

Datensicherheit in der IT. Rechtliche und wirtschaftliche Anforderungen an den Umgang mit Risiko in der IT.

Compliance smart & easy kann Sicherheit in der IT gewährleisten

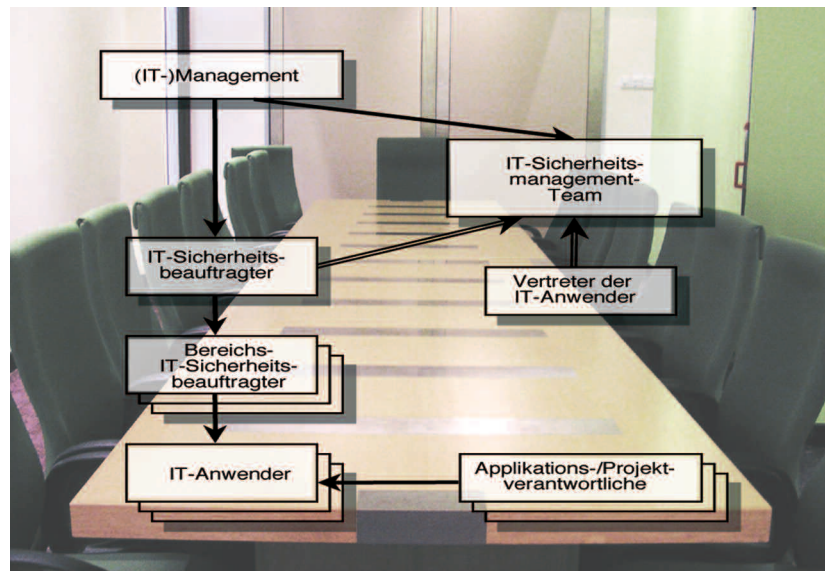
Knappe Personalressourcen, niedrige Budgets und hartes Tagesgeschäft führen dazu, dass gerade im KMU-Bereich (Informations-) Sicherheit oft hinten angestellt wird. Wie ein vernünftiges Risikomanagement in der IT auch bei kleinen Budgets möglich und wirtschaftlich sinnvoll machbar sein kann, skizziert Holger Schellhaas von evoltas (www.evoltas.de), Compliance-Guru und Prozessmanagement-Experte aus München

Lexpress: Sicherheit wird oft wie ein Stiefkind behandelt: Kostet nur Geld, bringt nichts für den Unternehmenserfolg – Inwieweit gibt es auch wirtschaftliche Argumente für einen IT-Grundschutz?

Holger Schellhaas: „Erfolgreiche Unternehmen – gerade auch KMU – wissen, dass die IT zur eigenen Wertschöpfung positiv beitragen kann, und sie haben auch verstanden, dass dies voraussetzt, die Risiken in der IT und durch die IT ausreichend kontrollieren zu können (und dies dann auch zu tun).

„Wer heute noch an der Existenzberechtigung eines IT-Grundschutzes zweifelt, hat die letzten Jahre verschlafen.“

Der IT-Grundschutzkatalog des BSI – in kompakter Form als Österreichische IT-Sicherheitshandbuch (www.cio.gv.at/securenetworks/sibb/) – stellt ein bewährtes Hilfsmittel zur Definition der Mindeststandards für die Informationssicherheit bereit, der eine schnelle und pragmatische Umsetzung des ISO-Standards 27001 erlaubt.“



Beispiel einer Grundstruktur zur Organisation des IT-Sicherheitsmanagements

Es gibt immer mehr rechtliche Anforderungen an die IT, insbesondere was die Datensicherheit betrifft. Wie kann man diesen Anforderungen genüge tun? Welche organisatorischen und technischen Mindestmaßnahmen sind erforderlich und wie viel darüber hinaus wirtschaftlich sinnvoll?

Holger Schellhaas: „Ich würde lieber von Informationssicherheit reden – also von der Vertraulichkeit,

Verlässlichkeit und Verfügbarkeit der Daten. Die immer gleiche Frage ist, ob es von Nutzen (also wirtschaftlich) ist, dies sicherzustellen und damit nicht nur Strafen vorzubeugen. Die Antwort ist ohne zu zögern „JA“. Die Bedeutung von Information und den zugrunde liegenden Technologien ist zweifelsohne nicht nur akzeptiert, sondern mittlerweile auch wirtschaftlich bewiesen.

Gesetze und Richtlinien setzen sich mit Kontrollen und daraus resultierenden Maßnahmen auseinander, jedoch findet dort die IT nur vereinzelt Niederschlag. In geradezu idealer Weise schließt das COBIT-Modell diese Lücke und kombiniert eine Vielzahl nationaler und internationaler Standards aus den Bereichen Qualität, Sicherheit und Ordnungsmäßigkeit. Das Resultat ist ein durchgängiges Modell, das für sämtliches IT-Ressourcen alle notwendigen organisatorischen und technischen Mindestmaßnahmen in klaren Worten festgelegt.“

Gibt es sinnvolle IT-Sicherheits-Strategien für KMU? Was muss oder sollte getan werden?

Holger Schellhaas: „Für mich gibt es keine KMU-Sicherheitsstrategie. Die entscheidende Frage lautet: ‚Wie kalkulieren und kontrollieren die KMU Ihr Risiko (wenn sie es denn kontrollieren)?‘

Die Kunst besteht doch darin, mit einer passenden Lösung die Mindestanforderungen zu erfüllen, ohne die Performance der IT

kaputt zu machen. Also ‚Compliance smart & easy‘.“

Inwieweit gibt es auch für KMU sinnvolle Argumente für den Einsatz eines IKS in der IT?

Holger Schellhaas: „Wenn die Unternehmen zumindest so groß sind, dass sie jährlich geprüft werden, können sie mit einem internen Kontrollsystem in der IT jederzeit dem zuständigen Wirtschaftsprüfer oder Auditor zeigen, dass die IT auf dem richtigen Weg ist.

Generell heißt ja nicht, dass ein IKS immer gleich viel Aufwand bedeuten muss. Es geht im Kern doch eigentlich nur um die Festlegung von Kontrollzielen und Durchführung von geeigneten Kontrollen, um die Dokumentation der Abweichungen und um die Dokumentation der eingeleiteten und umgesetzten Maßnahmen. Dass die IT nicht gerne dokumentiert, ist bekannt. Dass das aber so bleiben muss (und kann) steht nirgends.“

Interview: Mag. Michael Ghezze