IT-Sicherheit

Für Soloselbständige und Neugründer

Warum IT-Sicherheit wichtig ist

Als Neugründer oder Soloselbstständiger bist du oft selbst für deine IT-Sicherheit verantwortlich. Cyberangriffe, Datenverluste oder Identitätsdiebstahl können erhebliche finanzielle und rechtliche Konsequenzen haben. Eine gute IT-Sicherheitsstrategie schützt dein Geschäft und deine Kunden.

Wichtige IT-Sicherheitsmaßnahmen

Starke Passwörter und Passwortmanager

- Verwende lange, komplexe Passwörter (mind. 12 Zeichen mit Buchstaben, Zahlen und Sonderzeichen).
- Nutze einen Passwortmanager, um deine Passwörter sicher zu speichern.
- Aktiviere die Zwei-Faktor-Authentifizierung (2FA) für wichtige Konten.

Hardware & Netzwerk

- Halte dein Betriebssystem und alle Programme stets auf dem neuesten Stand.
- Installiere eine vertrauenswürdige Antivirensoftware und ggfs. eine Firewall.
- Deaktiviere ungenutzte Dienste und entferne nicht mehr benötigte Software.
- Router & WLAN sicher konfigurieren (verwende ein starkes Passwort und aktiviere WPA3).
- Nutze keine veralteten Geräte die ggfs. Sicherheitslücken aufweisen.
- Dokumentiere deine IT-Hardware (Seriennummern, Garantien, Zuständigkeiten). → optional

Datensicherung & Backup

- Erstelle regelmäßig Backups deiner wichtigen Daten.
- Speichere Backups an einem sicheren, externen Ort (z. B. externe Festplatte und im Cloud-Speicher mit Verschlüsselung).
- Teste, ob Backups wiederhergestellt werden können.

IHK Schwaben

Sicheres Arbeiten im Homeoffice oder unterwegs

- Nutze eine VPN-Verbindung, wenn du über öffentliche WLANs arbeitest.
- Vermeide die Nutzung von unsicheren Netzwerken für geschäftliche Zwecke.
- Sperre deinen Bildschirm, wenn du deinen Arbeitsplatz verlässt.

Sicherer Umgang mit Mobilgeräten

- Verschlüssele Smartphones und Tablets.
  (Seit Android 10 ist die Gerätespeicherverschlüsselung standardmäßig aktiviert. Apple verschlüsselt alle Geräte ab Werk, solange ein Sperrcode oder Face/Touch ID aktiviert ist.)
- Aktiviere eine Fernlöschfunktion für den Fall von Diebstahl oder Verlust.
- Vermeide es, geschäftliche Daten auf unsicheren Geräten zu speichern.

Sichere Cloud-Nutzung

- Wähle Cloud-Anbieter mit starker Verschlüsselung und prüfe die Datenschutzrichtlinien.
- Nutze Zwei-Faktor-Authentifizierung für den Zugriff auf Cloud-Dienste.
- Wähle sichere Cloud-Dienste (Google Drive, OneDrive, Nextcloud).

Benötigte Software und Konfiguration

Firewall einrichten

- In den meisten Fällen ist diese standardmäßig aktiviert, ob das bei dir der Fall ist, kannst du unter den Systemeinstellungen prüfen.
- Falls erforderlich, installiere eine Drittanbieter-Firewall.
- Konfiguriere die Firewall so, dass nur notwendige Anwendungen Internetzugriff erhalten.
- Stelle regelmäßige Updates sicher, um Schwachstellen zu vermeiden.

Antivirenprogramme

- Nutze bewährte Antivirenprogramme wie "Bitdefender", "Kaspersky" oder "Norton".
- Stelle sicher, dass die Software stets auf dem neuesten Stand ist.
- Führe regelmäßig Scans durch, um Bedrohungen frühzeitig zu erkennen.

VPN einrichten (optional, wenn man viel unterwegs ist)

- Wähle einen vertrauenswürdigen VPN-Anbieter wie "NordVPN", "ExpressVPN" oder ähnliche.
- Installiere die VPN-Software auf deinem Gerät und richte dein Konto ein.
- Aktiviere das VPN vor dem Verbinden mit unsicheren Netzwerken (z. B. öffentliche WLANs).
- Stelle sicher, dass das VPN keine Protokolle speichert ("No-Log-Policy").

Vorsicht vor Cyber-Attacken: Phishing & Social Engineering

Phishing ist eine der häufigsten Angriffsmethoden, um Zugang zu sensiblen Informationen zu erlangen.

Woran erkennst du Phishing?

- Verdächtige E-Mails oder Nachrichten mit Dringlichkeit ("Ihr Konto wird gesperrt!").
- Rechtschreib- und Grammatikfehler in E-Mails von angeblich seriösen Firmen.
- Links, die auf gefälschte Websites führen (Prüfe die URL, bevor du klickst!).
- Anhänge, die Malware enthalten könnten. Zum Schutz empfiehlt sich die Deaktivierung von Makros in Anwendungen wie z.B. Microsoft Office.

Wie kannst du dich schützen?

- Sei misstrauisch bei unerwarteten E-Mails oder Nachrichten.
- Öffne keine Links oder Anhänge von unbekannten Absendern.
- Prüfe die Absenderadresse sorgfältig.
- Nutze eine E-Mail-Sicherheitslösung mit Phishing-Erkennung.
- Melde verdächtige E-Mails deinem E-Mail-Anbieter oder IT-Dienstleister.

Schutz vor Social Engineering

- Sei dir bewusst, dass nicht nur technische, sondern auch psychologische Angriffe (z. B. Betrug durch Anrufe oder Fake-Mitarbeiter) eine Gefahr darstellen.
- Schule dich selbst in der Erkennung von Social-Engineering-Techniken.

▶ Schaue dir auch gerne mal unsere Erklärvideos an - dort haben wir die wichtigsten Themen nochmal aufgearbeitet | **Artikelnummer:** 5563644 auf unserer Website.

Regelmäßige Schulungen und Updates

- Halte dich über aktuelle Bedrohungen und Sicherheitstrends auf dem Laufenden.
  (Am besten abonnierst du den Newsletter vom BSI)

- Nimm regelmäßig an IT-Sicherheitsschulungen teil.

▶ Mit unserem kostenlosen Cyber-Security-Awareness-Test, deckst du deine Schwachstellen auf. Anmeldung unter: https://ihk.de/schwaben/CyberAwareness

▶ Außerdem bieten wir regelmäßig Webinare zum Thema IT-Sicherheit an, abonniere dafür unseren Newsletter | **Artikelnummer:** 5366908 auf unserer Website.

Notfallplan: Was tun bei einem Sicherheitsvorfall?

Falls du Opfer eines Cyberangriffs wirst, handle schnell:

1. Trenne dein Gerät sofort vom Internet.
2. Ändere deine Passwörter.
3. Informiere betroffene Kunden oder Partner.
4. Kontaktiere einen IT-Dienstleister.
5. Dokumentiere alle Sachverhalte, die mit dem Notfall in Zusammenhang stehen könnten.
6. Prüfe Kontaktaufnahmen mit der bayerischen Zentralen Ansprechstelle Cybercrime (ZACs) unter 089/1212-3300 oder dem Service Center des BSI unter 0800/274-1000.
7. Beachte Meldepflichten.

Rechtliche Aspekte

- Beachte Datenschutzrichtlinien (z. B. DSGVO), insbesondere wenn du Kundendaten verarbeitest.

▶ Weitere Informationen findest du auf unserer Website | **Artikelnummer:** 5246766

- Informiere dich über deine gesetzlichen Verpflichtungen bezüglich Datensicherheit.
- Halte deine Datenschutzerklärung auf deiner Website aktuell.

▶ Weitere Informationen findest du auf unserer Website | **Artikelnummer:** 3743266

- Schließe -falls nötig- Auftragsverarbeitungsverträge (AVV) mit Dienstleistern ab.
- Speichere und versende keine Kundendaten unverschlüsselt.

Fazit: IT-Sicherheit als Teil deiner Geschäftsstrategie

IT-Sicherheit ist kein einmaliges Projekt, sondern ein fortlaufender Prozess. Regelmäßige Updates, sichere Passwörter und ein wachsames Auge auf verdächtige Aktivitäten können dein Business langfristig vor Cyberbedrohungen schützen.

Bleibe informiert und investiere in deine digitale Sicherheit!
https://www.ihk.de/schwaben/it-sicherheit

Fragen? Dann melde dich gerne bei:
Beate Kille | beate.kille@schwaben.ihk.de | 0821/3162-357