

# Security Assessment

Schwachstellen erkennen, Lücken schließen, Schutz optimieren - Klarheit sorgt für Sicherheit

Es vergeht kaum ein Tag, an dem in den Medien nicht berichtet wird über erfolgreiche Angriffe von Cyber-Kriminellen auf Unternehmen und ihre IT-Infrastrukturen mit unterschiedlichsten Auswirkungen.

Viele Unternehmen fühlen sich gut gewappnet gegen Cyber-Angriffe, aber oftmals trägt der Schein

Deshalb waren schon viele Unternehmen mindestens einmal betroffen von Ransomware oder Phishing-Angriffen, die sie allein oder mit Unterstützung Externer bewältigt haben.

Und deshalb fühlen sich viele Unternehmen gut aufgestellt und sicher. Doch die Realität sieht oftmals anders aus, denn trotz bereits geschlossener Lücken gibt es andere Schwachstellen, die noch unerkannt sind - eine Gefahr, die nicht zu unterschätzen ist.

Wissen, wo das Unternehmen steht: Ermittlung des allgemeinen Sicherheitsniveaus

Genau in diesem Kontext setzt ein Security Assessment an: Es geht darum, den aktuellen Stand der Informationssicherheit zu messen und Schwachstellen aufzudecken.

Die Betrachtung bezieht sich dabei sowohl auf technische als auch auf organisatorische Komponenten im Bereich der Informationssicherheit und kann durch gezielte Analysen dazu beitragen, das Unternehmen vor externen und internen Angriffen zu schützen und neue Angriffsmöglichkeiten zu identifizieren und deutlich zu reduzieren.

Wir orientieren uns dabei an bestehenden Standards wie dem IT-Grundschutz oder einer ISO 27001.

Klare Sicht auf das IST bedeutet Klarheit über das SOLL

Neben der Orientierung an diesen Standards gestalten wir ein Security Assessment immer auch nach den individuellen Wünschen unserer Kunden. Im Rahmen eines Kick-Off-Workshops werden die zu behandelnden Themen festgelegt, so dass eine Aufwandschätzung vorgenommen werden kann. Entsprechend festgelegter Prüfschritte werden im Anschluss die Erkenntnisse in Reports dokumentiert und mögliche Handlungsempfehlungen vorgestellt, um daraus bei Bedarf eine Roadmap zur Erhöhung der Informationssicherheit zu entwickeln. Ziel ist es, mit einem Security Assessment die Messbarkeit der Sicherheit zu erhöhen und eine kontinuierliche Verbesserung zu erzielen.

## IHRE VORTEILE

- Ermittlung des allgemeinen Sicherheitsniveaus
- Proaktive Prüfung des Informations-Sicherheitsmanagements
- Messbarkeit ermöglichen
- Basis für die Entwicklung einer Security Strategie und eines ISMS
- Angepasstes Reporting für das ISMS