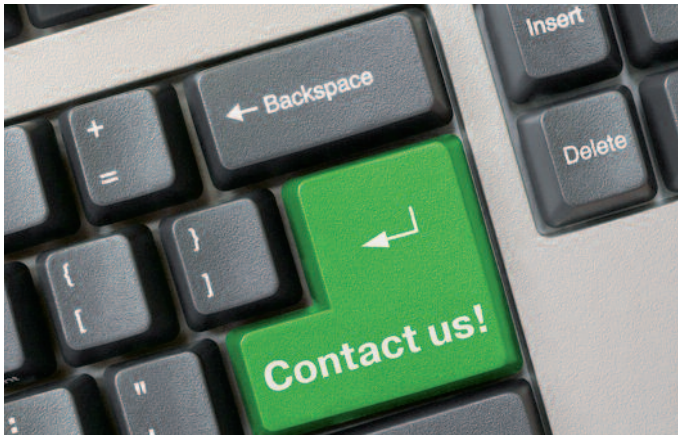
Empfehlungen

- Physikalische Trennung zwischen Unternehmensnetzwerk und Internet
- Regelungen im Umgang mit E-Mails
- Einsatz von Malwareschutz
- Erstellung von Notfallplänen
- Backup-Management
- Einschränkung von Zugriffs- und Nutzungsrechten
- Awareness-Schulungen für Mitarbeiter und Management

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



Ihre Ansprechpartner im 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:	© vchalup - Fotolia.com © Nikolai Sorokin - Fotolia.com
Stand:	März 2016

Verfassungsschutz

Bund Länder

Wirtschaftsschutz

Gefahren für Informations- und Kommunikationstechnik

Elektronische Angriffe

Prävention durch Dialog und Information

Gefahren durch Elektronische Angriffe

Immer ausgereiftere Angriffstechniken sind eine massive Bedrohung für IT-Systeme, Kommunikationsstrukturen und Daten geworden.

Viren, Würmer, Trojaner oder leistungsstarke Botnetze werden für Spionage- und Sabotagezwecke genutzt. Urheber können Einzelpersonen, kriminelle Organisationen, Konkurrenten und auch fremde Staaten sein.

Mögliche Angriffsmethoden

- Verbreitung von Schadprogrammen durch
  - Infizierte Webseiten
  - E-Mails
  - Trojaner auf USB-Sticks
  - (Spear-) Phishing
  - ungeschützte Netzwerkzugänge
- Informationsabfluss durch
  - Einsatz von Keyloggern
  - Abhören von VoIP
  - Bluetooth- und WLAN-Hacking
  - Trojaner
  - ‚Wanzen'
- Hardwaremanipulationen
- Ausnutzen von Softwareschwachstellen (Exploits)

Elektronische Angriffe mittels E-Mail

Ziel dieser klassischen Angriffsform ist, den Empfänger zum Öffnen der infizierten E-Mails/Anhänge zu verleiten (Phishing). Gefälschte Absender und die Einbeziehung persönlicher Daten dienen dazu, Bedenken zu reduzieren (Spear-Phishing).

So kann eine E-Mail durch eine gefälschte Absenderadresse den Anschein erwecken, von einem realen Geschäftspartner zu kommen. Durch Verwendung personalisierter Inhalte soll Handlungsdruck erzeugt und der Empfänger zum Öffnen eines Anhanges oder Links bewegt werden. Dadurch wird die darin verborgene Schadsoftware unbemerkt installiert und gestartet.

Das Schadprogramm stellt danach selbstständig eine Onlineverbindung mit dem Server des Angreifers her und erhält so weitere Befehle zur Spionage oder Sabotage.

Eine auf diesem Wege von innen hergestellte Verbindung wird vom System i.d.R. als unbedenklich akzeptiert und zugelassen.

APT (Advanced Persistent Threat)

Zielgerichteter, komplexer und langfristig angelegter, meist mit sehr großem Aufwand durchgeführter Angriff, um in Rechnernetze einzudringen.

Beispielhafte Vorgehensweise

- Umfangreiche Recherche zu Unternehmen und Personen (*)
- Planung des Elektronischen Angriffs unter Einbeziehung der Rechercheergebnisse (*)
- Durchführung des Angriffs
  - Einschleusen von Viren/Trojanern
  - Verbindung zum Angreifer
  - Erkundung des Netzwerkes
  - Maximierung der Zugriffsrechte
  - Erlangen und Verwenden weiterer Informationen durch Wiederholung und Modifizierung dieser Angriffsart

* siehe Flyer „Social Engineering"