



DATENSCHUTZ & IT-SICHERHEIT FÜR UNTERNEHMEN

Datenschutz- und IT-Sicherheitsanalyse der ITC

Der effektive Schutz sensibler Informationen gewinnt in allen wirtschaftlichen Bereichen zunehmend an Bedeutung. Die Gewährleistung der Vertraulichkeit, Verfügbarkeit, Integrität und Authentizität sensibler Informationen ist ein essentieller Faktor für die Konkurrenzfähigkeit und den Erfolg eines Unternehmens.

Zweck und Zielsetzung

Ziel der Unterstützungsleistungen durch die IT-Consult Halle ist eine möglichst umfassende Analyse von IT-Infrastruktur, IT-Sicherheitsmanagement und Datenschutzmanagement für Unternehmen. Basierend auf einer Analyse der vorhandenen IT-Infrastruktur und des Umsetzungsgrades wesentlicher Schutzmaßnahmen werden Sicherheitslücken im Rahmen des bestehenden IT-Sicherheits-/ Datenschutzmanagements identifiziert und dokumentiert. Auf Basis der gewonnenen Erkenntnisse werden daraus in einem nächsten Schritt eine adäquate Vorgehensweise zur Abstellung erkannter Defizite erarbeitet. Hinweise und Handlungsempfehlungen unterstützen dabei die verantwortlichen Entscheidungsträger des IT- und Datenschutzmanagements.

Vorgehensweise

Die Datenschutz- / IT-Sicherheitsüberprüfung orientiert sich grundsätzlich an den Vorgaben des Bundes- und Landesdatenschutzgesetzes sowie des Bundesamtes für Sicherheit in der Informationstechnik (BSI) bzgl. der Durchführung einer IT-Sicherheitskonzeption gem. IT-Grundschutz. Hierbei handelt es sich um einen Standard für die Etablierung und Aufrechterhaltung eines umfassenden IT-Sicherheitsmanagements, welches sich am Schutzbedarf der betrachteten Informationen ausrichtet. Ein wesentlicher Bestandteil dieses Standards ist ein umfangreicher Katalog von Schutzmaßnahmen, welcher die Grundlage dieser Überprüfung darstellt. Aufgrund von Umfang und Komplexität dieses Regelwerkes wird die Überprüfung an die individuellen Bedürfnisse und Rahmenbedingungen des Unternehmens angepasst und beschränkt sich auf die wichtigsten Aspekte. Hier die wesentlichen Analyseschritte:

- Definition des Geltungsbereiches für die Analyse
- Strukturanalyse
- Schutzbedarfsanalyse
- Schutzmaßnahmenanalyse

Dienstleistungen der ITC

- **Datenschutz & IT-Sicherheitsanalyse**
- **Erstellung von Datenschutz- & IT-Sicherheitskonzepten**
- **externer Datenschutzbeauftragter**
- **Schulungen**
- **Nutzung eines gesamten „Sicherheitsteams“ mit Kernkompetenzen in IT-Strategie sowie Prozess- und Fachberatung**



TÜVRheinland®
CERT
ISO/IEC 27001



Referenzen:

- **Stadtwerke Halle GmbH**
- **EVH GmbH**
- **Wikana Keks und Nahrungsmittel GmbH**
- **Werkzeugmaschinenfabrik Zerbst GmbH**
- **Ingenieurbüro Stork Plan**
- **ALS Dienstleistungsgesellschaft**
- **EMAG Leipzig Maschinenfabrik**

Strukturanalyse

Im Rahmen einer Strukturanalyse werden die wichtigsten Elemente des IT-Verbundes erfasst. Hierbei erfolgt eine Analyse der Zusammenhänge zwischen den Geschäftsprozessen des Unternehmens, der eingesetzten Soft- und Hardware sowie den entsprechenden infrastrukturellen Rahmenbedingungen. Diese Elemente werden berücksichtigt:

- Anwendungen/ Dienste
- IT-Systeme
- Kommunikationsverbindungen
- Gebäude und Räume

Schutzbedarfsanalyse

Der Schutzbedarf einer Information leitet sich im Allgemeinen aus der potentiellen Schadenshöhe im Falle des Verlustes der IT-Sicherheit ab. Der Schutzbedarf einer Anwendung, Applikation oder Funktionalität ist demnach mit dem Schutzbedarf der verarbeiteten, gespeicherten oder übertragenen Information gleichzusetzen. Die IT-Sicherheit selbst wird dabei an Teilzielen festgemacht wie Vertraulichkeit, Integrität, Verfügbarkeit und Verbindlichkeit der Informationen.

Die Schäden, welche durch den Verlust dieser sensibler Informationen entstehen können, lassen sich wie folgt einteilen:

- Verstöße gegen Gesetze, Vorschriften oder Verträge,
- Beeinträchtigung des informationellen Selbstbestimmungsrechts,
- Beeinträchtigung der persönlichen Unversehrtheit,
- Beeinträchtigung der Aufgabenerfüllung,
- negative Innen- und Außenwirkung und
- finanzielle Auswirkungen.

Schutzmaßnahmenanalyse

Basierend auf dem potentiellen Schaden bei Verlust der IT-Sicherheit werden diese Schutzmaßnahmen überprüft, welche die IT-Sicherheit mit einem angemessenen Aufwand gewährleisten. Diese Auswahl repräsentiert einen ausgesuchten Teil der Maßnahmenkataloge des BSI:

- Personelle IT-Sicherheitsmaßnahmen
- Infrastrukturelle IT-Sicherheitsmaßnahmen
- Organisatorische IT-Sicherheitsmaßnahmen
- Technische IT-Sicherheitsmaßnahmen



Nähere Informationen: