SWISS BUSINESS PROTECTION
www.swissbp.ch
@ info@swissbp.ch
+4141 511 42 33

Cyber-Security Assessment

Produkte / Dienstleistungsumschreibung (Summary)

Cyber-Angriffe gehören heute leider zum Alltag. Sie sollten sich deshalb rasch ins Bild setzen können, ob Ihre technischen, organisatorischen und mitarbeiterbezogenen Massnahmen zum Schutz vor Cyberrisiken ausreichen. Um langfristig erfolgreich zu sein, müssen KMU's mittels digitaler Technologien ihre Lieferanten, Mitarbeitenden 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.

Informationssicherheit ist mehr als das Sichern von Daten (z.B. Backup). Es umfasst auch die Absicherung der längerfristigen Geschäftstätigkeiten und den Schutz des Wissens im Unternehmen. Informationssicherheit ist daher eine strategisch /organisatorische und keine rein technische Frage. In unserem Angebot stellen wir Ihnen unseren 20-jährigen Erfahrungsschatz im Bereich der Informationssicherheit zur Verfügung.

Abgrenzung: Dieses Angebot ist kein Penetrations-Test und kein technischer Audit.

Nutzen	Mit unserem Cyber-Security Assessment erhalten Sie ein objektives Bild Ihrer IT-Sicherheit. Sie erfahren, ob Ihre organisatorischen Sicherheitsmassnahmen wirklich effektiv sind. Das Ergebnis des Cyber-Security Assessments zeigt Ihnen eindeutig, welcher Handlungsbedarf besteht. • Schwachstellen erkennen • IT-Risiken identifizieren • Sicherheitsniveau ermitteln • Sicherheitsmassnahmen definieren • Sensibilisierung der Mitarbeitenden erhöhen • Einen IT-Grundschutz etablieren
Inhalt	• Feuer, Blitz, Sturm, Überschwemmung, Stromausfall • Unwissen, falsches Verhalten Krankheit, Fehlmanipulation, fehlende Sensibilisierung • Nichteinhalten der Gesetze oder vertraglicher Kunden-Anforderungen • Netzwerkausfall, Ausfall Disk-Systeme, etc. • Versagen der Prozesse, Softwarefehler, Viren, etc. • Unzureichende physische Zutrittskontrollen • Falsche Zugriffsrechte auf Daten und Programme • Abgang von Schlüsselpersonen (Knowhow-Verlust) • Manipulation, Hacking, Erpressung, Diebstahl, Sabotage • Missbrauch, Spionage, organisierte Kriminalität, etc.
Methodik	Informationsfindung, Situationsanalyse, Auswertung, Diskussion, Planung, Umsetzung.
Zielgruppe	KMU aller Branchen
Dauer / Ort	½ Tag vor Ort, zusätzlich ½ Tag Vorbereitung und ½ Tag Abschlussbericht
Kosten (exkl. MWST)	• 3'000.- als Kostendach (1.5 Tage) • 2'000.- / Tag (1 Tag = 8 Std.) • 250.- / Std.
Leitung	Wolfgang Sidler