Cyber Security

concepts and more …

Cyber Resilienz durch IT Security Checks

Das Risiko von Cyberangriffen ist heute eine ernstzunehmende Bedrohung, das von vielen Unternehmen nach wie vor unterschätzt wird. Dies hat zur Folge, dass Massnahmen zur Erkennung und Abwehr oft vernachlässigt werden. Es ist eine stetige Herausforderung, den eigenen Status Quo zu kennen sowie deren Stärken und Schwächen zu identifizieren, um daraus die strategische Richtung inklusive deren konkrete Verbesserungsmassnahmen ableiten und umsetzen zu können.

Für viele Unternehmungen stellt sich aber bei der Risikoabwägung die Frage der Angemessenheit von Sicherheitsvorkehrungen – wieviel ist nötig und sinnvoll?

Im ICT-Sicherheitsumfeld zielt eine ICT-Sicherheitsstrategie darauf ab, Verletzungen der ICT-Sicherheit zu erkennen, darauf zu reagieren sowie die Konsequenzen der Sicherheitsverletzung zu minimieren bzw. zu mildern. Die Strategie verfolgt einen holistischen Ansatz, welcher alle ICT-Betriebsmittel (Personen, Prozesse, Objekte, Daten und Geräte) gegen beliebige Risiken zu schützen versucht. Die Ressourcen des Unternehmens sollen so eingesetzt werden, dass ein effektiver Schutz vor bekannten Risiken sowie eine umfassende Überwachung potenzieller zukünftiger Risiken gewährleistet ist.

Die Resultate des Cyber Security Assessments* mit Analyseresultaten und Umsetzungsmassnahmen sensibilisieren Unternehmen auf ihre Risiken aus dem Cyberraum und bilden die Grundlage für wirksame Vorkehrungen gegen Cyber-Attacken und für die Vorfallbewältigung – im Sinne der ICT-Resilienz.

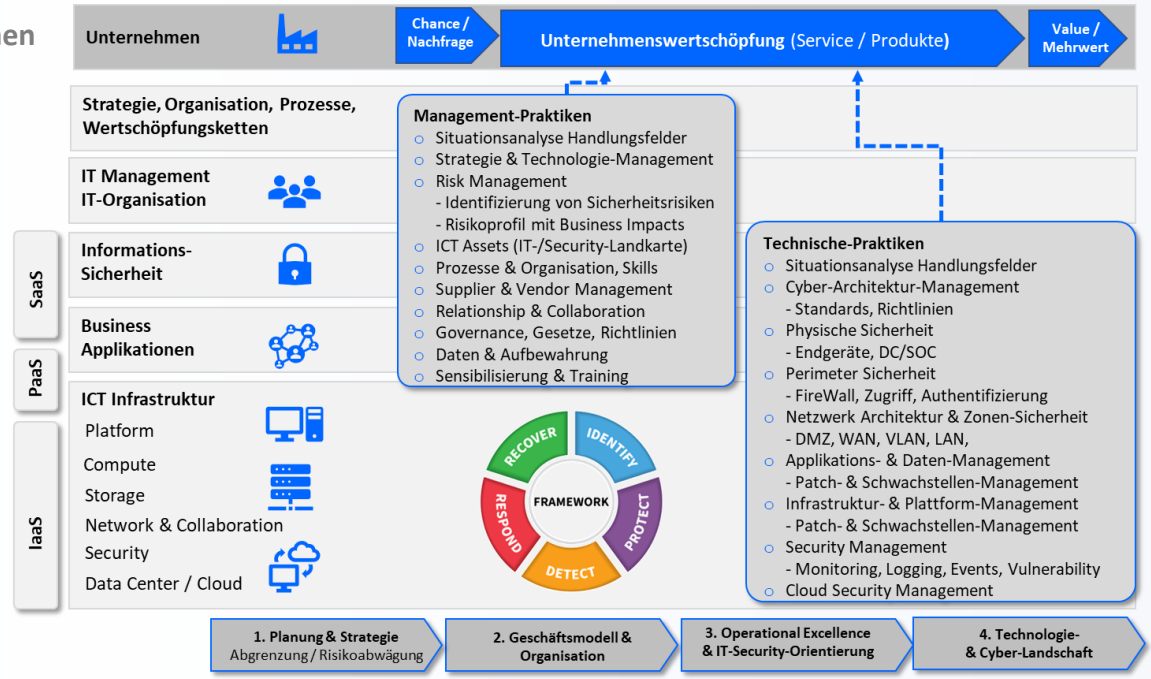
**Das praxisorientierte Security-Assessment-Konzept basiert auf dem Cyber Security Framework von NIST – dem National Institute of Standards and Technology - und ist mittlerweile Standard im Umgang mit Cyberrisiken. Unser Konzept basiert auf dem NIST Cybersecurity Framework Core.3 und NIST Guide to Industrial Control Systems (ICS) Security sowie auf dem Standard zur Verbesserung der ICT-Resilienz für KMU vom Eidgenössisches Departement für Wirtschaft, Bildung und Forschung WBF, Bundesamt für wirtschaftliche Landesversorgung BWL und der Melde- und Analysestelle Informationssicherung MELANI. Weitere im Konzept integrierte Normen sind ISO 2700x, COBIT, ENSA Good Practice Guide on National Cyber Security Strategies, BSI 100-2 und ITIL V4.*

Wir verstehen durch Beratung und durch Durchführung von methodisch strukturierten Analysen und Konzepten Ihre Bedürfnisse – mit Technologiekompetenz entstehen mit Ihnen innovative und sichere Lösungen sowie Produkte, welche im Betrieb Ihre Digitalisierung, Sicherheit und Wertschöpfung verbessern – **WIR MACHEN IHRE IT BUSINESSTAUGLICH.**

Wir stimmen mit Ihnen im Rahmen des Cyber Security Assessments* ein praxisorientiertes und adäquates Sicherheits-Maturitäts-Level ab, welches mit entsprechenden Prozessen, Konzepten und einer Organisation zur Durchführung und Überwachung der Kontrollen erreicht werden kann. Es entsteht folgender Nutzen:

- Erkennung und Bekämpfung von Anomalien, um bei einem Cyber-Vorfall richtig zu reagieren.
- Verhindern von Angriffen auf die Systeme und Infrastrukturen.
- Verhindern von Datenverlust durch Verschlüsselung oder Löschung.
- Ermöglichung eines einheitlichen und sicheren Zugriffs auf Applikationen (intern/extern).
- Vorschläge für Make- or Buy-Entscheidungen von ausstehenden Massnahmen und Verantwortungen.

Prüfungsrahmen



Vorgehen & Resultate