

## Sicherheitsmaßnahmen für IT-Systeme

Die folgenden Standardsicherheitsmaßnahmen gelten für typische IT-Systeme mit „normalem“ Schutzbedarf. Dies betrifft ca. 90 Prozent aller privaten und kommerziellen Anwender:

- Alle Standardsicherungen der benutzen Software aktivieren.
- Zutritt (abschließbare Räume), Zugang (Passwörter für Netze und einzelne PCs) und Zugriff (Passwörter für Dateien) für jeden Rechner kontrollieren, zum allgemeinen Datenschutz und Schutz vor Sabotage etc.
- Firewalls und Virenschutzprogramme zur Abwehr von Hackern, Viren, Trojanischen Pferden etc. installieren und regelmäßig aktualisieren.
- Daten regelmäßig sichern.

## Weitere Sicherheitsmaßnahmen für Unternehmen

- Typische Gefährdungen und Risiken erfassen: Wer weiß, welche Gefahren drohen, ist motiviert, sich dagegen zu wehren.
- Jede Software protokolliert automatisch, welche Probleme wie oft auftreten. Alle vorhandenen Software-Protokolle zu Sicherheitsproblemen nutzen.
- Ausführlich festlegen, wie der Prozess aller Sicherheitsmaßnahmen bis zu einem angemessenen IT-Sicherheitsniveau aussehen soll.
- Ausführlich festlegen, wie Sicherheitsmaßnahmen umgesetzt werden sollen.
- Alle getroffenen Sicherheitsmaßnahmen dokumentieren.
- Regelmäßig checken: Sind alle Sicherheitsmaßnahmen umgesetzt?
- Regelmäßig Soll-Ist-Vergleich des IT-Sicherheitsniveaus.