

Praktische Umsetzung von Informationssicherheitsstandards

In der iznMail 2/2006 wurden zwei anerkannte Standards für Informationssicherheitsmanagementsysteme (ISMS) vorgestellt. Der folgende Teil behandelt die praktische Umsetzung des Standards ISO 27001 auf Basis von IT-Grundschutz des Bundesamtes für Sicherheit in der Informationstechnik (BSI).

Die Entscheidung zur Einführung und Umsetzung von Informationssicherheitsstandards beruht auf unterschiedlichen internen und externen Anforderungen:

- ▶ externe, wie z. B. der Nachweis eines bestimmten Sicherheitsniveaus oder die Erfüllung gesetzlicher Anforderungen
- ▶ interne, z.B. die Einführung des ITIL-Prozesses „Security Management“.

Soll nun ein Informationssicherheitsstandard in einer Organisation eingeführt werden, so muss zunächst eine Vielzahl von Fragen beantwortet werden, u.a.:

- ▶ Welche Abgrenzungen hat der IT-Verbund?
- ▶ Wer ist für die Umsetzung verantwortlich?
- ▶ Welche internen und externen Ressourcen müssen eingebunden werden?
- ▶ Welche Fachkenntnisse sind für die Umsetzung erforderlich?
- ▶ Wie lange dauert die Einführung?

Die prinzipielle Vorgehensweise bei der Einführung eines ISMS wird in dem BSI-Stan-

dard 100-2 ausführlich beschrieben. Gemäß dieser Vorgehensweise muss eine IT-Sicherheitskonzeption für einen IT-Verbund erstellt werden; dabei ist der Begriff „IT-Verbund“ wie folgt definiert:

„Unter einem IT-Verbund ist die Gesamtheit von infrastrukturellen, organisatorischen, personellen und technischen Komponenten zu verstehen, die der Aufgabenerfüllung in einem bestimmten Anwendungsbereich der Informationsverarbeitung dienen. Ein IT-Verbund kann dabei als Ausprägung die gesamte IT einer Institution oder auch einzelne Bereiche, die durch organisatorische Strukturen (z. B. Abteilungsnetz) oder gemeinsame Geschäftsprozesse bzw. IT-Anwendungen (z. B. Personalinformationssystem) gegliedert sind, umfassen.“



Diese Definition klingt zunächst erst einmal relativ einfach, bereitet aber in der Praxis häufig Schwierigkeiten, wenn nicht eine gesamte Organisation, sondern lediglich ein Teilverbund (z.B. ein Fachverfahren) betrachtet wird oder Abhängigkeiten zu anderen Organisationen bestehen. In beiden Fällen müssen klare und eindeutige Schnittstellen definiert werden.

Eine Hilfestellung bei der Definition des IT-Verbundes liefert Abb. 1. Für den Fall, dass ein IT-Sicherheitskonzept für die gesamte Organisation gefordert wird, müssen alle Anwendungen, IT-Systeme, Mitarbeiter und Beschäftigten sowie Räume und Gebäude in den IT-Verbund mit aufgenommen werden. Die Grenzen dieses IT-Verbundes sind die „natürlichen“ Netzwerkgrenzen, an Dritte ausgelagerte Anwendungen oder IT-Systeme werden später durch den Baustein „Outsourcing“ der IT-Grundschutz-Kataloge modelliert. Wird jedoch nicht eine einzelne Organisation in ihrer Gesamtheit, sondern einzelne oder mehrere Geschäftsprozesse bzw. Fachverfahren zugleich betrachtet, so wird es ein wenig komplizierter, da noch unterschieden werden muss, ob diese Geschäftsprozesse ausschließlich die eigene Organisation betreffen oder sich auf weitere Organisationen außerhalb der eigenen erstrecken. Sind mehrere Organisationen betroffen, so kann meist nur bedingt Einfluss auf die externen Organisationen ausgeübt werden. Es müssen geeignete Schnittstellen der zu betrachtenden Geschäftsprozesse gefunden und definiert werden. Eine technische Schnittstelle können aus Sicht eines IT-Dienstleisters z.B. ein Router, ein VPN-Gateway oder die Endgeräte für die Erbringung eines IT-Service sein, die im eigenen Haus aufgestellt sind oder dem Servicenehmer entliehen wurden und sich in der (Administrations-) Hoheit der eigenen Organisation befinden. Empfehlenswert ist es hier, dem Nutzer im Laufe der Erstellung des IT-Sicherheitskonzepts Hinweise für den sicheren Einsatz der genutzten Services zu geben. Erstreckt sich der IT-Verbund ausschließlich auf die eigene Organisation, so

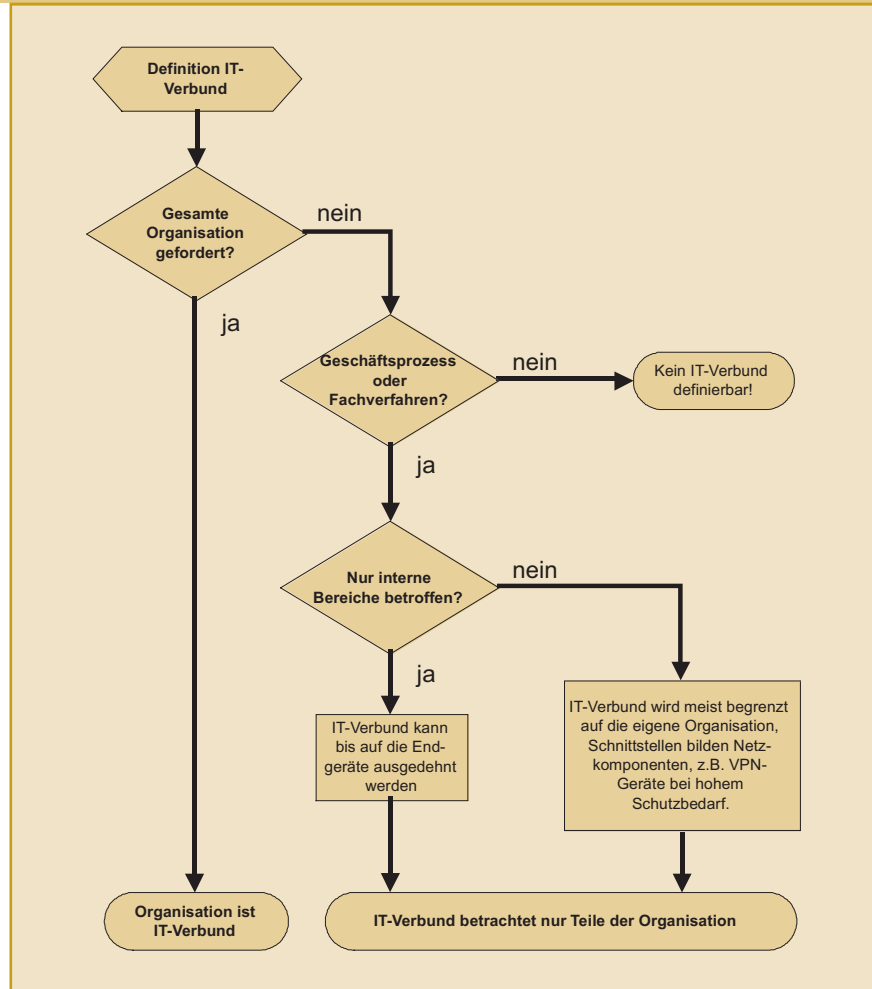
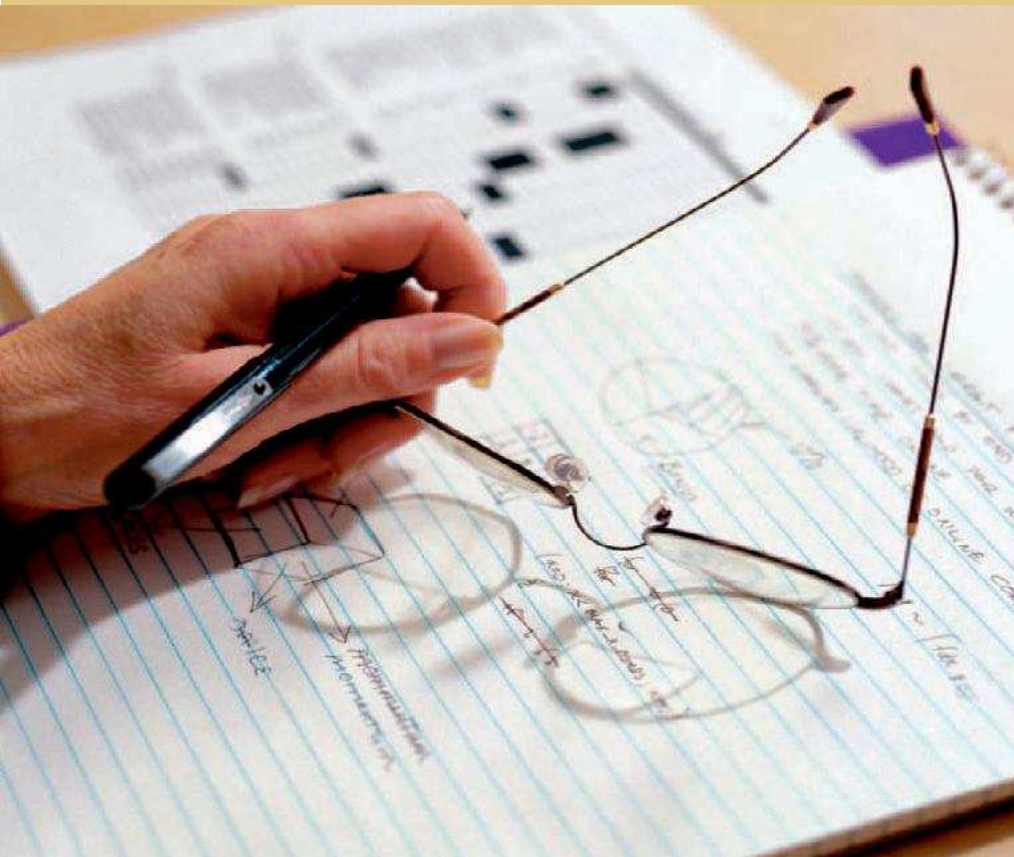


Abb. 1: Entscheidungskriterien bei der Definition eines IT-Verbundes

werden häufig die Endgeräte mit in den IT-Verbund einbezogen. Im Allgemeinen ist eine pragmatische Vorgehensweise zielführender als eine langwierige Entscheidungsfindung mit der Folge, dass die IT-Sicherheitskonzeption verzögert wird und Geschäftsprozesse oder Fachverfahren ggf. gefährdet sind und bleiben. Sofern eine spätere Zertifizierung des IT-Verbundes erwogen wird, sollte dieser auf jeden Fall bereits vor der Erstellung der eigentlichen IT-Sicherheitskonzeption mit dem BSI abgestimmt werden.

Nach der Definition eines geeigneten IT-Verbundes müssen Verantwortlichkeiten definiert werden. Idealerweise existiert bereits ein unabhängiger IT-Sicherheitsbeauftragter z.B. als Stabsstelle innerhalb der Organisation. Häufig wird dieser gerade in kleineren Organisationen aber auch erst im Rahmen der Erstellung einer IT-Sicherheitskonzeption

ernannt, insbesondere dann, wenn eine Zertifizierung angestrebt wird. Aufgabe des IT-Sicherheitsbeauftragten ist es unter anderem, die Erstellung eines IT-Sicherheitskonzeptes zu koordinieren. Abhängig von der Größe und der Struktur der Organisation werden Projektverantwortliche ernannt. In der Praxis trifft man auch häufig auf IT-Sicherheitsbeauftragte, die über eine reine Koordinations- und Kontrolltätigkeit hinausgehend weitestgehend selbst an der Erstellung der IT-Sicherheitskonzeption beteiligt sind. Dieses ist problematisch, da eine unabhängige Kontrollinstanz (Vier-Augen-Prinzip, Interessenkollision) zur Beurteilung der IT-Sicherheitskonzeption fehlt. Häufig ist eine Trennung dieser Rollen (IT-Sicherheitsbeauftragter und Ersteller des IT-Sicherheitskonzeptes) nicht möglich. Insbesondere gilt dieses für kleinere Organisationen, wo der IT-Sicherheitsbeauftragte noch weitere Funktionen und Rollen wahrnimmt. Gerade hier



sollte in Erwägung gezogen werden, diese Kontrollfunktion durch Dritte ausführen zu lassen.

Die Erstellung des IT-Sicherheitskonzeptes selbst ist nicht trivial, da eine Vielzahl von Rahmenbedingungen und Abhängigkeiten erfasst und berücksichtigt werden muss. Auch die Anwendung und der Umgang mit den IT-Grundschutz-Katalogen des BSI sind nicht immer selbsterklärend. Der Aufwand und das eigene Know-how werden meist unterschätzt, vor allem, wenn innerhalb der Organisation noch keine oder nur wenige Erfahrungen mit der Thematik vorhanden sind. Hier bietet sich ein frühzeitiger Erfahrungsaustausch mit anderen, bereits erfahrenen Organisationen an. Alternativ sollte überlegt werden, einen externen Berater bereits im frühen Projektstadium heranzuziehen. Der externe Coach ist aufgrund seiner Erfahrung in ähnlichen Projekten in der Lage, korrigierend in den Projektverlauf einzugreifen, so dass die „Stolpersteine“ bereits frühzeitig aus dem Weg geräumt werden. Die Gefahr, dass die Organisation aus Mangel an Erfahrung bei der Erstellung der Sicherheitskonzeption in eine falsche

Richtung steuert und dieses erst sehr viel später nach hohem internen Aufwand bemerkt wird, wird damit auf ein Minimum reduziert.

Eine konkrete Abschätzung zur Dauer der Erstellung und Umsetzung eines IT-Sicherheitskonzeptes ist ohne Kenntnis näherer Einzelheiten über den IT-Verbund nicht möglich, da dieses von zahlreichen Faktoren abhängig ist: die Größe des IT-Verbundes und die Komplexität der Geschäftsprozesse, das vorhandene interne Know-how, die zur Verfügung stehenden Ressourcen, bereits vorhandene oder nicht vorhandene Dokumentationen etc. Entscheidend ist auch, ob

es sich um die reine Erstellung einer IT-Sicherheitskonzeption für eine interne Verwendung handelt oder ob eine Zertifizierung des IT-Verbundes erfolgen soll. Wird keine Zertifizierung angestrebt, sollten für die Erstellung einer qualifizierten IT-Sicherheitskonzeption drei bis sechs Monate eingeplant werden. Soll der IT-Verbund hingegen auf Basis von ISO 27001/GS zertifiziert werden, so muss auch die zeitliche Dauer für die Umsetzung der relevanten Maßnahmen mit einkalkuliert werden, so dass unter optimalen Bedingungen eine Dauer von 12 bis 24 Monaten realistisch ist. Optimale Bedingungen bedeutet dabei, dass die Methodik nach den BSI-Standards bekannt ist und der jeweilige Projektstand durch eine interne oder externe Kontrollfunktion regelmäßig überprüft wird.

Fazit:

Die zielführende und wirtschaftliche Umsetzung von Informationssicherheitsstandards ist das Ergebnis einer planvollen Vorgehensweise nach einem anerkannten Standard („best-practise“). Erfolgskritisch ist die realistische Einschätzung der benötigten internen und externen Ressourcen, des eigenen Know-hows sowie eine regelmäßige Kontrolle der jeweiligen Teilschritte von unabhängiger bzw. neutraler Seite. Auch kann es sinnvoll sein, zunächst nur einen kleinen, überschaubaren Teilverbund als IT-Verbund zu definieren, um im Anschluss mit dem dazu gewonnenen Know-how den IT-Verbund auf die gesamte Organisation auszuweiten.

Quellenangaben:
www.bsi.de

*Detlef Kilian
Senior Consultant
Lizenzierter ISO 27001 Auditor
auf Basis von IT-Grundschutz
DS DATA SYSTEMS GmbH
in Braunschweig.*

*Kontakt:
dkilian@datasystems.de
Tel. 0531/23731-0*

