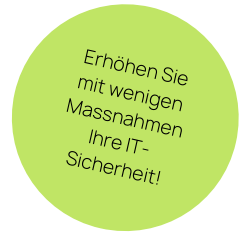


# IT-Sicherheit für Ihr KMU

Vernetzte Geräte und Maschinen, Daten in der Cloud und Kommunikation per E-Mail: Die Digitalisierung erhöht die Effizienz, bringt aber auch neue Risiken. Ein Datenverlust oder eine IT-Fehlfunktion kann verheerend sein. Es gilt deshalb, minimale Standards einzuhalten.

## Minimale Grundregeln für jedes KMU:

- **Backup:** Die wohl wichtigste Grundregel: Sichern Sie Ihre Daten! **Was soll wie oft vom wem wohin und wie lange** gesichert werden? Beziehen Sie auch ihre SaaS und Cloud-Dienste mit ein. Von wem können die Daten wieder hergestellt werden und wie lange dauert ein operativer Unterbruch bei einem Datenverlust? Wenden Sie beim Backup die **3-2-1-Regel** an: **3** Kopien aller kritischen Daten auf **2** unterschiedlichen Medien, davon sollte **1** offsite gelagert werden, sprich an einem anderen Standort als die Original-Daten.
- **Passwortrichtlinien:** Erstellen Sie eine interne Passwortrichtlinie mit ihren Vorgaben. Für jedes Portal/Login ein eigenes Passwort, 2-Faktor-Authentifizierung sollte Standard sein. Die Passwörter unbedingt sicher aufbewahren!
- **Berechtigungskonzept:** Jeder Mitarbeitende (Rolle) sollte nur so viele Rechte haben, wie nötig. Vergeben Sie keine lokale Administratorenrechte. In einem Portal sollte die Rolle «Admin» immer mit einem separaten Benutzer gelöst werden.
- **Technische Schutzmassnahmen:** Aktueller Virenschutz, Spamfilter dazu evtl. eine Firewall. Je nach Branche sind weitere Massnahmen notwendig, Server und andere zentrale Infrastrukturkomponenten sollten zudem vor physischem Zutritt und vor Überspannung geschützt werden. Ebenfalls sollten Updates und Patches zeitnah nach Veröffentlichung bei allen mit dem Internet verbundenen Geräten und Systemen installiert werden.
- **Mitarbeiter-Sensibilisierung:** Häufigstes Einfallstor für Cyber-Attacken sind die Mitarbeitenden, welche durch gezielte Manipulation (Phishing-Mails, betrügerische Anrufe) dazu gebracht werden, Informationen preiszugeben oder Handlungen auszuführen. Eine regelmässige Thematisierung von Cyber-Gefahren und Datenschutz ist unerlässlich.
- **IT-Verantwortlicher:** Bestimmen Sie einen internen IT-Verantwortlichen und ziehen Sie in Ihre Überlegungen die Lieferanten und Verträge mit ein. Wer ist bei den Applikationen Ihr Ansprechpartner (1st Level/2nd Level)? Was sind Ihre **Sofortmassnahmen** bei einem Cyber-Vorfall?



## Denken Sie auch an folgende Themen:

- Verschlüsselung besonders schützenswerter Daten gemäss **neuem Datenschutzgesetz** (in Kraft ab ca. Sept. 2023). Wer ist ihr Datenschutzverantwortlicher?
- Gesicherte und **verschlüsselte E-Mails** oder Kommunikationsverbindungen im Internet (VPN)
- Erfüllung der **PCI-DSS Standards** beim Angebot von Kredit-/Debitkarten-Zahlungen für Ihre Kunden.

## Unsere Partner für Ihr KMU – auch ausserhalb der IT-Themen

IT-Sicherheit  
**Weibel/IT**  
Weibel/IT AG, Kirchberg SG  
www.weibel-it.ch

Digitale Langzeitarchivierung  
**docu team**  
docuteam AG, Baden AG  
www.docuteam.ch

Treuhand, Revision und Steuern  
**TIREGA CONSULTING**  
Tirega Consulting AG, Wald ZH  
www.tirega.ch

Rechtsanwälte  
**SteuFiFisch**  
SteuFiFisch AG, Wil SG  
www.steurifisch.ch

Treuhand, Revision und Steuern  
**rawp**  
rawp raschle wirtschaftsprüfung,  
Wil SG - www.rawp.ch

Marketing & Werbung  
**KOMET**  
Komet Werbeagentur AG, Bern  
www.komet.ch

Treuhand und Steuern  
**WerSa-Treuhand**  
Büro für Landwirtschaft, Gewerbe & Private  
WerSa Treuhand GmbH, St. Peterzell  
www.wersa-treuhand.ch

Marketing & Werbung  
**e3 eigengrau**  
eigengrau gmbh, Wollerau SZ  
www.eigengrau.ch

Dazu viele regionale Betriebe im Bereich Immobilien, Haushalt und Fahrzeuge – auch im Schadenfall!