



IT-Sicherheit und Informationssicherheit in der Wirtschaft

Informations- und Beratungs-
angebot des Bayerischen Landes-
amts für Verfassungsschutz

Stand: Februar/2009

Schutz Ihrer IT

Das Bayerische Landesamt für
Verfassungsschutz bietet Ihnen an:

- Sensibilisierung von Management
und Mitarbeitern für die Belange
der Informationsschutzes
- Vorträge und Präsentationen im
Unternehmen zu allen Aspekten
der IT-Sicherheit
- Aufklärung über spezielle Risiken
und Schutzmaßnahmen bei
Auslandsreisen
- Erläuterung konkreter IT-Risiken
und Bedrohungsszenarien
- Individuelle Gefährdungs- und
Schwachstellenanalyse
- Beratung bei Konzeption und
Optimierung Ihrer Maßnahmen
zur Informationssicherheit
- Aufbau einer langfristigen Sicher-
heitspartnerschaft
- Absolut vertrauliche Behandlung
aller Informationen

**Alle Informations- und Beratungsangebote
sind kostenlos**

Kontakt

Ihr Ansprechpartner für IT-Sicherheit
und Informationssicherheit:

Dr. Michael Triller
Tel.: 089 / 31201 - 193
E-Mail: iswi@lfv.bayern.de

Ihr Kontakt für allgemeine Fragen
des Wirtschaftsschutzes:

Tel.: 089 / 31201 - 500
E-Mail: wirtschaftsschutz@lfv.bayern.de

Zusätzliche Informationen und
Publikationen zum Download auf der
Webseite des Bayerischen Landes-
amts für Verfassungsschutz:
www.verfassungsschutz.bayern.de

Herausgeber:

**Bayerisches Landesamt für
Verfassungsschutz
Knorrstr. 139
80937 München
Telefon: 089 / 31201-0**



Wirtschaftsspionage und IT

Die Bedrohung ist konkret:

- Viele Staaten beauftragen ihre Nachrichtendienste mit Wirtschaftsspionage (Hauptakteure sind China und Russland)
 - Innovative Technologie steht im Fokus (Luft- und Raumfahrt, Maschinen- und Anlagenbau, Telekommunikation, IT, ...)
 - Ausgeforscht werden technische und strategische Informationen
- Gezielte IT-Angriffe mit Spionagehintergrund nehmen zu

Sind Sie darauf vorbereitet?

- Nachrichtendienstliche Aktivitäten werden unterschätzt oder negiert
 - Das eigene Know-how wird als nicht gefährdet gesehen
 - Ganzheitliche Schutzkonzepte unter Einbeziehung der IT fehlen
- IT-Schwachstellen erleichtern den Abfluss von sensiblem Know-how

IT-Angriffsszenarien

Angriffe auf mobile IT-Systeme (Notebooks, PDAs, Handys)

- Vielfache Manipulationsmöglichkeiten (Einsatz als „Wanze“, Einspielen von Schadsoftware, Erstellen von Bewegungsprofilen, ...)
- Abhören drahtloser Schnittstellen (WLAN, Bluetooth)
- Diebstahl von Geräten oder Datenträgern

Angriffe auf Unternehmensnetze

- Attacken gegen Firewalls und Webserver (Hacking, DoS, ...)
- Abhören von drahtlosen Netzwerken (WLAN)
- Flächendeckende Kommunikationsüberwachung im Ausland

Angriffe durch Innentäter (Mitarbeiter, Dienstleister, Besucher)

- Zugriff auf interne Daten (direkter Zugriff, Keylogger, USB-Sticks, ...)
- Manipulation von Sicherheitseinrichtungen
- Ausnutzen interner Schwachstellen
- Mangelndes Sicherheitsbewusstsein und unzureichende Schulung der Mitarbeiter

Gezielte Trojaner-Angriffe mit gefälschten E-Mails

- Maßgeschneiderte Spionagesoftware im Anhang
- Firewalls und Virens Scanner bieten keinen Schutz