ISIS 12

Informationssicherheit
für den Mittelstand

Was bedeutet ISIS12?
ISIS12 steht für Informations Sicherheitsmanagement System in 12 Schritten. Die Bild-/Wortmarke ist markenrechtlich geschützt. ISIS12 ist ein Sicherheitsstandard, der speziell für mittelständische Unternehmen entwickelt wurde.

Wer hat ISIS12 entwickelt?
ISIS12 wurde vom Netzwerk Informationssicherheit im Mittelstand (NIM) entwickelt. Das Netzwerk NIM besteht aus neun Unternehmen und zwei Hochschulen. Die Entwicklung wurde vom Bayerischen Staatsministerium für Wirtschaft, Infrastruktur, Verkehr und Technologie gefördert. Der Bayerischer IT-Sicherheitscluster e.V. ist für das Netzwerkmanagement verantwortlich.

Was umfasst ISIS12 genau?
ISIS12 ist ein detailliertes Vorgehensmodell zur Einführung eines Informationssicherheits-Managementsystems (ISMS) zur Verbesserung der Informationssicherheit in mittelständischen Unternehmen. Ziel ist es, dem Anwender einen konkreten Handlungsrahmen vorzugeben. So wurde der abstrakte Charakter der ISO/IEC 27001 durch ein konkretes Vorgehensmodell in 12 sequentiell zu durchlaufenden Schritten ersetzt. In diesem ersten Zyklus wird das ISMS etabliert. Nach dem ersten „Durchlauf“ dient das Verfahrensmodell als Vorlage für interne und externe Audits und stellt die Aktualität und Optimierung des ISMS sicher.

Was sind die Besonderheiten von ISIS12?
ISIS12 ist ein verständlich beschriebener 12-stufiger Prozess für die Etablierung eines ISMS (ISMS light). Es integriert ISMS und IT-Service Management. ISIS12 wird vom Anwender in Zusammenarbeit mit einem zertifizierten ISIS12-Dienstleister auf Basis eines speziell für den Mittelstand angepassten ISIS12-Maßnahmenkatalogs eingeführt. Es bildet eine Vorstufe zur möglichen ISO/IEC 27001- bzw. BSI IT-Grundschutz-Zertifizierung.

Welcher Aufwand ist für die Etablierung von ISIS12 erforderlich?
Der Aufwand für die Einführung von ISIS12 hängt stark von der jeweiligen Organisation und von den verarbeiteten Informationen ab. Der konkrete Aufwand kann erst nach einer entsprechenden Analyse durch einen ISIS12-Berater ermittelt werden. Generell kann jedoch angemerkt werden, dass der Aufwand nur einen Bruchteil eines ISO/IEC 27001- bzw. eines BSI IT-Grundschutz-Projektes ausmacht.

Ich möchte ISIS12 einsetzen. Was muss ich tun?
Nehmen Sie dazu Kontakt mit uns auf – wir beraten Sie gerne.
Für welche Organisationen ist ISIS12 geeignet?
ISIS12 wurde speziell für mittelständische Unternehmen entwickelt (ca. 50 – 1.500 rechnergestützte Arbeitsplätze). Darüber hinaus kann ISIS12 auch in anderen Organisationen erfolgreich eingesetzt werden.

Welche Rolle spielt das Datenschutzmanagement in ISIS12?
Das Datenschutzmanagement spielt bei ISIS12 eine wichtige Rolle. Beginnend bei der Besetzung des Sicherheitsteams bis hin zu konkreten Sicherheitsmaßnahmen aus dem Bereich Datenschutz im ISIS12-Katalog.

Ist Notfallmanagement (BCM) Bestandteil von ISIS12?
Der Standard ISIS12 beinhaltet auch den Bereich Notfallmanagement in Form von spezifischen Sicherheitsmaßnahmen zur Geschäftsfortführung im ISIS12-Katalog.

Gibt es für ISIS12 ein unterstützendes Tool, vergleichbar etwa mit dem BSI GSTOOL?
Durch den Einsatz eines speziell entwickelten ISIS12-Tools wird dem Anwender das Arbeiten mit dem Vorgehensmodell wesentlich erleichtert. Das Tool bildet den ISIS12 Workflow komplett ab, liefert Hinweise für die einzelnen Arbeitsschritte und dokumentiert diese zugleich. Das ISIS12-Tool wird bereits erfolgreich in ISIS12-Projekten eingesetzt und bietet neben einer Orientierung bei der Einführung des ISMS auch eine wertvolle Basis für die nachfolgenden Revisionsaufgaben im Rahmen der PDCA-Zyklen.

Besteht die Möglichkeit einer Zertifizierung?
Das ISIS12 Managementsystem ist zertifizierbar. Hierzu wurde ein ISIS12 Zertifizierungsschema entwickelt, das sich an der verbreiteten Praxis der ISMS-Zertifizierung orientiert: Die Gültigkeit des Zertifikats beträgt drei Jahre und wird durch zwei Überwachungsaudits begleitet.

Worin besteht der Unterschied zwischen ISIS12 und der ISO/IEC 27001 bzw. dem BSI IT-Grundschutz?
ISIS12 wurde mit der Möglichkeit der Skalierbarkeit entwickelt. Nach deren erfolgreichen Implementierung und optionalen ISIS12-Zertifizierung, steht der Weg in Richtung einer de-jure Zertifizierung nach „ISO/IEC 27001“ bzw. „ISO 27001 auf Basis von IT-Grundschutz“ offen. Hierzu müssen noch weitere Arbeitsschritte durchlaufen und entsprechende Dokumente angefertigt werden. Den dafür erforderlichen Aufwand kann ein ISIS12-Berater nach entsprechender Beratung ermitteln.

Warum gibt es bei ISIS12 keine Risikoanalyse?
Die Aussage ist so nicht korrekt. Es kommt im ISIS12 Vorgehensmodell eine implizite Risikoanalyse zum Einsatz. Es wurde bei der Entwicklung von ISIS12, ausgehend von den Designkriterien, zunächst bewusst auf eine vorangestellte Risikoanalyse verzichtet, wie dies etwa bei der ISO/IEC 27001 der Fall ist, da dieser basale Arbeitsschritt in der Praxis, nicht nur bei mittelständischen Unternehmen, zu größeren Problemen führen kann, die sich auf die daraus resultierende Sicherheitskonzeption negativ auswirken können. Auch nachgestellt wird wie bei der BSI IT-Grundschutzmethodik bewusst keine Risikoanalyse explizit angewandt (BSI 100-3). Vielmehr beinhaltet das an die BSI Grundschutzmethodik angelehnte Verfahren eine immanente Risikoanalyse: Die empfohlenen Sicherheitsmaßnahmen des ISIS12-Katalogs, die in der Umsetzungsphase wirksam umgesetzt werden müssen decken Grundgefährdungen ab. Somit kommt bei ISIS12 eine implizite Risikoanalyse zum Einsatz. Bei Organisationen, die über einen höheren Schutzbedarf verfügen (Unternehmen mit Forschungsabteilungen, Just-in-Time-Lieferanten, Behörden u.ä.) ist eine Risikoanalyse empfehlenswert. Aus

Kompatibilität zum ISIS12 Vorgehensmodell bietet sich hier eine Vorgehensweise nach den 2011 angepassten BSI 100-3 Standard (Version 2.5) an. Durch die Verwendung der vom BSI publizierten 46 Grundgefährdungen reduziert sich der dafür notwendige Aufwand erheblich. Es wird somit noch einmal analysiert, inwieweit die in der Sicherheitskonzeption enthalten Sicherheitsmaßnahmen aus dem ISIS12-Katalog für die Organisation angemessen sind. Es können sich daraus noch weitere zusätzliche Sicherheitsmaßnahmen ergeben, die in die Sicherheitskonzeption integriert werden müssen.

Worin besteht der Unterschied zwischen ISIS12 und bzw. dem BSI IT-Grundschutz bzw. der ISO/IEC 27001 (GAP-Analyse)?
ISIS12 wurde speziell mit der Möglichkeit der Skalierbarkeit entwickelt. Nach der erfolgreichen Implementierung des ISMS, Etablierung der Sicherheitskonzeption und der optionalen ISIS12-Zertifizierung, steht der Weg in Richtung einer de-jure Zertifizierung nach „ISO 27001 auf Basis von IT-Grundschutz“ bzw. „ISO/IEC 27001“ offen. Der Sicherheitsprozess ist nachweislich dokumentiert, es ist ein Managementsystem für die Informationssicherheit mit der kontinuierlichen Weiterentwicklung aktiv am Arbeiten: Die erforderlichen nächsten Arbeitsschritte sind je nach angestrebten Zertifizierung und Art der Organisation unterschiedlich. Die nachfolgenden Ausführungen dienten als Orientierung:

– ISIS12 –> ISO 27001 auf Basis von IT-Grundschutz:
Da sich die Architektur des ISIS12 Vorgehensmodells sich in den Schritten 1 und 6-12 sehr stark an der BSI IT-Grundschutzmethodik orientiert hat, ist nach erfolgter ISIS12-Zertifizierung der Weg zur Zertifizierung nach „ISO 27001 auf Basis von IT-Grundschutz“ zwar noch lange, aber in Sachen Methodik vertraut und somit abschätzbar. Folgende „Stationen des Wegs“ sind im Wesentlichen zu nennen:
a) Es sind noch weitere Maßnahmen aus den BSI IT-Grundschutzkatalogen der Siegelstufen A, B und C umzusetzen, die im ISIS12-Katalog nicht enthalten sind.
b) Es sind noch zusätzliche Bausteine der BSI IT-Grundschutzkataloge bei der Modellierung zu berücksichtigen. Speziell Bausteine in der Schicht 1 (Übergreifende Aspekte) und der Schicht 3 (IT-Systeme) fallen hier an.
c) Es ist noch eine ergänzende Sicherheitsanalyse mit einer eventuell daraus abgeleiteten Risikoanalyse (BSI 100-3) durchzuführen.
d) Aus dem BSI Zertifizierungsschema ergeben sich noch einige Dokumente (Referenzdokumente) die noch erstellt werden müssen.

– ISIS12 –> ISO/IEC 27001
Folgende markante Wegpunkte sind im Wesentlichen auf dem Weg zur ISO/IEC 27001 zu gehen:
a) Es ist eine Risikoanalyse (Risikoeinschätzung, Analyse, Bewertung und Messung der Risiken) durchzuführen, deren Ergebnisse die Grundlage der Sicherheitskonzeption sind.
b) Umsetzung der daraus abgeleiteten Sicherheitsmaßnehmen in Verbindung damit den anzuwendenden Maßnahmenzielen aus Annex A (A.5 – A.18)
c) Eine „Erklärung zur Anwendbarkeit“ (SOA) ist zu erstellen.
d) Ein Prozess zur kontinuierlichen Messung der Effizienz des ISMS ist zu etablieren.
e) Die permanente Weiterentwicklung und Anpassung des ISMS gilt es dokumentiert zu betreiben.
Der jeweils dafür erforderliche Aufwand ist für jede Organisation im Detail differenziert zu bewerten.