PRAXIS-LEITFADEN

IT-Sicherheit für kleine *Unternehmen.*

10 Maßnahmen, die sofort wirken. Kein Panikmachen, nur pragmatische Schritte.

43 % aller Cyberangriffe zielen auf kleine und mittlere Unternehmen. Die meisten Angriffe nutzen keine Hightech-Lücken – sondern menschliche Fehler und fehlende Basics.

01 **Starke Passwörter + Passwort-Manager** — GERING
Mindestens 12 Zeichen, keine Wörter. Ein Passwort-Manager (z. B. Bitwarden) speichert alles sicher.

02 **Zwei-Faktor-Authentifizierung (2FA) aktivieren** — GERING
Für E-Mail, Cloud, Banking und alle Admin-Zugänge. Authenticator-App statt SMS.

03 **Regelmäßige Backups (3-2-1 Regel)** — MITTEL
3 Kopien, 2 verschiedene Medien, 1 extern. Testen, ob die Wiederherstellung funktioniert.

04 **Updates und Patches sofort einspielen** — GERING
Betriebssystem, Browser, CMS, Plugins. Automatische Updates aktivieren wo möglich.

05 **E-Mail-Sicherheit: Phishing erkennen** — GERING
Absender prüfen, keine Links in unerwarteten Mails klicken. Im Zweifel: anrufen statt antworten.

06 **WLAN absichern** — GERING
WPA3 oder WPA2 mit starkem Passwort. Gäste-WLAN vom Firmennetz trennen.

07 **Mitarbeiter sensibilisieren** — MITTEL
Kurze Schulung (1 Stunde reicht): Phishing, Passwörter, USB-Sticks, Social Engineering.

08 **Zugriffsrechte minimieren** — MITTEL
Jeder Mitarbeiter nur die Rechte, die er braucht. Admin-Zugänge auf ein Minimum.

09 **Notfallplan erstellen** — MITTEL
Wer wird angerufen, wenn etwas passiert? Offline-Kontaktliste mit IT-Dienstleister, Provider, Bank.

10 **Professionelle Hilfe holen** — INVESTITION
Ein IT-Sicherheits-Check durch einen Experten deckt Lücken auf, die du selbst nicht siehst.

Sofort-Maßnahme:
Prüfe heute noch deine Backup-Situation. Wann war das letzte Backup? Weißt du, wo es liegt? Hast du schon mal eine Wiederherstellung getestet?