

Cyber-Security Assessment für KMU

- Wie gut ist Ihr Unternehmen vor Angriffen aus dem Cyberspace geschützt und darauf vorbereitet?
- Die Risiken von Cyberangriffen werden oft stark unterschätzt.
- Der Gesundheits-Check für Ihre Informationssicherheit und Ihren Datenschutz.

Ihre Situation

Cyber-Angriffe gehören heute leider zum Alltag. Sie sollen sich deshalb rasch ins Bild setzen können, ob Ihre technischen, organisatorischen und mitarbeiterbezogenen Massnahmen zum Schutz vor Cyberrisiken ausreichen.

KMUs bilden das Rückgrat der Schweizer Wirtschaft. Um langfristig erfolgreich zu sein, müssen KMUs mittels digitalen Technologien, Lieferanten, Mitarbeitende und Kunden in ihre Prozesse einbeziehen. Dies bedingt eine zunehmende Vernetzung von Unternehmensinfrastrukturen und –Daten mit dem Internet. Dadurch erhöhen sich die Risiken aus dem Cyberspace drastisch, da Ihre Daten exponiert sind.

Unser Angebot

Wir stellen Ihnen unser 20-jähriger Erfahrungsschatz im Bereich der Informationssicherheit und des Datenschutzes zur Verfügung.

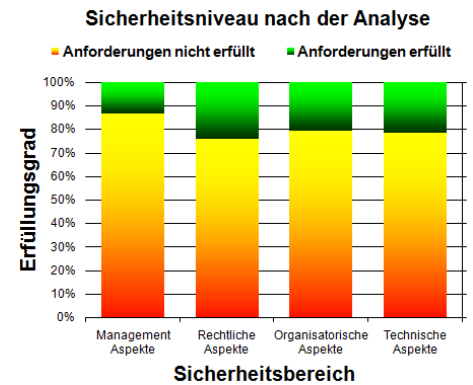
Ihr Nutzen

- Schwachstellen erkennen
- IT-Risiken identifizieren
- Sicherheitsniveau ermitteln
- Sicherheitsmassnahmen definieren
- Sensibilisierung der Mitarbeitenden
- Einen IT-Grundschutz etablieren

Ablauf

Mit unserem **Cyber-Security Assessment** erhalten Sie ein objektives Bild Ihrer IT-Sicherheit. Sie erfahren, ob Ihre IT-Infrastruktur wirklich sicher ist. Das Ergebnis des Cyber-Security Assessments ist klar und zeigt Ihnen eindeutig, welche Handlungsbedarf bestehen und was Sie dagegen tun sollten. Informationssicherheit ist also mehr als das Sicherstellen von Daten (z.B. Backup). Es umfasst auch die Sicherung der längerfristigen Geschäftstätigkeiten und den Schutz des Wissens der Mitarbeitenden im Unternehmen. Informationssicherheit ist daher eine strategische/organisatorische und keine rein technische Frage.

**Informationssicherheit neu definiert
angemessen—konkret—auf den Punkt gebracht**



**„Sicherheit ist – keine unvermeidbaren
IT-Risiken mehr zu haben!“**

Gefahren und Risiken

Eine Auflistung möglicher Gefahren und Bedrohungen:

- Feuer, Blitz, Sturm, Überschwemmung, Stromausfall
- Krankheit, Fehlmanipulation, fehlende Sensibilisierung
- Unwissen, falsches Verhalten
- Nicht einhalten der Gesetze
- Nicht einhalten vertraglicher Kunden-Anforderungen
- juristische Konsequenzen bei einer Vertragsverletzung
- Netzwerkausfall, Ausfall Disk-Systeme, etc.
- Mangelnde Kompatibilität bei einer Migration
- Softwarefehler, Viren, etc.
- Unzureichende physische Zutrittskontrollen
- Falsche Zugriffsrechte auf Daten und Programme
- Abgang von Schlüsselpersonen (Knowhow-Verlust)
- Versagen der Prozesse
- Manipulation, Hacking, Erpressung
- Diebstahl, Sabotage
- Missbrauch, Spionage, organisierte Kriminalität, etc.



SIDLER
Information Security

Holzhäuserstrasse 5a
6331 Hünenberg / Zug

Tel. 041 781 57 72
www.sidler-security.ch
info@sidler-security.ch