Giegerich & Partner

30 Tipps für mehr Informations- und IT-Sicherheit im Unternehmen

Kommunikative Maßnahmen

IT-Sicherheit beginnt mit Sensibilisierung und Schulung der Mitarbeiter sowie mit einer klaren Kommunikation der internen Verhaltensregeln zur Informationssicherheit:

- **Sichere Passwörter**: Komplexe Passwörter aus Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen, mind. achtstellig.
- **Passwortdiebstahl**: Niemals vertrauliche Daten weitergeben oder/und notieren.
- **E-Mailsicherheit**: E-Mails signieren, sensible Daten verschlüsseln, Vorsicht beim Öffnen von E-Mail Anlagen und Links.
- **Soziale Manipulation**: Bewusst mit vertraulichen Informationen umgehen, nur an berechtigte Personen weitergeben, sich nicht manipulieren oder aushorchen lassen.
- **Vorsicht beim Surfen im Internet:** Nicht jeder Link führt zum gewünschten Ergebnis.
- **Nur aktuelle Software einsetzen**: Eine nicht aktualisierte Software lässt mehr Sicherheitslücken offen.
- **Verwendung eigener Software**: Unternehmensvorgaben beachten und niemals Software fragwürdiger Herkunft installieren.
- **Unternehmensvorgaben**: Nur erlaubte Daten, Software (Apps) und Anwendungen einsetzen.
- **Backups**: Betriebliche Daten regelmäßig auf einem Netzlaufwerk speichern und Daten auf externen Datenträgern sichern.
- **Diebstahlschutz**: Mobile Geräte und Datenträger vor Verlust schützen.
- **Gerätezugriff**: Keine Weitergabe von Geräten an Dritte, mobile Geräte nicht unbeaufsichtigt lassen und Arbeitsplatz-PCs beim Verlassen sperren.

Organisatorische Maßnahmen

- Definition und Kommunikation von **Sicherheitsrichtlinien**
- Regelung der **Zugriffsrechte** auf sensible Daten
- Keine Vergabe von **Administratorenrechten** an Mitarbeiter
- Automatische und regelmäßige Verteilung von **Softwareupdates**
- Kontrolle der **Logfiles**
- Vollständige und regelmäßige **Dokumentation** der IT
- Auslagerung der **Datensicherung**
- Regelmäßige **Überprüfung der Sicherheitsmaßnahmen** durch interne und externe Sicherheitsanalysen
- Erstellung eines **Notfallplans** für die Reaktion auf Systemausfälle und Angriffe

Technische Maßnahmen

- Dokumentation der **WLAN-Nutzung**, auch durch Gäste
- Absicherung der Internetverbindung durch **Firewalls**
- Einsatz von **Zugangsschutz**/**Kennwörter**/**Biometrie**
- Physische **Sicherung**/**Zugangskontrolle** und -dokumentation
- **Schutz vor Schadsoftware** sowohl am Endgerät als auch am Internetgateway, idealerweise durch zwei verschiedene Antivirenprogramme
- Definition einer strukturierten **Regelung der Webzugriffe**
- **Verschlüsselung** zum Schutz von Dateien und Nachrichten mit sensiblen Inhalten
- **Sicheres Löschen** der Daten bei Außerbetriebnahme
- Sicherstellung regelmäßiger **Updates** der Sicherheitssysteme
- Permanente **Überwachung des Netzwerkverkehrs** auf Auffälligkeiten