

Einleitung

Zielgruppe: Geschäftsführung, IT-Entscheider, IT-Dienstleister

Ansatz: Orientierung an ISO/IEC 27001 ohne Zertifizierungsziel.

Einleitung

Dieses interne Handbuch beschreibt einen praxisnahen Weg zum Aufbau eines Informationssicherheits-Managementsystems für kleine und mittlere Unternehmen. Es richtet sich an IT-Entscheider, Geschäftsführungen und IT-Dienstleister, die bei einem Unternehmen praktisch bei Null beginnen: keine Dokumentation, keine geregelte Wartung, kein strukturiertes Risikomanagement und oft nur ein externer Dienstleister, der bei Störungen angerufen wird.

Das Ziel ist nicht, möglichst schnell eine ISO-27001-Zertifizierung zu erreichen. Das Ziel ist ein belastbares, nachvollziehbares und im Alltag nutzbares Sicherheitsniveau. Die ISO/IEC 27001 dient dabei als Orientierung, wird aber bewusst pragmatisch auf die Realität von KMU übertragen.

Warum dieses Handbuch?

Viele KMU sind vollständig von ihrer IT abhängig, verfügen aber nicht über die organisatorischen Strukturen, die für einen sicheren Betrieb notwendig wären. Häufig existieren keine aktuellen Netzwerkpläne, keine vollständige Asset-Liste, keine geprüften Backups, keine klaren Verantwortlichkeiten und kein Notfallplan.

Dieses Handbuch soll helfen, diese Lücke strukturiert zu schließen. Es beschreibt nicht nur, welche Themen betrachtet werden müssen, sondern auch, warum sie wichtig sind und welche Arbeitsergebnisse am Ende jeder Phase vorliegen sollten.

Grundprinzip

Informationssicherheit beginnt nicht mit Technik. Sie beginnt mit dem Verständnis des Unternehmens, seiner Geschäftsprozesse, Informationen und Risiken. Erst danach werden technische Maßnahmen sinnvoll ausgewählt und umgesetzt.

Revision #3

Created 1 July 2026 07:53:36 by Stefan Kittel

Updated 1 July 2026 08:32:12 by Stefan Kittel