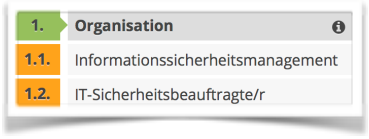
1.1 INFORMATIONSSICHERHEITSMANAGEMENT

Ordner Informationssicherheit - Kapitel 1. Organisation



Erstellt von: Vorname Name
10. Januar 2017
Version: 1.0

MUSTER

1.1 INFORMATIONSSICHERHEITSMANAGEMENT

Informationssicherheit - Das ist uns wichtig !

Die online Ordner von OSPREE sind digitale Produkte, in denen eine Vielzahl von Kunden- und Partnerdaten auf Servern gespeichert und elektronisch übermittelt werden. Ein Systemausfall oder der Verlust von Daten birgt ein hohes Risiko für das Geschäftsmodell. Der Informationssicherheit kommt deshalb einen hohen Stellenwert zu. Sie werden mit den konkreten Sicherheitsaspekten vertraut gemacht, die beim Umgang mit geschäftsrelevanten Informationen und beim Einsatz von Informationstechnologie in einer kleinen Firma zu beachten sind.

Der Aufbau des Informationssicherheitsmanagements

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) beschreibt eine systematische Vorgehensweise zur Erstellung von IT-Sicherheitskonzepten. Diese Dokumentation (online Ordner) basiert auf den Empfehlungen und den Standards des BSI. Die aktuelle Fassung der BSI-Standards findet sich im Internet unter http://www.bsi.bund.de/gshb/.

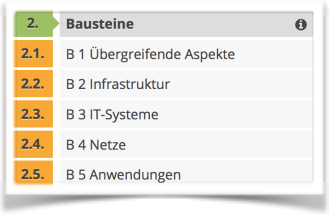
Der Aufbau gliedert sich in folgende vier Hauptkapitel:

- eine Beschreibung der Rahmenbedingungen (Bausteine)
- eine Analyse der möglichen Gefährdungen
- eine Aufstellung von konkreten Massnahmen
- ein Kapitel zur öffentlichen Kommunikation

Informationen zum Aufbau der Hauptkapitel

In den Hauptkapiteln werden zuerst die Rahmenbedingungen in Bausteinen (Kapitel 2) analysiert und festgehalten. In den Gefährdungskatalogen (Kapitel 3) werden mögliche Gefahren und deren Risiken festgehalten. Aus den Rahmenbedingungen und den Gefährdungen werden danach Massnahmenkataloge abgeleitet und erstellt (Kapitel 4). Im Kapitel Öffentliche Kommunikation (5) wird zum Schluss festgehalten, was unseren Kunden und Partner zum Thema Informationssicherheit und Schutz der Daten kommuniziert wird.

2. Bausteine (Rahmenbedingungen)



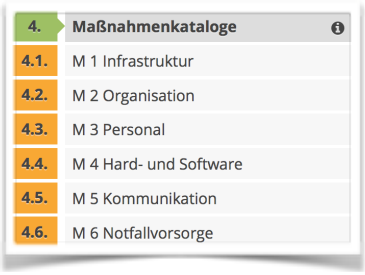
Was sind unsere wichtigsten Geschäftsprozesse ? Wissen wir, welche Daten so bedeutend sind, dass ihr Verlust oder Diebstahl einen Verstoß gegen ein Gesetz oder einen Vertrag bedeutet ? Wie wichtig sind uns unsere Kundendaten ? Können wir noch problemlos arbeiten, wenn ein Computer defekt ist, der Cloud-Server ausfällt oder die Telefonverbindung gestört ist ? Wer hat Zugang zu unseren Daten und wo sind diese gespeichert ? Wer hat Zugang zu unseren Büros und wie sind diese geschützt ? Wer kauft, pflegt und

überwacht unsere IT und Kommunikation ? - Dies sind einige der Fragen, die wir uns im Kapitel Bausteine stellen. Die Antworten zeigen uns die Rahmenbedingungen auf, die für unsere Geschäftstätigkeit relevant sind.

3. Gefährdungskataloge

Die Gefährdungen sind nach den Bereichen Elementare Gefährdungen, Höhere Gewalt, Organisatorische Mängel, Menschliche Fehlhandlungen, Technisches Versagen und Vorsätzliche Handlungen unterteilt. In den einzelnen Katalogen erstellen wir eine Einschätzung zu möglichen Auswirkungen von Gefährdungen auf unsere Firma sowie unsere Kunden und Partner. Eine abgestufte, differenzierte Risikoeinschätzung ist elementar. Beispiel: Ein grosses Erdbeben hätte zwar katastrophale Folgen, die Wahrscheinlichkeit eines solchen an unserem Standort in Berlin ist jedoch gleich Null.

4. Massnahmen



Dieses Kapitel beschreibt ausführlich unsere konkreten Massnahmen für die beschriebenen Rahmenbedingungen (Bausteine in Kapitel 2) und berücksichtigt die erstellten Gefährdungsbeurteilungen in Kapitel 3. Der grösste Teil widmet sich den „normalen“ Rahmenbedingungen, also dem regulären Betrieb. Das Unterkapitel 4.6 Notfallvorsorge enthält Massnahmen, die wir treffen, wenn eine Gefährdung eintritt.

5. Öffentliche Kommunikation

Eine gezielte, öffentliche Kommunikation, was mit Daten und persönlichen Informationen geschieht und wie ein Unternehmen damit umgeht, schafft Transparenz und Vertrauen bei unseren Kunden und Partnern. Die wichtigsten Massnahmen des Informationssicherheitsmanagement und eines IT-Grundschutzes kommunizieren wir bei OSPREE deshalb auch nach Aussen.