
Cyberschutz – Sicherheit im digitalen Arbeitsumfeld

Cyberangriffe betreffen nicht nur die IT, sondern auch die Sicherheit/Gesundheit der Beschäftigten.

Folgen können sein:

- Arbeitsunterbrechungen, Produktionsstillstände oder Datenverlust,
- psychische Belastungen durch Stress, Unsicherheit oder Schuldgefühle,
- Sicherheitsrisiken, wenn digitale Steuerungen (z.B. Maschinen, Zutrittssysteme) manipuliert werden,
- Verletzung von Datenschutz und Vertraulichkeit (rechtlichen Konsequenzen).

Organisatorische Schutzmaßnahmen:

Beschäftigte über alle relevanten Gefährdungen unterwiesen werden – auch **Cyber Risiken**.

Inhalte einer Cyber-Unterweisung:

- Erkennen von z.B. Phishing-Mails
- Umgang mit Passwörtern, Zugangsdaten und mobilen Geräten
- Sicheres Verhalten im Internet und bei Cloud-Diensten
- Meldepflichten bei verdächtigen Vorfällen
- Sensibilisierung für psychische Belastung durch digitale Angriffe

Technische Schutzmaßnahmen:

Technische Prävention ist die Basis, ersetzt aber nicht die menschliche Aufmerksamkeit.

Wichtige Punkte:

- Verwendung von **aktueller Antivirensoftware & Firewalls**
- Regelmäßige **System- und Sicherheitsupdates**
- **Datensicherung (Backups)** auf getrennten Systemen
- **Zugriffskontrollen & Verschlüsselung**
- **VPN und Mehrfaktor-Authentifizierung** für externe Zugänge
- **Sichere IT-Arbeitsplätze im Homeoffice** (z. B. keine privaten Geräte)

