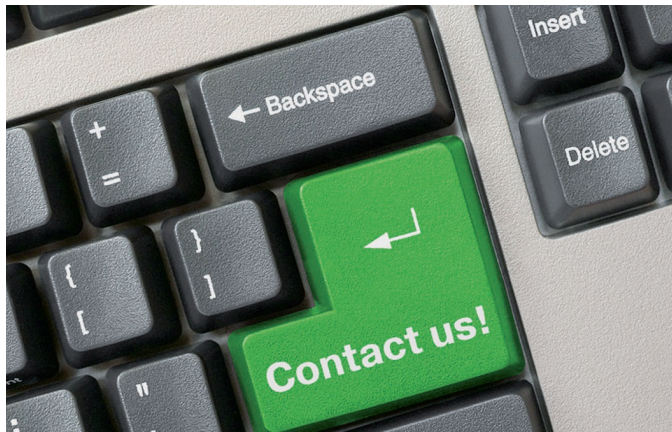


Empfehlungen

- ▶ Üben Sie Zurückhaltung im Umgang mit der Preisgabe persönlicher Daten im Internet
- ▶ Beachten Sie die AGB. Sie stimmen ggf. einer weitreichenden Verwendung Ihrer Daten zu
- ▶ Überprüfen Sie die Zugriffsrechte. Stellen Sie nur wenige sichtbare Informationen für „Fremde“ im Profil bereit
- ▶ Erweitern Sie als Arbeitgeber Ihre internen Sicherheitsbestimmungen um den Punkt „Social Media“
- ▶ Sensibilisieren Sie Ihre Mitarbeiter hinsichtlich des Umgangs mit unternehmensbezogenen Informationen

Sprechen Sie uns an und vereinbaren Sie einen Termin für ein vertrauliches Sensibilisierungsgespräch



Ihre Ansprechpartner im Wirtschaftsschutz

Ministerium für Inneres und Kommunales
des Landes Nordrhein-Westfalen



Wirtschaftsschutz

Ministerium für Inneres und Kommunales NRW
Abteilung Verfassungsschutz
Postfach 10 30 13
40021 Düsseldorf

Telefon: 0211 / 871-2899
Fax: 0211 / 871-2980
E-Mail: wirtschaftsschutz@mik1.nrw.de
Internet: www.mik.nrw.de/wirtschaftsschutz



Gemeinsam. Werte. Schützen.

Dort finden Sie weitere Informationen sowie die Kontaktdaten Ihrer örtlichen Ansprechpartner.



www.wirtschaftsschutz.info

Impressum

Herausgeber: Bundesamt für Verfassungsschutz für den Verfassungsschutzverbund

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

Stand: März 2016

Verfassungsschutz



**Bund
Länder**

Wirtschaftsschutz

**Risiken durch
soziale Netzwerke**

Social Media

Social Media – ein selbstverständliches Kommunikationsmittel

Das Internet hat das Alltagsverhalten vieler Menschen nachhaltig verändert. Soziale Netzwerke erfreuen sich als moderne Kommunikationsplattform enormer Beliebtheit. Weltweit tauschen sich Millionen Nutzer in Netzwerken wie Facebook oder Xing über ihre Hobbys, gemeinsame Interessen oder auch berufliche Aspekte aus.



Ein Sicherheitsrisiko für Ihr Unternehmen?

Ja, denn viele Nutzer dieser Plattformen offenbaren unbewusst sensible Informationen. Preisgegeben werden neben persönlichen Daten oft Angaben zum Arbeitgeber und der Funktion im Unternehmen.

Durch Auswertung und Kombination dieser Informationen werden Angriffspunkte im Unternehmen aufgedeckt und ausgenutzt.

Je mehr offenbart wird, desto höher sind die Erfolgschancen für einen Angreifer.

Kriminelle Einzeltäter, professionelle Nachrichtenhändler und Konkurrenzunternehmen sammeln gezielt Informationen über Firmenmitarbeiter. Auch für fremde Nachrichtendienste stellen soziale Netzwerke eine wahre Fundgrube dar.

Personensuchmaschinen scannen die Profilseiten. Umfassende Persönlichkeitsprofile werden so mit „einem Klick“ zusammengestellt.



Fremde Nachrichtendienste nutzen diese Offenheit zur Kontaktaufnahme und Anwerbung eines Mitarbeiters als Informationsquelle.

Dies kann nicht nur nachteilige Folgen für den Mitarbeiter, sondern auch für das Unternehmen haben. Neben finanziellen Schäden droht auch ein Imageverlust.

Mögliche negative Folgen

Angreifer missbrauchen diese Informationen zum Beispiel für:

- Daten- oder Identitätsdiebstahl
- Spam- und Phishing-Attacken
- Social Engineering
- Illegalen Datenhandel

