# Sicherheit ist Chefsache

**Ohne IT läuft nichts. Das gilt auch für KMU. Zehn einfache Schritte sorgen für minimalen Schutz gegenüber den Risiken der Informationsverarbeitung. Die Sorgfaltspflicht liegt aber bei der Geschäftsleitung.**

Wolfgang Sidler, Präsident InfoSurance

Sicherheit ist **eine strategische und nicht nur eine technische Frage.** Firmen können IT-Sicherheit nur wirkungsvoll und nachhaltig umsetzen, wenn sie fester Bestandteil der Unternehmenspolitik ist. Das IT-Sicherheitsmanagement muss organisatorisch im Unternehmen eingebunden sein. Die Erkennung und Festlegung der kritischen Informationen für ein Unternehmen und die Auswahl der geeigneten Sicherheitsmassnahmen sind Führungsaufgaben. Sie lassen sich nur eingeschränkt delegieren. Damit Firmen die IT-Sicherheit aber erfolgreich umsetzen können, ist die volle Unterstützung des Managements nötig. Die Verantwortung für die IT-Sicherheit liegt dabei beim Management. Dieses muss die notwendigen Massnahmen initiieren und deren Umsetzung kontrollieren. Dabei gelten folgende zehn Management-Grundregeln:

1. Das Management entscheidet über den Umgang mit Risiken, stellt die notwendigen Mittel zur Verfügung und trägt das verbleibende Restrisiko
2. Informationssicherheit muss in alle Prozesse und Projekte integriert sein, bei denen Mitarbeiter Informationen verarbeiten und nutzen
3. Der IT-Sicherheits-Prozess muss vom Management überwacht sein
4. Die Firmen müssen für den IT-Betrieb und die IT-Sicherheit ausreichende Ressourcen bereitstellen
5. Es müssen die organisatorischen Rahmenbedingungen für die IT-Sicherheit geschaffen sein
6. Die Umsetzung muss wirtschaftlich sein; IT-Sicherheit darf nicht mehr kosten als die damit erreichte Risikominderung
7. Die IT-Sicherheit muss in sinnvoller Relation zum Schutzbedarf stehen
8. Die Schutzmassnahmen müssen realisierbar sein und dürfen die Sicherheitslage nicht verschärfen (Praktikabilität); sie müssen nachweisbar Bedrohungen abwehren bzw. Risiken mindern (Wirksamkeit)
9. IT-Sicherheit darf nicht behindern und alle müssen sie als notwendig erachten (Akzeptanz)
10. Firmen müssen die IT-Sicherheitspolitik regelmässig überprüfen

Dafür wurde von Infosurance ein 10-Punkte-Programm geschaffen. Es ist einfach gehalten und Sie können die Massnahmen realisieren ohne viel Geld zu investieren. Wo das spezifische Fachwissen in einer Firma fehlt, können Sie sich von einem externen Experten unterstützen lassen.

- Pflichtenheft für IT-Verantwortliche erstellen
- Daten regelmässig mit Backups sichern
- Antivirus-Programm aktuell halten
- Internetzugang mit Firewall schützen
- Software regelmässig aktualisieren
- Starke Passwörter verwenden
- Mobile Geräte schützen
- Benutzerrichtlinien bekanntmachen
- Umgebung der IT-Infrastruktur schützen
- Dokumente und Datenträger ordnen

Das detaillierte 10-Punkte-Programm steht in deutsch und französisch zum Download zur Verfügung unter www.infosurance.ch.

**SWISS SECURITYDAY**

Der SwissSecurityDay ist der nationale Tag der Computersicherheit in der Schweiz und wird jeweils vom Verein InfoSurance im ersten Quartal des Jahres durchgeführt. Der nächste SwissSecurityDay findet am 10. März 2010 statt. Die Informationskampagne macht die Schweizer Bevölkerung auf den sicheren Umgang mit ihrem Computer aufmerksam. Fünf einfache Schritte für Ihre Computersicherheit vermitteln grundlegende Schutzmassnahmen zur Vorbeugung gegen die Gefahren im Internet. Im Zentrum der von Partnern getragenen Aktivitäten stehen regionale Schulungsangebote, um die Anwendung der fünf Schritte im Detail zu lernen. Partner des SwissSecurityDay sind grosse und kleine Unternehmen, Banken, Versicherungen, Hochschulen, Dienstleister, Hersteller sowie die Bundesverwaltung.

**KONTAKT:** Geschäftsstelle
Infosurance
Zentralstrasse 9
6002 Luzern
Tel. 041 228 41 92
mail@infosurance.ch
www.infosurance.ch