FSKB IT Guideline – Ausgabe 2018

Inhalt

Präambel

Die IT-Guideline soll den Mitgliedern des FSKB einen Überblick über mögliche Handlungsfelder im Zusammenhang mit IT-Sicherheit geben und einen Gesamtüberblick verschaffen. Die IT-Guideline kann nicht alle Fragestellungen im Detail erläutern, sie soll vielmehr sensibilisieren, die jeweiligen Themenkreise vor dem Hintergrund der jeweiligen Organisation zu betrachten und zu beurteilen. Für weitergehende Bearbeitungen sind entsprechende Spezialisten beizuziehen.

Insbesondere sind teilweise rechtliche Randbedingungen zu beachten, die über das Thema IT-Anwendung hinausgehen. Die IT-Infrastruktur versteht sich als Werkzeug zur Unterstützung von anderen Tätigkeiten. Über deren rechtliche und ethische Beurteilung kann das vorliegende Dokument keine Aussagen machen.

Der Übergang zwischen geschäftlichen und privaten Nutzungen ist häufig fliessend. Dies kann zu Konflikten bezüglich der Sicherheitsfragen führen. Die Frage des angestrebten Sicherheitsniveaus ist zu definieren, ob es sich gegen den "Gelegenheitstäter" richtet oder vor Personen mit grosser krimineller Energie schützen soll.

Das Thema IT-Sicherheit sollte immer auf den folgenden Ebenen behandelt werden:
- Strategische Aspekte
- Operative Prozess
- Technik

1 Vorbemerkung/Einleitung

1.1 Bedeutung des Themas IT-Sicherheit für die Kies- und Betonbranche

IT-Sicherheit ist ein umfangreicher, teilweise abstrakter Begriff. Ihn konkret werden zu lassen, ist auch Aufgabe einer noch so kleinen Unternehmung. Im Folgenden wird IT-Sicherheit umfassend verstanden und nicht nur auf "Virenschutz-Programme" und "Passwort-Management" reduziert.

Bezüglich der Informationssicherheit sind grosse Unternehmen und Behörden aufgrund ihrer finanziellen und personellen Ausstattung oft besser aufgestellt, als kleine und mittelständische Unternehmen. Auch wenn das Bewusstsein für Fragen der IT-Sicherheit stetig zunimmt, können die notwendigen Massnahmen oft mangels geschultem Personal, finanziellen und zeitlichen Ressourcen nicht ausreichend umgesetzt werden.

Diese IT-Guideline erläutert die erforderlichen Schritte zur Überprüfung des bestehenden IT-Sicherheitsniveaus, sowie schnell realisierbare Massnahmen, die auch mit geringen finanziellen Mitteln und wenigen Mitarbeitern in Unternehmen, die sich das erste Mal mit diesem Thema befassen, umsetzbar sind.

Zentral ist der bewusste Umgang bezüglich der Fragestellungen der IT-Sicherheit. Dies beinhaltet auch die bewusste Nicht-Umsetzung von Massnahmen, wenn dies im spezifischen Umfeld angezeigt erscheint.

1.2 Basis-Absicherung

Die internationale Norm ISO/IEC 27001 Information Security Management Systems (ISMS) spezifiziert die Anforderungen für Einrichtung, Umsetzung, Aufrechterhaltung und fortlaufende Verbesserung eines dokumentierten Informationssicherheits-Managementsystems.

ISMS-Methoden etablieren drei Vorgehensweisen bei der Umsetzung des IT-Grundschutzes:

- Die **Basis-Absicherung** (für jedermann) liefert einen Einstieg zur Initiierung eines ISMS.
- Mit der **Standard-Absicherung** kann ein kompletter Sicherheitsprozess implementiert werden, der kompatibel zur ISO 27001-Zertifizierung ist.
- Die **Kern-Absicherung** (für Betriebseinheiten im Konzernverbund) ist eine Vorgehensweise zum Einstieg in ein ISMS, bei der zunächst ein kleiner Teil eines grösseren Informationsverbundes betrachtet wird. Mit der Kern-Absicherung können zeitnah die wichtigsten Ressourcen und Geschäftsprozesse abgesichert werden. So kann in einem ersten Schritt zunächst der kritischste Geschäftsprozess abgesichert werden, um in weiteren Schritten wahlweise die nächsten kritischen Geschäftsprozesse abzusichern oder für alle Bereiche der Institution die Basis- oder Standard-Absicherung zu beginnen.

Die Basis-Absicherung ist für Institutionen empfehlenswert, auf die folgende Punkte zutreffen:

- Die Umsetzung der IT-Sicherheit steht noch am Anfang, sie hat ein eher niedriges Niveau
- Die Geschäftsprozesse haben kein deutlich erhöhtes Gefährdungspotential bezüglich der IT-Sicherheit
- Das angestrebte Sicherheitsniveau ist normal
- Es sind keine digitalen oder analogen Werte vorhanden, deren Diebstahl, Zerstörung oder Kompromittieren einen existenzbedrohenden Schaden für die Institution bedeutet
- Kleinere Sicherheitsvorfälle können toleriert werden – das heisst solche, die zwar Geld kosten oder anderweitig Schaden verursachen, aber in der Summe nicht existenzbedrohend sind

1.3 Relevanz der Mitarbeiter-Sensibilität als Ergänzung zu technischen Massnahmen

Das Personal eines Unternehmens bzw. einer Behörde bildet die Grundlage für dessen bzw. deren Erfolg oder Misserfolg. Gleichzeitig sind die Mitarbeiterinnen und Mitarbeiter ein wesentlicher Bestandteil der Informationssicherheit. Wie die Erfahrung zeigt, sind selbst die aufwendigsten technischen Sicherheitsvorkehrungen ohne das richtige Verhalten der Mitarbeiter wirkungslos. Ein Bewusstsein dafür, was Informationssicherheit für die Institution und deren Geschäftsprozesse bedeutet und der richtige Umgang der Mitarbeiter mit den zu schützenden Informationen der Institution sind daher wesentlich.

Der beste Virenschutz und die beste Firewall sind nutzlos bei Personalausfall, fehlerhaften Gebrauch von Berechtigungen, Social Engineering und Sorglosigkeit im Umgang mit Informationen.