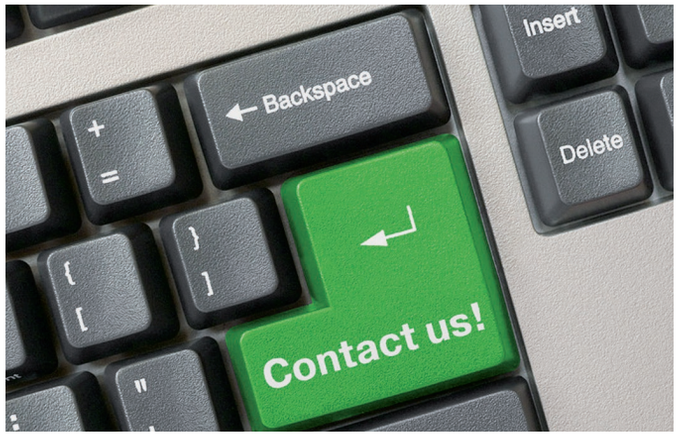
Begleitende Maßnahmen

- Preisgabe persönlicher Informationen nur an Berechtigte
- Generell Vorsicht bei E-Mails und dem öffnen von Dateianhängen
- Zurückhaltung beim Umgang mit sozialen Netzwerken
- Telefonische Bestätigung eines Kontaktes bei Zweifeln an dessen Echtheit

Binden Sie alle Beschäftigten ein, da andernfalls deren Kenntnisse und Insiderinformationen ausgenutzt werden können.

Die frühzeitige Einbeziehung erhöht das Verständnis und die Akzeptanz für neue Schutzmaßnahmen.

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

initiative 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: © XtravaganT - Fotolia.com
© ViewApart - Fotolia.com
© Nikolai Sorokin - Fotolia.com

Stand: März 2016

Verfassungsschutz

Bund Länder

Wirtschaftsschutz

Informations-beschaffung durch soziale Manipulation

Social Engineering

Prävention durch Dialog und Information

Was ist „Social Engineering“?

Von Social Engineering spricht man immer dann, wenn ein Angreifer versucht, menschliche Schwächen auszunutzen, um an bestimmte Informationen zu kommen. Hierbei ist er bestrebt, über scheinbar belanglose an schützenswerte Daten zu gelangen. Diese extrem effiziente Methode dient dazu, Schwachstellen in Unternehmen zu identifizieren, um sie für Angriffe zu missbrauchen.

In diesem Kontext werden grundsätzlich positive Eigenschaften wie Hilfsbereitschaft, Kundenfreundlichkeit, Dankbarkeit, aber auch Stolz auf die Arbeit bzw. das Unternehmen manipulativ ausgenutzt.

Fallbeispiele

- Ein Mitarbeiter plaudert beim Restaurantbesuch vertrauliche Informationen über eine aktuelle technische Entwicklung aus
- Einem Anrufer, der sich als Niederlassungsleiter ausgibt, werden persönliche Daten eines Kollegen herausgegeben
- Ein Angreifer gibt sich als Journalist aus und entlockt dem Vorstandssekretariat wichtige strategische Zukunftspläne des Unternehmens
- Ein Mitarbeiter gibt in sozialen Netzwerken private Informationen und Interessen preis, die eine gute Gesprächsbasis für einen Angriff bilden
- Ein Außenstehender ruft beim Helpdesk an und gibt sich als Mitarbeiter aus, der sein Passwort vergessen hat. Er bittet darum, dieses zurückzusetzen
- Ein Angreifer weckt die Neugierde eines Mitarbeiters durch die geschickte Wahl der Betreffzeile und des Absenders in einer E-Mail

Sensibilisieren Sie regelmäßig Ihre Mitarbeiter!

Begleitende Maßnahmen

- Vertrauliche Gespräche nur in geschützter Atmosphäre führen. Informationsverlust kann an Orten wie Messen, Gaststätten, öffentlichen Verkehrsmitteln o.ä. nicht ausgeschlossen werden
- Betriebsinterna nicht an Unternehmensfremde weitergeben
- Sichtbares Tragen von Firmen-/Besucherausweisen