Checkliste: IT-Sicherheit fur Startups

Zugangssicherheit

- Verwenden Sie starke Passworter oder Passphrasen (mind. 12 Zeichen)
- Setzen Sie uberall Zwei-Faktor-Authentifizierung (2FA) ein
- Nutzen Sie einen Passwortmanager (z. B. Bitwarden, 1Password)
- Trennen Sie private und geschaftliche Konten strikt

Nutzer- und Rechteverwaltung

- Prinzip der minimalen Rechte: Nur Zugriff auf das, was notig ist
- Regelmaige Kontrolle und Entzug veralteter Benutzerzugange
- Onboarding- und Offboarding-Prozesse definiert und dokumentiert

Cloud- und SaaS-Sicherheit

- Anbieter mit Sicherheitszertifikaten wahlen (z. B. ISO 27001, SOC 2)
- Backup-Funktionalitaten regelmaig testen
- Zugriff auf Cloud-Dienste uber VPN oder SSO absichern

Netzwerksicherheit

- Firewall eingerichtet (auch fur Homeoffice)
- WLAN-Zugang mit WPA3 verschlusseln, getrennte Gaste-WLANs verwenden
- Remote-Zugriffe nur uber sichere Protokolle (z. B. VPN, SSH)

Updates und Patches

- Betriebssysteme, Software und Plugins regelmaig aktualisieren
- Automatische Updates aktivieren, wo moglich
- Legacy-Systeme konsequent ersetzen oder isolieren

Backup-Strategie

- Regelmaige, automatisierte Backups (mind. taglich)
- Backups auch auerhalb der Cloud speichern (z. B. lokal, offline)
- Wiederherstellung regelmaig testen

Notfallplane und Vorfalle

- IT-Notfallplan erstellen (z. B. bei Ransomware-Angriff)
- Verantwortliche fur Vorfallreaktion festlegen
- Kontakte zu Experten (z. B. IT-Forensik) griffbereit halten

Sensibilisierung & Schulung

- Awareness-Trainings fur alle Mitarbeitenden (Phishing, Social Engineering)
- Richtlinien zur sicheren IT-Nutzung schriftlich festhalten
- Regelmaige Auffrischungen und Tests (z. B. Phishing-Simulationen)

Rechtliche Anforderungen & DSGVO

- Auftragsverarbeitungsvertrage (AVV) mit allen Dienstleistern prufen
- Datenschutzbeauftragten benennen (wenn notig)
- Loschkonzepte und Datenklassifizierung etablieren

Sicherheitsuberprufung & Monitoring

- Sicherheits-Scans (z. B. mit Nessus, OpenVAS)
- Log-Analyse & Monitoring (z. B. mit SIEM-Tools)
- Regelmaige Pentests einplanen